JUNE 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Legal Privilege for Data Security Incident Investigation Reports

Data security incident response activities usually involve the creation of sensitive communications and documents that might be subject to legal disclosure obligations unless they are protected by legal privilege. The recent U.S. District Court decision in *Re Experian Data Breach Litigation* provides helpful guidance for establishing legal privilege over data security incident investigation reports prepared for use in connection with litigation.

Legal Privilege

- **Basic Rules**

There are two kinds of legal privilege under Canadian law that might be relevant to data security 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, depending on the circumstances. 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 lawyer and client for the purpose of seeking or giving legal advice. The privilege applies whenever a client seeks legal advice from a 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" privilege 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 lawyer and client and to certain kinds of communications and documents between a lawyer and third parties. 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.

A client may waive legal privilege. 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.

- **Legal Privilege Strategy**

It is prudent for an organization to establish a legal privilege strategy for its cyber risk management activities, including preparing for and responding to data security incidents, so that the organization is able to establish legal privilege, where appropriate, over communications and documents created in the course of those activities.

The importance of a legal privilege strategy is illustrated by the U.S. court decisions in *Genesco Inc. v. Visa USA Inc.* and *Re Target Corporate Customer Data Security Breach Litigation*. Each of those lawsuits related to a data incident that was subject to two separate internal investigations by separate teams – a business investigation for business purposes, and a legal investigation (directed by an external lawyer) for legal advice and litigation purposes. The plaintiffs in the lawsuits sought disclosure of the investigation reports. In each lawsuit, the court held that the report resulting from the business investigation had to be disclosed, but the report resulting from the legal investigation was protected by legal privilege and did not have to be disclosed.

More information about data security incident reporting and disclosure obligations, the basic rules for legal privilege and practical recommendations for a legal privilege strategy for cyber risk management activities may be found in BLG bulletins *Cyber Risk Management – Legal Privilege Strategy – Part 1* and *Cyber Risk Management – Legal Privilege Strategy – Part 2*.

Experian Data Breach Litigation Decision

The decision in *Re Experian Data Breach Litigation* involved a consolidated class action arising out of an alleged theft of personal information of millions of T-Mobile customers and subscribers that was hosted on a server operated by Experian. After the data breach was discovered, Experian's external litigation counsel hired Mandiant, an independent forensic consultant, to conduct an analysis of the breach and prepare an expert report. Mandiant delivered the report to Experian's external litigation counsel, who then shared the report with Experian's in-house counsel. The report was used by Experian's external litigation counsel and in-house counsel to develop their legal strategy.

Experian refused to disclose Mandiant's report to the class action plaintiffs on the basis that the report was protected by work product privilege. The class action plaintiffs applied to court for an order compelling Experian to disclose Mandiant's report. The plaintiffs made four arguments, each of which was rejected by the court, as follows:

- The plaintiffs argued that Mandiant's report was not privileged because Experian had independent business duties to investigate the data breach, and Mandiant was hired for that purpose. The court rejected that argument because the evidentiary record made it clear that Mandiant conducted the investigation and prepared the report for external litigation counsel in anticipation of litigation, even if that was not the only purpose of the report. The court noted that Mandiant's report had not been given to Experian's incident response team. The court found that Mandiant's report would have had different form and content were it not prepared for the purpose of anticipated litigation.
- The plaintiffs argued that Mandiant's report was not privileged because Experian had previously engaged Mandiant to perform similar work regarding a data breach that occurred two years earlier, and Mandiant was just again doing work in the course of ordinary business for Experian. The court rejected that argument because Mandiant's previous work for Experian was separate from the work that Mandiant did for Experian's litigation counsel.
- The plaintiffs argued that fairness required Mandiant's report be disclosed because Mandiant must have prepared the report based on an analysis of Experian's live servers, and it was impossible for the plaintiffs' experts to go back in time and conduct a similar analysis. The court rejected that argument because the evidence showed that Mandiant's report was based on an analysis of server images rather than access to Experian's live systems, networks or servers. The court reasoned that the plaintiffs could engage their own experts to analyze the same server images used by Mandiant, and the resulting expense and inconvenience to the plaintiffs was not sufficient to overcome legal privilege.
- The plaintiffs argued that Experian had waived legal privilege by disclosing Mandiant's report internally and to T-Mobile. The court rejected that argument because disclosure of the report had been closely controlled by Experian's external litigation counsel and in-house legal department, and did not constitute a waiver of legal privilege. The court noted that the report was not given to Experian's incident response team or personnel working on remediation of Experian's systems affected by the data breach. The court also noted that disclosure of a redacted version of the report to T-Mobile was pursuant to a written joint defence agreement between Experian and T-Mobile, which was made because they recognized the risk of litigation arising from the data breach.

The *Experian Data Breach Litigation* decision illustrates some measures that a Canadian organization might take to support claims of litigation privilege over a data security incident investigation report, including:

1. The forensic investigator should be hired by outside legal counsel expressly retained to advise the organization regarding the incident and related litigation.
2. The organization, outside legal counsel and the forensic investigator should jointly create an accurate evidentiary record that clearly demonstrates that the investigation report is prepared primarily for legal privilege purposes, and not for ordinary business purposes.
3. The forensic investigator's engagement should be limited to work relevant to assisting outside legal counsel to provide legal advice and prepare for litigation.
4. The forensic investigator should deliver its report to, and communicate with, outside legal counsel only. The forensic investigator should not communicate directly with the organization's in-house legal counsel or the incident response team.
5. The investigation report should be based on an analysis of documents and data (e.g. server images) that are preserved for subsequent disclosure in litigation.
6. Any disclosure of the forensic investigator's report and related documents should be limited and consistent with litigation privilege purposes and carefully controlled to demonstrate confidentiality and avoid inadvertent waiver of privilege.
7. If actual or anticipated litigation involves multiple defendants, then any disclosure of the forensic investigator's report and related documents to co-defendants should be limited (e.g. disclosure of redacted versions only) and made pursuant to an appropriate written joint defence agreement that maintains confidentiality and privilege.

It is important to note that the *Experian Data Breach Litigation* decision involved a claim of litigation privilege for an expert investigation report prepared for the purpose of reasonably anticipated litigation regarding a specific data security incident. The decision did not involve a claim of legal advice privilege for a technical report prepared for the purpose of legal advice regarding preventative cyber risk management activities, which would require the application of a different legal test that might not be satisfied in all circumstances.

Comment

A legal privilege strategy can help establish legal privilege over certain kinds of communications and documents created during preventative cyber risk management activities and data security incident response activities. A legal privilege strategy should be carefully planned, effectively implemented and periodically reviewed and refreshed to reflect legal advice based on guidance provided by recent court decisions. U.S. cases can be instructive for Canadian organizations, but those cases must be considered with caution because U.S. rules for legal privilege are different, in some respects, from Canadian rules. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

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

For more information about cyber risk management and BLG's related legal services, please see the BLG website.

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com