LifeLabs: Court considers privilege claims over cybersecurity investigation materials

May 16, 2024

In most cases, a cybersecurity breach triggers a multi-faceted response which may involve legal counsel, internal personnel, external investigators, and others. A responding organization or public body will usually take steps to investigate, whether it be as a matter of internal business procedure, compliance with statutory obligations, seeking or obtaining legal advice, or preparation for anticipated litigation. Often these purposes overlap, which raises the question: what information in the investigation file is privileged?

The Divisional Court of the Ontario Superior Court of Justice recently addressed this question in the judicial review decision of *LifeLabs LP v. Information and Privacy Commr. (Ontario)*, 2024 ONSC 2194 (CanLII). The Court upheld a decision by the Information and Privacy Commissioner of Ontario (ON IPC) that certain documents requested in the course of a regulatory investigation were not subject to privilege. The Court found that litigation and solicitor-client privilege do not extend to underlying facts that would otherwise be disclosed pursuant to a statutory duty. Moreover, it held that copying counsel to a document does not automatically cast a "cloak" of privilege over the document or its underlying facts.

The Court's analysis highlights the interplay between the law of privilege and compliance with statutory investigative obligations in a cybersecurity incident response context. In our view the decision is fact-specific and does not change the law, but it is cautionary and instructive.

Background

This case arose from a 2019 cyber incident in which criminals accessed the personal information of millions of individuals, the majority of whom lived in Ontario and British Columbia.

LifeLabs is a health information custodian under the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A (PHIPA). Under PHIPA, LifeLabs has duties in relation to privacy breaches and the ON IPC has the authority to conduct investigations in relation to those duties.

The privacy commissioners for Ontario and British Columbia coordinated a joint investigation. During the investigation, the commissioners relied on their statutory powers to order LifeLabs to disclose various documents relating to LifeLab's investigation. LifeLabs resisted and asserted privilege over five sets of documents and the information within them:

1. The investigation report prepared by a third-party cybersecurity firm hired by LifeLabs, which described how the cyberattack occurred.
2. Email correspondence between a cyber intelligence firm, hired by LifeLabs, and the cybercriminals.
3. An internal data analysis prepared by LifeLabs to determine whose personal health information was affected for statutory notification purposes.
4. A submission from LifeLabs, through legal counsel, to the commissioners in response to certain specific questions.
5. A report by Deloitte LLP, hired by LifeLabs, which was prepared as part of the representations that LifeLabs submitted to the commissioners.

On June 25, 2020, the commissioners jointly decided that LifeLabs' claims of privilege were not substantiated on the evidence and that they should fail. The commissioners also held that facts which exist independently outside the privileged documents are not protected from regulatory investigations simply because they are included in privileged documents.

In response, LifeLabs sought judicial review of the commissioners' decision.

The judicial review decision

The Divisional Court dismissed LifeLabs' application for judicial review and upheld the commissioners' decision. The Court's analysis focused on the application of fundamental principles of litigation and solicitor-client privilege in the regulatory context of this case. Several important findings were made:

a) Unprivileged facts are producible

Litigation privilege protects confidential documents and communications whose "dominant purpose" is preparation for litigation. It applies to a party's litigation strategy but does not extend to underlying facts that would otherwise have to be disclosed, even if those facts are obtained through counsel or are useful in preparing for litigation. The Court held that LifeLabs could not claim litigation privilege over facts that LifeLabs had an obligation to disclose under PHIPA.

Similarly, the Court held that solicitor-client privilege, which protects confidential communications made between counsel and their client for the purpose of seeking or giving legal advice, does not extend to facts that are required to be produced pursuant to a statutory duty. The Court echoed the ON IPC's submission that "[w]hen deciding if such facts are privileged, one must keep one eye on the need to protect the freedom and trust between solicitor and client and another eye on the potential use of privilege to insulate otherwise discoverable evidence."[1]

The Court upheld various findings of fact made by the ON IPC that the evidence did not substantiate LifeLabs' privilege claims. In particular, LifeLabs did not provide evidence that disclosure of the disputed information would reveal litigation strategy or solicitor-client communication, or that the investigation report prepared by the third-party cybersecurity firm was prepared for the dominant purpose of litigation.

