Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PHIPA DECISION 114

Complaint HR19-00519

LIFE LABS LP

March 30, 2020

Summary: The IPC issues an interim order directing LifeLabs to produce documents relevant to the IPC's investigation into the cyberattack on LifeLabs' computer systems.

Cases Considered: *Blank v. Canada (Minister of Justice)*, 2006 SCC 39 (CanLII); *Thomson v. Berkshire Investment Group Inc. et al.*, 2007 BCSC 50; *Lizotte v. Aviva*, 92016] 2 SCR 521; *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44, *Huang v. Silvercorp Metals Inc.*, 2017 BCSC 795; *General Accident Assurance Company v. Chrusz*, 45 O.R. (3d) 321; 1999 CanLII 7320 (ON CA); *Shen v. Canada (Minister of Citizenship and Immigration)* 2017 FC 115 (CanLII); *Fresco v. Canadian Imperial Bank of Commerce*, 2019 ONSC 3309 (CanLII); *Shaughnessy Golf & Country Club v. Drake International Inc.*, 1986 CanLII 163 (BC CA); *Hosanna Enterprises Ltd. (Seraphim Christian Books 7 Supplies) v. Laser City Audio Video Ltd.*, 1999 CanLII 5836 (BC SC); *Waugh v. British Railway Board*, [1979] 2 All E.R. 1169; *Fred v. Westfair Foods Ltd. et al.*, 2003 YKSC 39 (CanLII); *Whitehead v. Braidnor Construction Ltd.*, 2001 ABQB 994 (CanLII); *Dow Chemical Canada ULC. v. Nova Chemicals Corporation*, 2014 ABCA 244 (CanLII); *Borkowski (Litigation guardian of) v. Ontario (Minister of Health)*, 2007 CanLII 18017 (ON SC); *Prescott and Russell (United Counties) v. David S. LaFlamme Construction Inc.*, 2016 ONSC 1059 (CanLII); *Alberta v. Suncor Energy Inc.*, 2017 ABCA 221 (CanLII); *Susan Hosiery Ltd. v. Canada (Minister of National Revenue – M.N.R.)*, [1969] 2 Ex. C.R. 27; *Pearson v. Inco Limited*, 2008 CanLII 46701 (ON SC); *Ontario (Provincial Police) v. Assessment Direct Inc.*, 2017 ONSC 5686, [2017] O.J. No. 4996 (Q.L.); *Canada (Office of the Information Commissioner) v. Canada (Prime Minister)*, 2019 FCA 95 (CanLII); *Canada (Public Safety and Emergency Preparedness) v. Canada (Information Commissioner)*, 2013 FCA 104 (CanLII)

INTRODUCTION:

[1] This decision addresses a claim of legal privilege by LIFE LABS LP ("LifeLabs") over a number of documents demanded by the Office of the Information and Privacy Commissioner of Ontario ("IPC") in its investigation into a cyberattack on LifeLabs' computer systems.

[2] Based on the reasons set out below, I have decided to issue an interim Order requiring that the documents at issue be produced to the IPC. In summary, I find that LifeLabs has failed to provide sufficient evidence to support their claims of legal privilege.

BACKGROUND:

[3] In November 2019, LifeLabs notified the IPC that it was the subject of a cyberattack (the "breach"). LifeLabs told the IPC that cyberattackers had penetrated LifeLabs' computer systems, extracted data, and demanded a ransom. It informed the IPC that the affected systems contained the personal health information of approximately 15 million LifeLabs customers in Canada, including names, addresses, emails, customer logins and passwords, health card numbers, and laboratory test results.[1] With respect to laboratory test results, LifeLabs informed the IPC that the breach involved approximately 85,000 customers in Ontario from 2016 or earlier.

[4] The IPC commenced an investigation into the breach, in co-ordination with the Office of the Information and Privacy Commissioner for British Columbia ("OIPC"[2]). Among other information initially provided to both the IPC and OIPC, LifeLabs indicated that it had retained a third party cybersecurity firm, CrowdStrike, to help LifeLabs respond to the breach. LifeLabs also informed both the IPC and OIPC that when the cyberattackers first contacted LifeLabs demanding a ransom, it engaged another firm, Cytelligence, to communicate with the cyberattackers on its behalf.

[5] On December 23, 2019, a letter was issued jointly by the IPC and OIPC asking LifeLabs to answer a number of questions regarding the circumstances of the breach and ordering LifeLabs to provide a number of documents to the IPC and OIPC. LifeLabs responded on January 15, 2020, providing some but not all of the documents. On January 21, 2020, the OIPC issued a follow-up letter to LifeLabs clarifying that LifeLabs had been ordered by the OIPC to produce the documents pursuant to section 38(1)(b) of the OIPC's enabling statute, the *Personal Information Protection Act*[3] ("*PIPA*").

