

Loss of Legal Privilege over Cyberattack Investigation Report

Cyber incident response activities often involve the creation of forensic investigation reports that might be protected by legal privilege, depending on the purpose of the reports and the circumstances surrounding their creation and use. The 2018 Ontario Superior Court decision in *Kaplan v. Casino Rama Services* illustrates how an organization can lose the right to assert legal privilege over a cyber incident investigation report.

Legal Privilege – Basic Rules

Cyber incident response activities usually involve the creation of many kinds of communications and documents, including forensic investigation reports, that might be subject to legal disclosure obligations in connection with contractual audits, regulatory investigations or civil lawsuits, even if the organization's personnel expected the communications and documents to remain confidential. However, an organization might be able to protect some of those communications and documents against involuntary disclosure by invoking a doctrine known as "legal privilege".

Two Kinds of Legal Privilege

There are two kinds of legal privilege under Canadian law that might be relevant to cybersecurity incident activities – "legal advice" privilege and "litigation" privilege. Each kind of privilege is different in purpose, scope and duration. Communications and documents might be protected by either or both kinds of privilege. An organization that asserts legal privilege over a communication or document has the burden of proving that the privilege applies.

Legal advice privilege (also known as "solicitor-client" privilege) applies to confidential communications between a client and their lawyer for the purpose of seeking or giving legal advice. The privilege applies whenever a client seeks legal advice from their lawyer, regardless of whether or not litigation is ongoing or anticipated. The privilege lasts unless and until it is waived by the client.

Litigation privilege (also known as "work product" or "lawyer's brief" privilege) applies to communications and documents created for use in connection with ongoing or reasonably anticipated litigation. The privilege applies to communications and documents between a client and their lawyer and to certain kinds of communications and documents between a lawyer and a third party (e.g. a technical advisor engaged by the lawyer). The privilege applies only if a communication or document is made for the "dominant purpose" (but not necessarily the sole purpose) of use in connection with ongoing or reasonably anticipated litigation. The privilege

lasts until the relevant litigation and any closely related litigation have ended or the privilege is waived by the client.

Waiver of Legal Privilege

A client may waive their right to assert legal privilege over communications and documents. Waiver of privilege ordinarily requires the client to knowingly and voluntarily demonstrate, by words or conduct, an intention to waive privilege. Nevertheless, privilege can also be waived inadvertently or implicitly in circumstances where fairness and consistency require it.

Waiver of Privilege – *Kaplan v. Casino Rama Services*

The Ontario Superior Court decision in *Kaplan v. Casino Rama Services* illustrates how an organization can waive legal privilege over a forensic investigation report by disclosing information contained in the report. The case involved a proposed class action against the owners and operators of the Casino Rama Resort relating to a cyberattack that resulted in the theft of personal and financial information of Casino Rama's employees and customers.

Casino Rama publicly disclosed the attack and notified approximately 200,000 individuals. Casino Rama and its legal counsel engaged Mandiant, an independent cybersecurity company, to conduct a forensic investigation and prepare two reports: (1) a report summarizing Mandiant's observations, findings and opinions regarding the cyberattack; and (2) a report outlining Mandiant's suggested remediation activities. Casino Rama considered both reports to be protected by legal privilege.

In connection with the plaintiffs' application for certification of a class action lawsuit, Casino Rama filed an affidavit that provided details of the cyberattack based on the results of the Mandiant investigation. The affidavit explained that Casino Rama did not waive legal privilege over communications with Mandiant. The plaintiffs then applied to court for an order requiring Casino Rama to produce the Mandiant reports. Casino Rama resisted the application on various grounds, including by asserting legal privilege over the reports.

The court did not decide whether the Mandiant reports were protected by legal privilege. Instead, the court held that even if the reports were protected by legal privilege, the privilege had been waived by Casino Rama when it filed an affidavit based on information provided by Mandiant. The court reasoned that “it would be unfair to the Plaintiffs to ask the court to accept the Defendants’ evidence on the size and scope of the prospective class, based on the Mandiant investigation, without producing those parts of the Mandiant Reports relating to that issue”. The court stated: “A party cannot disclose and rely on certain information obtained from a privileged source and then seek to prevent disclosure of the privileged information relevant to that issue. Waiver of privilege would be required as a matter of fairness, but limited only to the issue disclosed”.

The court rejected Casino Rama’s argument that it had not waived legal privilege over the Mandiant reports because it was required by the Ontario *Class Proceeding Act* to provide its best information on the number of members in the class. The court held that Casino Rama, having chosen to rely on information obtained from Mandiant as a basis for evidence of the size of the class, could not assert legal privilege to refuse to disclose parts of the Mandiant reports that discuss that issue.

The court explained that waiver of legal privilege was limited to aspects of the Mandiant reports referenced or relied on in the affidavit. The court stated: “. . . reliance on one aspect of an expert’s opinion or report does not waive privilege with respect to other unrelated aspects. Fairness is a two-way street and the court must be cautious not to waive privilege on unrelated aspects of an opinion

as an overbroad remedy to address disclosure which relates only to one aspect of the opinion”. The court also held that principles of relevance and proportionality limited the required disclosure of the reports to the parts relevant to the size and scope of the potential class.

Comment

The *Casino Rama* decision illustrates the importance of implementing a legal privilege strategy when preparing a cyber incident response plan and responding to a cybersecurity incident. To the extent practicable, the strategy should enable the organization to establish and maintain legal privilege over sensitive forensic investigation reports regarding a cyber incident while still complying with legal obligations to report the incident to regulators, give notice of the incident to affected individuals and organizations, and disclose information about the incident in legal proceedings. The strategy should be periodically reviewed and refreshed to be consistent with guidance provided by recent court decisions.

For more information about legal privilege, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*; *Cyber Risk Management – Legal Privilege Strategy (Part 2)*; and *Legal Privilege for Data Security Incident Investigation Reports*.

For more information about data security breach obligations, see BLG bulletins *Preparing for Compliance with Canadian Personal Information Security Breach Obligations* and *Canadian Investment Industry Regulator Proposes Mandatory Cybersecurity Incident Reporting*. ■

Author

Bradley J. Freedman

T 604.640.4129

bfreedman@blg.com

BLG’s Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG’s Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

BORDEN LADNER GERVAIS LLP LAWYERS | PATENT & TRADEMARK AGENTS

Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances. Copyright © 2018 Borden Ladner Gervais LLP.

BLG Vancouver

1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com