Significantly, this is a warning that health information custodians cannot defeat their duty to respond to investigatory inquiries by placing facts inside privileged documents. If an investigator retained by an organization's counsel to conduct a privileged investigation, for example, reports to counsel that the digital evidence shows that the threat actor(s) used a data staging tool – a precursor to data exfiltration – the *fact* the threat actor(s) used a staging tool (and possibly the underlying evidence) must be produced. The report itself (which may contain nuance and context) remains privileged. Understanding the distinction between a privileged and non-privileged document or communication is one of the most important things for organizations under attack to understand; it allows for safe communication of facts and evidence to regulators and all other stakeholders while protecting privilege.

b) *In re Capital One* is persuasive in relation to third-party cybersecurity service providers

The Court also made an important finding about the basis for a privilege claim, particularly when an organization uses a forensic investigator who provides services in advance of an incident. The Court noted that the U.S. decision *In re Capital One Consumer Data Security Breach Litigation*, 2020 U.S. Dist. LEXIS 91736 (E.D. Va May 26, 2020) is persuasive authority for the proposition that where a company hired a cybersecurity firm to perform essentially the same services before and after the breach, simply inserting counsel's name into the contract and having counsel receive deliverables on behalf of the client does not render those deliverables subject to the U.S. work product doctrine, which is akin to Canada's litigation privilege.

The Court upheld the ON IPC's reliance on *In re Capital One* and its finding that the cybersecurity firm retained by LifeLabs that produced a report on the breach did so for business purposes and not for the dominant purpose of litigation.

Many organizations hire third-party providers to provide managed security services that entail monitoring networks for intrusion. Managed service provider contracts often include a bundle of hours for incident response. Use of these services is appropriate for initial investigation, but *LifeLabs* suggests that use of the same provider to conduct a privileged forensic investigation (without very careful documentation) is a risk.

Practical takeaways

Protecting legal privilege is critical when responding to a cybersecurity breach and, as illustrated in *LifeLabs*, a careful approach to creating and making privilege claims is required. The following practices will help organizations establish, maintain, and assert privilege when responding to a cybersecurity breach.

1. **Be proactive and have an incident response plan** . Having a plan in place before an incident occurs will help avoid an *ad hoc* and under-protective approach to

establishing a privilege claim. The plan should include a procedure for invoking privilege that is intentional, discretionary, and alive to the relevant risks. Automatic and non-discretionary procedures, such as routinely copying a lawyer to documents without more, are insufficient.

2. **Engage legal counsel at the outset** . Ideally this would be part of the incident response plan. Involving legal counsel before any investigative steps are taken is critical to establishing and maintaining privilege. Counsel can provide essential advice on statutory and legal obligations, anticipated or actual litigation, third-party service provider retainers, and public communications, all of which trigger privilege considerations.
3. **Understand that some very sensitive work by third-party experts will not be privileged because it is fact and only fact** . Communications between third-party experts and threat actor(s) are the best example of this type of sensitive but non-privileged communication. Put clearly, they can never be privileged. Not only may such communications be producible in litigation or in a regulatory investigation, but they are also often leaked by threat actor(s) themselves. Counsel should direct the expert to speak carefully, with a view to eventual disclosure.
4. **Be prepared to substantiate a privilege claim on the evidence** . Parties asserting privilege should be prepared to put forward evidence that substantiates their claims on a document-by-document basis.[2] As the Divisional Court in *LifeLabs* noted, a privilege claim may require proof that disclosure of the facts would disclose litigation strategy or solicitor-client communication. A party claiming litigation privilege over a document should be able to show that it was prepared for the dominant purpose of litigation.

If you have questions about this publication or if you would like to speak with us about BLG's leading cyber incident response practice, please contact the authors or the individuals identified below.

Footnotes

[1] *LifeLabs LP v. Information and Privacy Commr. (Ontario)*, 2024 ONSC 2194 (CanLII) at para. 80.

[2] *Alberta v. Suncor Inc*, 2017 ABCA 221 (CanLII) at para. 43; *Mamaca v. Coseco Insurance Company*, 2007 CanLII 54963 (ON SC) at paras. 16-23; *Shaughnessy Golf & Country Club v. Drake International Inc.*, 1986 CanLII 163 (BC CA) at 14.

By

Ingrid Vanderslice, Daniel J. Michaluk

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2025 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.