[6] In response, on January 28, 2020, LifeLabs asserted solicitor-client or litigation privilege over a number of the documents that the OIPC had ordered it to produce and

---

[1] The IPC has since been informed that the affected information also contains dates of birth, gender, telephone numbers and password security questions

[2] OIPC File No. P19-8097

[3] S.B.C. 2003, c. 63

declined to waive the privilege. In particular, the documents over which LifeLabs asserted solicitor-client and/or litigation privilege were: a penetration test conducted by CrowdStrike after the breach occurred (the "Penetration Test"); the communications between the attacker and Cytelligence (the "Cytelligence Communications"); and "other requested communications, reports, summaries, analyses and briefing materials related to the [breach]."

[7] On February 7, 2020, the IPC issued a Notice of Review notifying LifeLabs that a review had been commenced under the *Personal Health Information Protection Act, 2004*[4] ("*PHIPA*"). The IPC also issued a Demand for Production, under section 60(2)(a) of *PHIPA*, for the incident response report generated by CrowdStrike for LifeLabs (the "CrowdStrike Report"). The demand further required that LifeLabs produce all correspondence and communication between LifeLabs, or any third party acting for LifeLabs, and the cyberattackers (i.e., the Cytelligence Communications).

[8] In response to this demand, LifeLabs asserted solicitor-client or litigation privilege over these documents and declined to waive the privilege.[5]

[9] On February 7, 2020, the IPC and OIPC also informed LifeLabs that, as part of their co-ordinated investigation of the breach, they intended to summons representatives of LifeLabs to give evidence on a number of identified topics. In response to a request from the IPC and OIPC, LifeLabs' counsel identified four LifeLabs representatives that were "best placed to respond" to questions regarding those topics.[6]

[10] As LifeLabs continued to assert legal privilege over certain documents, the IPC asked LifeLabs to confirm that the individuals summonsed would be able to answer questions regarding the basis of the privilege claims, or to identify additional individual(s) who would be able to do so.[7] In response, counsel for LifeLabs wrote to the IPC and confirmed the addition of LifeLabs' Interim General Counsel to the list of witnesses.[8]

[11] On February 18, 2020, the IPC issued a further Demand for Production for various documents, including all "documents, reports, draft reports, alerts, findings, emails and communications" with CrowdStrike in the months prior to and following the breach. LifeLabs produced some documents that pre-dated the breach, but continued to assert privilege over the remainder of the documents, including the CrowdStrike Report, and declined to waive the privilege.[9]

---

[4] S.O. 2004, c. 3, Sched. A
[5] Letter from LifeLabs' counsel to the IPC and OIPC, dated February 11, 2020
[6] Letter from LifeLabs' counsel to the IPC and OIPC, dated February 11, 2020
[7] Letter from the IPC and OIPC to LifeLabs' counsel, dated February 13, 2020
[8] Letter from LifeLabs' counsel to the IPC and OIPC, dated February 14, 2020
[9] Letter from LifeLabs' counsel to the IPC and OIPC, dated February 21, 2020

[12] In a telephone conversation with counsel for LifeLabs on February 19, 2020, the IPC requested an itemized list of documents responsive to the previous demands/orders of the IPC and OIPC over which LifeLabs is claiming privilege. Counsel for LifeLabs agreed to provide this itemized list.[10]

[13] In an email dated February 24, 2020, the IPC reiterated its request that LifeLabs produce an itemized list of documents over which it claims privilege, containing sufficient specificity to establish what documents exist and the basis for each claim (the "itemized list").[11] LifeLabs did not provide the itemized list, but only a broad statement that its external counsel engaged the following third parties to assist in counsel's efforts to defend LifeLabs in ongoing litigation: CrowdStrike, Cytelligence, Deloitte and KPMG. Counsel, on behalf of LifeLabs, claims litigation privilege and/or solicitor-client privilege over all reports and related correspondence between counsel and these third parties[12] (the "third party documents").

