OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

Order F19-40

MINISTRY OF HEALTH

Celia Francis
Adjudicator

November 8, 2019

CanLII Cite: 2019 BCIPC 45
Quicklaw Cite: [2019] B.C.I.P.C.D. No. 45

Summary: An applicant requested records related to a review by Deloitte LLP (Deloitte) of the Ministry of Health's (Ministry) data security and handling. The Ministry disclosed the responsive records, withholding some information under several exceptions to disclosure under the *Freedom of Information and Protection of Privacy Act* (FIPPA). The Ministry ultimately abandoned reliance on all exceptions but s. 15(1)(l) (harm to security of a property or system). Deloitte argued that ss. 21(1) (harm to business interests of a third party) and 22(1) (unreasonable invasion of third-party personal privacy) applied to some information. The applicant argued that s. 25(1)(b) (public interest override) applied to the withheld information. The adjudicator found that s. 25(1)(b) did not apply but that s. 15(1)(l) applied to some of the information. The adjudicator also found that s. 21(1) did not apply to some of the information and ordered the Ministry to disclose it. It was not necessary to consider s. 22(1).

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 15(1)(l), 21(1)(a)(ii), 21(1)(b), 21(1)(c)(i), 21(1)(c)(ii), 21(1)(c)(iii), 25(1)(b).

INTRODUCTION

[1] This case concerns a request under the *Freedom of Information and Protection of Privacy Act* (FIPPA) for records related to a review by Deloitte LLP (Deloitte) of the Ministry of Health's (Ministry) data security and handling.[1] The Ministry disclosed the responsive records to the applicant in phases. It disclosed

[1] The request, which covered the period January 2012 to October 2013, included the "final costs paid to Deloitte, preparatory and administrative documents on how the contract was awarded and all deliverables and reports the Province had received."

the first phase in full and withheld information in the subsequent five phases under ss. 15(1)(l) (harm to a property or system), 17(1) (harm to public body's economic or financial interests), 21(1) (harm to third-party business interests) and 22(1) (harm to third-party personal privacy).

[2] The applicant requested a review by the Office of the Information and Privacy Commissioner (OIPC) of the Ministry's decision to withhold information. She also argued that s. 25(1)(b) (public interest override) applied to the records.[2] Mediation by the OIPC did not resolve the matter and it proceeded to inquiry. The OIPC received submissions from the Ministry, Deloitte and the applicant.

ISSUES

[3] The Ministry stated in its initial submission that it was no longer relying on ss. 17(1), 21(1) and 22(1) to withhold information but would rely only on s. 15(1)(l).[3]

[4] Deloitte argued that some information should be withheld under s. 21, s. 22 or both.[4] However, its submissions dealt principally with information the applicant accepts may be withheld[5] or information the Ministry has disclosed[6] and which is, therefore, not at issue. This includes all of the information that Deloitte argued falls under s. 22(1). I need not, therefore, consider Deloitte's s. 22(1) arguments. Although Deloitte did not request a review by the OIPC of the Ministry's decision not to apply s. 21(1), I have considered Deloitte's arguments that s. 21(1) applies to some of the information.[7]

---

[2] The applicant did not argue that the information was about a risk of significant harm to the environment or to the health and safety of the public or a group of people (s. 25(1)(a)). I have, therefore, considered only whether disclosure is clearly in the public interest under s. 25(1)(b).

[3] Ministry's initial submission, para. 4. While Deloitte made a submission on s. 17(1), I have not considered it, as the Ministry no longer relies on this exception.

[4] Deloitte argued that this information should be withheld: its staff's qualifications, experience, cell phone numbers and hourly rate; its banking information; its rate negotiations with the Ministry; and the description of its proposed approach, procedure and methodology for the Data Security Review.

[5] The applicant said that this information could be withheld: Deloitte's staff's hourly rates, its staff's cell phone numbers, information about its rate negotiations with the Ministry and its banking information. I include here information on Deloitte's hourly rates and its projected costs and hours of effort for implementing part of a project (on pages 107, 108, 111-113, Phase 6), as it is similar in character to the information on Deloitte's hourly rates and rate negotiation information.