[14] On February 26, 2020, the representatives of LifeLabs attended under summons to give evidence at the offices of the IPC.[13] At this time, IPC counsel noted that LifeLabs had still not provided the itemized list. Counsel for LifeLabs indicated that LifeLabs would provide the itemized list to the IPC.[14]

[15] Counsel for LifeLabs continued to refuse to produce any of the third party documents. Moreover, counsel for LifeLabs refused to allow the summonsed witnesses to reveal any information or facts that would be contained in the third party documents.[15] A witness advised that the CrowdStrike Report was not finalized but that a draft version had been prepared.[16]

[16] A subsequent Demand for Production was issued on February 28, 2020 by the IPC for:

> An itemized list of the documents that are responsive to any of the production demands or orders issued by the IPC and/or OIPC in the course of their co-ordinated investigation of the breach experienced by LifeLabs and over which LifeLabs has claimed solicitor-client or litigation privilege,

---

[10] Letter from the IPC to LifeLabs' counsel, dated February 28, 2020, referencing the telephone call on February 19, 2020 between LifeLabs' counsel and the IPC

[11] Email from the IPC to LifeLabs' counsel, dated February 24, 2020

[12] Email from LifeLabs' counsel to the IPC, dated February 25, 2020

[13] Some of the witnesses summonsed were not questioned due to a lack of time. Those witnesses were, however, identified by counsel for LifeLabs to speak to questions related to LifeLabs' call centre and the notification strategy undertaken by LifeLabs to notify individuals whose personal health information was subject or potentially subject to the breach

[14] Transcript of IPC/OIPC interviews, February 26, 2020, p. 6, line 22 to p. 8, line 2

[15] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' Chief Information Security Officer ("CISO"), Q. 37, pp. 23-25

[16] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 575, p. 230

containing sufficient specificity to establish what documents exist, and the basis for each claim.

[17] The deadline for this Demand for Production was March 6, 2020. Counsel for LifeLabs responded on March 6, 2020.[17] He did not provide the itemized list, but instead made a number of objections to providing it.

[18] The IPC responded[18] by reiterating that LifeLabs was required to produce the itemized list in order for the IPC to be satisfied that the claims of privilege were properly made. The IPC demanded the itemized list be produced forthwith, but in any event no later than 12:00 p.m. on March 11, 2020.

[19] On March 11, 2020 at 7:39 p.m., LifeLabs' counsel responded that he was "in ongoing discussions with [LifeLabs] regarding [the IPC's] request to provide" the itemized list and that he would provide a "further response" by Monday March 16, 2020.[19]

[20] On March 12, 2020, the IPC responded, directing LifeLabs' counsel to confirm by 5:00 p.m. that day whether or not it would be providing the itemized list by 12:00p.m. on Monday March 16, 2020.[20]

[21] At 9:35 p.m. that evening, LifeLabs' counsel responded by email that he was "currently in the process of preparing a proposal in relation to the potential disclosure of certain privileged documents" and that this must be brought to the attention of LifeLabs' executive and board of directors before providing a response.[21] LifeLabs' counsel further stated that "we intend to revert back to you, if possible, before end of day tomorrow with our response as to the materials or the proposal that we intend to present to you on Monday".

[22] On March 13, 2020, counsel for LifeLabs requested a telephone conversation with the IPC which took place later that afternoon. During this telephone conversation, LifeLabs' counsel advised that a meeting of a "special committee" of LifeLabs' board of directors had been convened for Tuesday March 17, 2020 at which time proposals regarding LifeLabs' response to the demands for production would be considered.

[23] Following this telephone conversation, the IPC sent an email to LifeLabs counsel, asking LifeLabs' counsel to confirm, in writing, the IPC's understanding from this telephone call that LifeLabs would not be providing the itemized list by 12:00 p.m. on Monday March 16, 2020.[22]

---

[17] Letter form LifeLabs' counsel to the IPC, dated March 6, 2020
[18] Letter from the IPC to LifeLabs' counsel, dated March 9, 2020
[19] Letter from LifeLabs' counsel to the IPC, dated March 11, 2020
[20] Letter from the IPC to LifeLabs' counsel, dated March 12, 2020
[21] Email from LifeLabs' counsel to the IPC, dated March 12, 2020, at 9:34 pm
[22] Email from the IPC to LifeLabs' counsel, dated March 13, 2020, at 1:42 pm

[24] Later that afternoon, LifeLabs' counsel responded to this email confirming that LifeLabs would not provide "a response" to the IPC by Monday March 16 at 12:00 p.m. as it needed to obtain approvals from LifeLabs executives and the special committee of the board of directors. [23] Further, LifeLabs' counsel suggested that LifeLabs would not be providing the itemized list, but only categories of their documents. [24]

[25] Just before noon on Monday, March 16, 2020, LifeLabs' counsel emailed the IPC an attachment that was identified as the "itemized list" ("the attachment").[25]

[26] The attachment noted that following the breach, LifeLabs engaged counsel for legal advice and to defend the class actions filed against it. It further mentioned LifeLabs' retainers with the third parties noted above, namely, Cytelligence, CrowdStrike, Deloitte and KPMG. The attachment also named two additional third parties over whose documents LifeLabs was asserting privilege: Optiv[26] and Kroll[27]. Documents related to Optiv will be included in the defined term of "third party documents" used in this Order.

[27] Instead of providing a list of actual individual documents that exist, or bundles of like documents, the attachment only recites, using boiler-plate language, broad categories of documents that could exist for each retainer and asserts that all of these documents are subject to both solicitor-client and litigation privilege.

[28] The attachment also asserts litigation privilege for all its "internal analyses performed or created for the dominant purpose of preparing for litigation in relation to the incident…"[28] ("internal analyses"). Although no details were provided in the attachment about the internal analyses, through oral evidence of its Chief Information Security Officer ("CISO") given under oath, LifeLabs stated that, after becoming aware of the breach, its security staff took various actions in response to the breach and that these actions would be documented in change management control logs ("change management control logs").[29] In addition, the CISO testified that there exist data analyses performed internally by various LifeLabs' IT business units to determine the

---

[23] Email from LifeLabs' counsel to the IPC, dated March 13, 2020 at 5:16 pm

[24] In an email in reply, sent March 16, 2020, the IPC noted that with respect to emails only, the IPC did not expect LifeLabs to itemize each one and emails could be set out in categories. The IPC reiterated that rest of the itemized list must be set out with sufficient specificity to establish what documents exist and the basis for each of LifeLabs' claims of privilege.

[25] Email from LifeLabs' counsel to the IPC, dated March 16, 2020 at 11:57 am

[26] Privilege has not been asserted over any Optiv documents prepared prior to or outside of the Optiv retainer made after the breach

[27] LifeLabs' attachment, sent to the IPC on March 16, 2020, states that it has "already elected to produce" to the IPC and OIPC the documents related to LifeLabs' retainer with Kroll. This Interim Order therefore does not address these documents

[28] LifeLabs' attachment, sent to the IPC on March 16, 2020

[29] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 519-522, pp. 213-214

extent of the data compromised in the breach ("data analyses").[30] It appears that the internal analyses category would include the change management control logs and data analyses.

[29] On March 17, 2020, LifeLabs' counsel had a telephone conversation with the IPC and the OIPC where he indicated that he would be sending a written proposal for the release of some of the documents.[31]

[30] On March 19, 2020, LifeLabs' counsel sent this written proposal, but did not provide any further details about the documents over which privilege is claimed.[32] In response, the IPC sent a letter indicating that the proposal was not acceptable, noting that LifeLabs had still not provided the itemized list, and attaching this Order.[33]

[31] For the following reasons, I order LifeLabs to produce the third party documents and internal analyses.

[32] For greater certainty, the third party documents and internal analyses include, but are not limited to, the following:

a. The CrowdStrike Report

b. Any draft versions of the CrowdStrike Report that exist

c. The Cytelligence Communications

d. The Penetration Test

e. Change management control logs

f. Data analyses

ANALYSIS AND FINDING

[33] In its responses to the IPC and OIPC dated January 28, 2020 and February 11, 2020, LifeLabs argued that if it produced the third party documents, it would risk losing the privilege attached to them. LifeLabs cited cases[34] that support the principle that privilege cannot be overcome absent explicit language in the statute that gives a regulator

[30] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 50, pp. 29-31, 35
[31] Telephone call between LifeLabs' counsel, the IPC and the OIPC, March 17, 2020
[32] Letter from LifeLabs' counsel to the IPC and OIPC, dated March 19, 2020
[33] Letter from the IPC to LifeLabs' counsel, dated March 30, 2020
[34] *Blank v. Canada (Minister of Justice)*, 2006 SCC 39 ("*Blank*"); *Thomson v. Berkshire Investment Group Inc. et al.*, 2007 BCSC 50; *Lizotte v. Aviva*, 92016] 2 SCR 521; *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44, *Huang v. Silvercorp Metals Inc.*, 2017 BCSC 795

its investigative powers. LifeLabs argues that neither the IPC nor the OIPC has the power to compel documents subject to legal privilege.

[34] I will not be commenting on the interpretation of the OIPC's powers under *PIPA*. With respect to the IPC's powers under *PHIPA*, I do not need to address the question of whether *PHIPA* gives me the authority to compel the production of documents over which privilege is properly claimed. Rather, the issue before me is whether sufficient evidence has been provided in this case to support LifeLabs' claims of privilege.

[35] LifeLabs takes the position that all of the third party documents are subject to litigation privilege and/or solicitor-client privilege, and that the internal analyses are subject to litigation privilege. I will deal with each type of privilege in turn.

Litigation Privilege

[36] Litigation privilege is intended to create a "zone of privacy"[35] within which counsel can prepare draft questions, arguments, strategies or legal theories. In order to fall within this class of privilege, documents must be prepared or gathered by counsel (or someone under counsel's direction), this preparation or gathering must be done in anticipation of litigation, and the dominant purpose of the creation of the documents must be for preparing for that litigation.