[6] The Ministry disclosed this information: Deloitte's staff's qualifications and experience; some information about Deloitte's negotiations with the Ministry on its hourly rates (pages 17, 18, 20, 21, 46 and 47, Phase 2); and Deloitte's proposed approach, procedure and methodology for the Data Security Review in its statement of work.

[7] "Ministry of Health Security Dashboard" and issue log, pages 285-297, Phase 4, and small amounts of information pages 8 and 153, Phase 6.

[5] Thus, the issues before me are these:

1. Whether the Ministry is required by s. 21(1) to withhold information;
2. Whether the Ministry is authorized by s. 15(1)(l) to withhold information; and
3. Whether, under s. 25(1)(b), the Ministry is required to disclose information.

[6] Under s. 57(1) of FIPPA, the Ministry has the burden of proof regarding s. 15(1)(l). Under s. 57(3)(b), Deloitte has the burden of proof regarding s. 21(1).

[7] Section 57 is silent as to who has the burden of proof respecting s. 25(1)(b). Past orders have said that, in light of the absence of a statutory burden of proof, "As a practical matter, both parties should provide evidence and argument to support their respective positions in an inquiry where the applicability of s. 25(1) is at issue."[8] I agree.

DISCUSSION

Information in dispute

[8] The information in dispute consists primarily of the following:

- tables and information flow diagrams, which the Ministry withheld under s. 15(1)(l);[9] and
- a Ministry security dashboard and issue log[10] and portions of two other pages,[11] which Deloitte wants withheld under s. 21(1).

Section 25(1)(b) – public interest override

[9] Section 25(1)(b) reads as follows:

> 25 (1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information
> ...
> (b) the disclosure of which is, for any other reason, clearly in the public interest.

[8] See, for example, Order F07-23, 2007 CanLII 52748 (BC IPC), and Order 02-38, 2002 CanLII 42472 (BC IPC).
[9] Phase 2, pages 153-166; all information withheld in Phase 5 records; Phase 6, pages 1-38, 45, 47-54, 58-60, 70, 78, 85-89, 91, 123, 126, 134-136, 139-142, 143-144, 154, 163.
[10] Pages 285-297, Phase 4.
[11] Pages 8 and 153, Phase 6.

[10] Section 25(1)(b) overrides all of FIPPA's discretionary and mandatory exceptions to disclosure.[12] Consequently, there is a high threshold before it can properly come into play.[13] Previous orders have explained this concept as follows: "... the duty under section 25 only exists in the clearest and most serious of situations. A disclosure must be, not just arguably in the public interest, but clearly (i.e., unmistakably) in the public interest ..."[14]

[11] Former Commissioner Denham expressed the view that "clearly means something more than a "possibility" or "likelihood" that disclosure is in the public interest." She added that s. 25(1)(b) "requires disclosure where a disinterested and reasonable observer, knowing what the information is and knowing all of the circumstances, would conclude that disclosure is plainly and obviously in the public interest." The Commissioner provided a non-exhaustive list of factors public bodies should consider in determining whether s. 25(1)(b) applies to information. These factors include whether the information would: contribute to educating the public about the matter; contribute in a substantive way to the body of information already available about the matter; or contribute in a meaningful way to holding the public body accountable for its actions or decisions.[15]
The Ministry said that s. 25(1)(b) applies only in the most extraordinary circumstances. In its view, this is not such a case. Section 25(1)(b) does not apply, the Ministry continued, simply because the public is interested in contracts between Deloitte and the public or because the applicant "is personally impacted by the project."[16]

[12] The applicant argued that it was in the public interest to make public the information she requested, as Deloitte received $1.5 million for its work, "yet very little has been made public."[17] The applicant did not explain how, in her view, disclosure of the information at issue is clearly in the public interest.