[37] There is no dispute that LifeLabs is currently subject to multiple class actions in Ontario and British Columbia related to the breach. LifeLabs must also demonstrate, however, that the documents at issue were created for the dominant purpose of that litigation. LifeLabs has failed to provide sufficient evidence to satisfy me that this was the case.

Dominant Purpose

[38] In order to establish that the dominant purpose for the creation of a document was for litigation preparation, the person asserting the privilege must provide more than a bare assertion of privilege.[36] The asserting party must provide cogent evidence in support of its claim. Inadequate evidence or a sufficient deficiency in the evidence will amount to a ground on which the privilege claim may be rejected.[37]

[39] The test of dominant purpose is a higher standard than that of a substantial purpose. It recognizes "the trend toward mutual and reciprocal disclosure which is the hallmark of the judicial process."[38]

---

[35] *General Accident Assurance Company v. Chrusz*, 45 O.R. (3d) 321; 1999 CanLII 7320 (ON CA) ("*Chrusz*")
[36] *Shen v. Canada (Minister of Citizenship and Immigration)* 2017 FC 115 (CanLII)
[37] *Fresco v. Canadian Imperial Bank of Commerce*, 2019 ONSC 3309 (CanLII)
[38] *Blank, supra*

[40] Here, LifeLabs bears the onus of providing evidence to the IPC that would demonstrate that the dominant purpose for the creation of each of the documents (or each bundle of like documents) was for the litigation.[39] If there are other possible purposes, those must be addressed by the party asserting the privilege.[40]

[41] During her evidence under summons, LifeLabs' Interim General Counsel, who was put forward by LifeLabs to speak to LifeLabs' claims of privilege, provided little to no evidence to support the claims of privilege.[41] Interim General Counsel has only been in this role since December 2019, i.e. after the breach occurred. She stated that she prepared herself to provide evidence under summons by reviewing documents, including her predecessor's email, correspondence and dockets. Nonetheless, counsel for LifeLabs refused to allow Interim General Counsel to answer any questions regarding what she knew or understood about the time period before her engagement at LifeLabs, or why or when CrowdStrike was engaged by LifeLabs. When asked about the purpose of the CrowdStrike Report, Interim General Counsel stated briefly that its purpose was to produce a forensic analysis and that she did not have the technical expertise to comment any further.[42] Notwithstanding her role of Interim General Counsel, when asked about whether CrowdStrike's work helped LifeLabs meet its obligations under *PHIPA* or *PIPA* to take reasonable steps to safeguard personal health information and personal information, she stated that she had no view on this.[43]

[42] A dominant purpose of litigation has not been found where there were other purposes for the creation of a document, including in situations where:

- a report prepared after a train accident was found to also have a purpose of helping to establish the cause of the accident[44]
- preparing the incident reports, photographs and witness statements was the usual practice or policy as the party expected litigation after each incident[45]
- the solicitor retained an investigator to look into a vehicle accident but the purpose of the investigator's reports was also to address Workers' Compensation Board claims[46]

---

[39] *Shaughnessy Golf & Country Club v. Drake International Inc.*, 1986 CanLII 163 (BC CA)
[40] *Hosanna Enterprises Ltd. (Seraphim Christian Books 7 Supplies) v. Laser City Audio Video Ltd.*, 1999 CanLII 5836 (BC SC)
[41] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' Interim General Counsel ("GC"), Qs. 586-644, pp. 238-255
[42] Transcript of IPC/OIPC interviews, February 26, 2020, Witness –GC, Qs. 636 and 643, pp. 250 and 254
[43] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – GC, Q. 617, p. 245
[44] *Waugh v. British Railway Board*, [1979] 2 All E.R. 1169
[45] *Fred v. Westfair Foods Ltd. et al.*, 2003 YKSC 39 (CanLII)
[46] *Whitehead v. Braidnor Construction Ltd.*, 2001 ABQB 994 (CanLII)

- spreadsheets over which privilege was claimed were also required for the operations of the party's business[47]

- documents related to a failure to test a newborn for a disorder were found to be created primarily for the purposes of the investigation into the alleged error and the need for corrective action if the error was confirmed[48]

- a risk management report was prepared as part of a risk management policy used to review all construction projects where there was a risk of litigation[49]

- an investigation was also done to comply with statutory obligations[50]

[43] In this case, LifeLabs has not provided sufficient information to counter the inference that the third party documents were necessarily also created in response to the operational needs of the company as it dealt with the breach. In other words, even absent litigation, LifeLabs would have engaged third parties in order to contain, investigate, and remediate the breach. Similarly, LifeLabs would have had to communicate with the cyberattackers, regardless of whether there was any litigation.

[44] This is consistent with the answers given by the CISO for LifeLabs during his evidence under summons. For example, he gave evidence that LifeLabs had engaged CrowdStrike several months prior to the breach to provide it with a number of services.[51] As set out in the initial retainer agreement, CrowdStrike was to provide incident response services to LifeLabs should it experience a breach. These incident response services included helping LifeLabs' information security staff to take immediate steps to respond to a breach, to contain, investigate and remediate a breach, and to provide LifeLabs with strategic recommendations going forward.[52]

[45] As part of its services for LifeLabs, CrowdStrike performed an assessment of LifeLabs' computer systems to see if any of them had been compromised. It was, in fact, CrowdStrike who had discovered the cyberattack while performing this assessment.[53]

[46] Immediately following the breach, LifeLabs, pursuant to the incident response services detailed in their initial retainer, instructed CrowdStrike to take several steps to

---

[47] *Dow Chemical Canada ULC. v. Nova Chemicals Corporation*, 2014 ABCA 244 (CanLII)
[48] *Borkowski (Litigation guardian of) v. Ontario (Minister of Health)*, 2007 CanLII 18017 (ON SC)
[49] *Prescott and Russell (United Counties) v. David S. LaFlamme Construction Inc.*, 2016 ONSC 1059 (CanLII)
[50] *Alberta v. Suncor Energy Inc.*, 2017 ABCA 221 (CanLII)
[51] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 335-341, pp. 145-150
[52] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 380-393, pp. 166-172
[53] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 39, p. 174

assist LifeLabs in responding to the breach.[54] The CISO testified that a second retainer was signed with CrowdStrike after the breach occurred and that the products and services in the second retainer were essentially the same as those in the initial retainer. He further testified that the reason for the new retainer was because the funds, paid at the beginning of the initial retainer, had run out.[55]

[47] After the breach, LifeLabs also engaged CrowdStrike, in a separate retainer, to perform the Penetration Test on its systems to ensure that they were secure.[56] The CISO testified that LifeLabs was going to make a public announcement about the breach and LifeLabs knew that when information about the breach was made public, other cyberattackers would try to attack its systems. The Penetration Test was performed in order to ensure that LifeLabs' systems were protected and secure before the announcement was made.[57] This evidence suggests that the Penetration Test was done for the purposes of operational needs, and not only for litigation purposes.

[48] The CISO also testified that LifeLabs needed CrowdStrike to respond to the breach, including by providing the services described above, as LifeLabs could not have, on its own, accomplished these tasks as quickly as was required.[58] This assessment of its operational needs was made by LifeLabs' when CrowdStrike was first retained, i.e. prior to the breach.[59] Given the very sensitive nature of the personal health information, and the reported estimate of millions of individuals affected, it is understandable that LifeLabs wanted, as part of its business operations, to address the breach as quickly as possible. The fact that LifeLabs required CrowdStrike's services for a timely and effective response to the breach does not alter the fact that LifeLabs was driven by its operational needs to respond, regardless of the existence of any litigation.

[49] With respect to the Cytelligence Communications, the CISO testified that Cytelligence had been retained to communicate with the cyberattackers on LifeLabs' behalf after LifeLabs received the ransom request from the cyberattackers.[60]

[50] The CISO testified that, in the course of communicating with the cyberattackers, data that the cyberattackers stated had been extracted from LifeLabs' systems was returned to LifeLabs.[61] The cyberattackers also provided LifeLabs with information about

---

[54] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 403-412, 531, pp. 174-182, 217
[55] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 493-496, pp. 207-208
[56] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 531, p. 217
[57] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 534-541, pp. 217-219
[58] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 563, pp. 226-227
[59] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 571, p. 229
[60] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 582, p. 232
[61] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Q. 56, p. 31

how they had compromised LifeLabs' systems.[62] Therefore, it is clear that even absent the prospect of litigation, LifeLabs would have needed to communicate with the cyberattackers. Like with CrowdStrike, the fact that Cytelligence was retained to perform these communications with the cyberattackers on behalf LifeLabs does not change the fact that LifeLabs had an operational need to engage in these communications. In fact, the attachment provided by counsel for LifeLabs to the IPC on March 16, 2020, confirms that LifeLabs does not assert privilege over direct communications that it had with the cyberattackers. Solely by hiring Cytelligence to take over these communications does not, absent more information, make the communications privileged.

[51] Information about the scope or nature of LifeLabs' retainers with Optiv, Deloitte and KPMG were not provided by LifeLabs and in absence of any specificity regarding the documents related to these third parties, I am unable to find that the dominant purpose of these documents was for litigation.