[13] I acknowledge the applicant's point that the public should know about the work Deloitte did for the Ministry. However, the Ministry disclosed much of the information in the 1,200 pages of responsive records, including the statement of work, contracts, modification agreements, reports, presentations and invoices. These records provide a detailed picture of the work Deloitte did for the Ministry and what it was paid. Disclosure of the withheld information would not, in my view, add significantly to the information already available on Deloitte's

---

[12] Section 25(2).
[13] See Investigation Report F15-02, 2015 BCIPC 30 (CanLII), pp. 28-29.
[14] Order 02-38, 2002 CanLII 42472 (BC IPC) at para. 45, italics in original.
[15] Investigation Report F16-02, 2016 BCIPC 36 (CanLII), pp. 26-27.
[16] Ministry's initial submission, paras. 73-74.
[17] Applicant's request for review. The applicant's second response submission argued that the names, qualifications and experience of Deloitte's staff should be disclosed in the public interest. As I noted above, however, the Ministry has disclosed this information and it is therefore not at issue here.

contractual arrangements with the Ministry (the topic of the request) or contribute to educating the public on this matter.

[14] The applicant also said that the Ministry "has never provided public justification for the firings."[18] She did not explain what she meant by "firings." However, the withheld information does not relate to any such events.

[15] I do not consider that this is a case in which the public interest outweighs and overrides all the exceptions to disclosure under FIPPA. It is not, in my view, clearly in the public interest for the withheld information to be disclosed. For these reasons, I find that s. 25(1)(b) does not apply to it.

Standard of proof for harms-based exceptions

[16] Numerous orders have set out the standard of proof for showing a reasonable expectation of harm.[19] The Supreme Court of Canada confirmed the applicable standard of proof for harms-based exceptions:

> This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground: paras. 197 and 199. This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations or consequences".[20]

[17] Moreover, in *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner)*,[21] Bracken J. confirmed that it is the release of the information itself that must give rise to a reasonable expectation of harm.

[18] I have taken these approaches in considering the arguments on harm under s. 15(1)(l) and s. 21(1)(c).

---

[18] Applicant's request for review.
[19] For example, Order 01-36, 2001 CanLII 21590 (BC IPC), at paras. 38-39.
[20] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)* [*Community Safety*], 2014 SCC 31, citing *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3, at para. 94. See also Order F13-22, 2014 BCIPC 31 (CanLII), at para. 13, and Order F14-58, 2014 BCIPC 62 (CanLII), at para. 40, on this point.
[21] *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875, at para. 43.

Harm to security of property or system – s. 15(1)(l)

[19] Section 15(1)(l) reads as follows:

> **Disclosure harmful to law enforcement**
>
> **15** (1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
> …
> (l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[20] The Ministry said that the information in question qualifies as information "system documentation."[22] The applicant did not discuss this issue.

[21] The information that the Ministry withheld under s. 15(1)(l) relates to the structure of the government's information network, including its composition, security and information flows. I find that this network is a "system" for the purposes of s.15(1)(l). The remaining issue is whether disclosure of the information in dispute could reasonably be expected to harm the security of this system.

[22] The Ministry said that disclosure of the information in question would increase the risk of compromise to the system.[23] The Ministry said that "it is a fundamental and widely-accepted principle of system security that the less system information an attacker has about a system, the harder it will be for him or her to attack or otherwise compromise the security of a system."[24] The Ministry supported its s. 15(1)(l) arguments with affidavit evidence from two government employees.[25] The applicant did not address the Ministry's harm arguments but said she would leave it to the OIPC to determine whether the exception applies.[26]

[23] I have reviewed the records and find that the information that the Ministry withheld under s. 15(1)(l) consists of the following types of information:

- diagrams, for example: networks of databases, data warehouses, applications, connections and authentication services, including their uses, and information flows; status of the current data environment;

---

[22] Such as technical architecture, business relationships, data flows, network protocols, security controls or access permission requirements.
[23] Ministry's initial submission, paras. 19, 21.
[24] Ministry's initial submission, para. 16.
[25] Affidavit of the Senior Manager IM/IT, Ministry of Health, and Affidavit of the Technology Director, Cybersecurity Intelligence and Investigations, Information Security Branch, Office of the Chief Information Officer, Ministry of Technology, Innovation and Citizens' Services.
[26] Applicant's response submission of June 13, 2017.

concepts for future architecture; network process flows for databases; the Ministry's security model and associated information; access management concepts;
- tables, for example: project updates; functions and task types; data sets, including their users, roles of staff and staff responsible for the data sets; inventories of databases and applications, with names of responsible staff; Ministry systems; effectiveness of the Ministry's information security program; sample tables of staff with access to data; risks and benefits of options for access management; threats to the system;
- schedule of access review and monitoring activities;
- various processes, for example: requesting and granting access to data; the secure transfer of data; data entry; internal data preparation;
- access management functions and issues;
- some acronyms
- names of systems, servers and hard drives; and
- observations, issues and risks concerning certain aspects of the system, together with recommendations and considerations for how to deal with them.