[52] Furthermore, LifeLabs is subject to statutory requirements in jurisdictions throughout Canada regarding the security and safeguarding of personal information and personal health information in its custody or control. In particular, and as noted in the IPC's Notice of Review, as a health information custodian, LifeLabs is required to comply with *PHIPA*, including sections 12(1) and 13(1) which state:

> 12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.
>
> […]
>
> 13 (1) A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.

[53] In order to comply with these and other statutory obligations in jurisdictions throughout Canada, and to respond to the investigations or other proceedings initiated by the corresponding regulators, LifeLabs would have been required to identify, contain, investigate and remediate the breach. In the absence of any evidence, I am not satisfied that the retainer of the third parties or the creation of the third party documents in this case was for the dominant purpose of litigation because LifeLabs was required to comply with its statutory obligations regardless of whether it engaged third parties to assist it in doing so.

---

[62] Transcript of IPC/OIPC interviews, February 26, 2020, Witness – LifeLabs' CISO, Qs. 57-65, pp. 31-34

[54] For example, and as noted above, when LifeLabs' Interim General Counsel—the witness identified by LifeLabs to speak to the issue of privilege—was asked about the purpose of the CrowdStrike Report, she only stated that it was a forensic report and that she did not understand its technical nature. The Interim General Counsel also testified that she had no view with respect to LifeLabs' statutory obligations under *PHIPA* or *PIPA*.

[55] Based on the foregoing, I am not satisfied that LifeLabs has adduced sufficient evidence to establish that the creation of the third party documents was for the dominant purpose of assisting with litigation.

[56] LifeLabs also asserts litigation privilege over all of its internal analyses performed or produced in relation to the breach. As with the third party documents, given the lack of any specificity about what internal analyses exist or any evidence that these documents were created for the dominant purpose of litigation, I am not satisfied that LifeLabs has discharged its onus to establish litigation privilege over the internal analyses.

Underlying Facts

[57] Even if LifeLabs had satisfied me that the documents were subject to privilege, I am not convinced by their counsel's position that the underlying facts are also subject to privilege.

[58] Facts that are otherwise not privileged do not become so merely by their inclusion in documents produced at the instructions of counsel.[63] The purpose of litigation privilege is to protect parties' preparation in adversarial proceedings, including legal theories and strategies, also known as the lawyer's work product. The privilege is not intended to shield from disclosure relevant facts that do not, on their own, constitute a lawyer's work product.[64]

[59] For example, the facts contained in the CrowdStrike Report would address the key questions of the cause of the breach, the scope of the breach, how the scope was determined, and what was done by CrowdStrike to contain and then remediate the breach. On its face, there is no indication that disclosure of these facts would undermine the legal strategy of LifeLabs' defence. LifeLabs has not proffered any evidence that would demonstrate why the disclosure of these facts would affect litigation privilege. No evidence has been given to show that the facts of what happened in the breach and how the breach was remediated would necessarily include or reveal counsel's theories and strategies of their legal defence.

---

[63] *Susan Hosiery Ltd. v. Canada (Minister of National Revenue – M.N.R.)*, [1969] 2 Ex. C.R. 27; *Pearson v. Inco Limited*, 2008 CanLII 46701 (ON SC); *Chrusz*, *supra*

[64] *Ontario (Provincial Police) v. Assessment Direct Inc.*, 2017 ONSC 5686, [2017] O.J. No. 4996 (Q.L.)

[60] With respect to the Penetration Test performed by CrowdStrike, it is also difficult to see, without any evidence or specifics from LifeLabs, how the facts underlying the Penetration Test and its results would be subject to litigation privilege.

[61] Similarly, the facts contained in the Cytelligence Communications would include what the hacker told Cytelligence about the data breach, their demands, whether the demands were met and how. It is unclear how disclosure of these facts would undermine or interfere with the lawyer's work product in the litigation.

[62] It is likewise unclear how the underlying facts in LifeLabs' internal analyses, including facts contained in their change management control logs or data analyses, would attract litigation privilege.

[63] With respect to the documents related to the retainers of Optiv, Deloitte and KPMG, as noted above, I was not given any information about the nature of those retainers and to what extent information contained in these documents would be responsive to the issues raised in the IPC and OIPC's joint investigation. Without further specification, I am not satisfied that the facts underlying the work or communications related to these retainers would be subject to litigation privilege.

Solicitor-Client Privilege

[64] LifeLabs has not provided adequate evidence to support its claim that the third party documents attract solicitor-client privilege. LifeLabs has only indicated that its external counsel has retained the third parties. As with litigation privilege, the party asserting the privilege bears the onus of establishing the basis for the privilege and a bare assertion will not be sufficient.[65]

[65] It is well-settled that the mere fact of communication between a lawyer and their client does not, on its own, support a claim of solicitor-client privilege.[66] Rather, the communication must be made in confidence between a lawyer and their client (or third party acting on behalf of their client), the communication must be made for the purpose of seeking/giving legal advice, and the parties must have intended the communication to be confidential.[67]

[66] Neither in its written submissions to the IPC nor in the evidence of its witnesses, has LifeLabs provided evidence that all of the communications between external counsel and the third parties meet the test for solicitor-client privilege. For example, the attachment provided by counsel for LifeLabs to the IPC on March 16, 2020, asserts solicitor-client privilege over all internal communications about the reports, summaries,

---

[65] *Canada (Office of the Information Commissioner) v. Canada (Prime Minister)*, 2019 FCA 95 (CanLII) ("*Canada (Office of the Information Commissioner*")
[66] *Chrusz, supra*
[67] *Canada (Office of the Information Commissioner), supra*

analyses or conclusions made by the third parties. It is not at all clear that all of these internal communications are made to/from either in-house or external counsel, much less satisfy the test for solicitor-client privilege.

[67] With respect to reports produced by any of the third parties, if these are stand-alone records under the control of LifeLabs, they must be examined as independent records and do not become privileged merely by the fact that they are given to LifeLabs' in-house or external counsel.[68]

[68] I would also note that while underlying facts given to counsel could be part of the "continuum of communication" protected by solicitor-client privilege, that is only to the extent that the disclosure of these facts would undermine the purpose of the privilege. In other words, unless disclosure of the underlying facts would reveal or allow for inference of confidential solicitor-client communications, the underlying facts themselves do not attract the privilege.[69] LifeLabs has not provided me with evidence to demonstrate that any of the underlying facts in this case would include or reveal confidential solicitor-client communications.

Conclusion

[69] I find that the documents that are responsive to the IPC's investigation must be produced by LifeLabs, absent a valid claim of privilege. Despite being given multiple opportunities in the IPC proceeding to do so, LifeLabs has failed to adduce sufficient evidence to satisfy me that privilege attaches to the third party documents or the internal analyses.

[70] It may be that some of the documents at issue are subject to privilege, but LifeLabs is required to provide more than an overly broad assertion of privilege over all documents at issue. Without more details on what documents exist and their nature, I cannot be satisfied as to whether any of the documents are, in fact, privileged. In order for the IPC to carry out its important mandate to investigate breaches such as this one, we require all relevant information.

[71] Section 61(1)(c) of *PHIPA* provides that:

> After conducting a review under section 57 or 58, the Commissioner may,
>
> …
>
> (c) make an order directing any person whose activities the Commissioner reviewed to perform a duty imposed by this Act or its regulations;

---

[68] *Canada (Office of the Information Commissioner), supra*

[69] *Canada (Public Safety and Emergency Preparedness) v. Canada (Information Commissioner)*, 2013 FCA 104 (CanLII)

…

[72] Duties imposed on LifeLabs under *PHIPA* include the duty to assist set out in section 60(8):

> If the Commissioner makes a demand for any thing under subsection (2), the person having custody of the thing shall produce it to the Commissioner and, at the request of the Commissioner, shall provide whatever assistance is reasonably necessary, including using any data storage, processing or retrieval device or system to produce a record in readable form, if the demand is for a document.

[73] Section 60(2) provides that:

> In conducting a review under section 57 or 58, the Commissioner may,
>
> (a) demand the production of any books, records or other documents relevant to the subject-matter of the review or copies of extracts from the books, records or other documents;
>
> (b) inquire into all information, records, information practices of a health information custodian and other matters that are relevant to the subject-matter of the review;
>
> (c) demand the production for inspection of anything described in clause (b);
>
> …

ORDER:

1. Pursuant to my powers under section 61(1)(c) of *PHIPA*, I order LifeLabs to perform its duty to assist the IPC with its review of the breach.

2. In particular, I order LifeLabs to deliver to IPC by **April 29, 2020**, reports or correspondence between LifeLabs or its external counsel and the following third parties retained by LifeLabs: CrowdStrike, Cytelligence, Optiv, Deloitte and KPMG. The third party documents include, but are not limited to, the following:

   a. The CrowdStrike Report

   b. Any draft versions of the CrowdStrike Report that exist

   c. The Cytelligence Communications

d. The Penetration Test

3. I further order LifeLabs to deliver to the IPC by **April 29, 2020**, its internal analyses including, but not limited to, the following:

   a. Change management control logs

   b. Data analyses

March 30, 2020

Brian Beamish
Commissioner