[24] The Ministry withheld a term and, in several places, its acronym in the pages 1-39 of the Phase 6 records. The Ministry did not address this information specifically. However, it disclosed the same information in the Phase 4 records. It is not clear why its re-disclosure in the Phase 6 records would cause the harm the Ministry fears and the Ministry did not explain. It is also not obvious from the face of the records how disclosure of this information could reasonably be expected to harm a system. I find that s. 15(1)(l) does not apply to this information.

[25] Regarding the remaining information at issue, however, I can readily see that its disclosure would give a hacker a picture of the complexity and inter-connected nature of the system's databases, data flows, systems and data warehouses, together with vulnerabilities and other potential issues. The Ministry acknowledged that there are several layers of security controls in place to combat attempts to compromise the system but said that websites and services, such as emails, are vulnerable to exploitation.[27] The Ministry also said, and I accept, that government systems are subject to "active compromise campaigns", including "targeted emails phishing campaigns," by those aiming to "capture authorized user credentials" which they then use to gain access to systems and extract information.

[26] The Ministry added, and I accept, that the Province of BC is "assaulted with millions of attempts to compromise" its information systems and that there

[27] Ministry's initial submission, paras. 22-23.

are several email phishing attempts every week.[28] The Ministry described other methods a hacker could use to gain access to its systems, such as by exploiting system flaws and vulnerabilities, bypassing firewalls and using previously compromised government computers.[29]

[27] I accept that a hacker could use the information, in conjunction with social engineering techniques[30] and publicly available information (such as government employees' names and email addresses), to gain access to various components of the systems, which host large volumes of personal information, such as medical and PharmaCare information. I am also satisfied that, having gained unauthorized access to the systems in ways the Ministry described, a hacker could attack the systems, causing financial harm, loss of productivity, harm to reputation, loss of availability of systems or services and an increased risk of inappropriate access to large volumes of personal information.[31]

[28] I also accept that the personal information in government systems is valuable to the "underground market," for example, for use in identity theft or through the sale of credit card numbers and medical health numbers.[32] For all these reasons, I find that disclosure of the remaining information in question could reasonably be expected to harm the security of the information systems.

[29] This finding is consistent with Order F11-14,[33] in which the adjudicator found that s. 15(1)(l) applied to information which is similar in character to that at issue here.[34] The adjudicator was satisfied that disclosure of the information in dispute in that case could reasonably be expected to harm the security of government computer systems, because it provided a "road map" for a hacker "to attack desired targets once inside the government's security perimeter."[35]

---

[28] Ministry's initial submission, paras. 22-23.
[29] Ministry's initial submission, paras. 39-61.
[30] Social engineering involves a person obtaining as much information as possible about an authorized user of a system to masquerade as that user and gain access to a system to which the person would not otherwise have access; para. 32, Ministry's initial submission.
[31] Ministry's initial submission, paras. 25-38. The Ministry also gave an example of an incident where this happened; Ministry's initial submission, paras. 36-38.
[32] Ministry's initial submission, para. 61.
[33] Order F11-14, 2011 BCIPC 19 (CanLII).
[34] The information to which Order F11-14 found that s. 15(1)(l) applied included the following: how certain software applications interact and interface with one another; an organizational flowchart explaining how various government system servers interact with each other; a table that ranked various software applications in terms of their criticality to the system as a whole, thus revealing vulnerabilities of the system; system technical specifications; and a diagram of system architecture.
[35] Order F11-14, at para. 22. I arrived at a similar conclusion in Order F18-13, 2018 BCIPC 16 (CanLII).

Section 21 – Third-party business interests

[30] I found above that s. 15(1)(l) applies to some of the information Deloitte wants withheld under s. 21(1). Therefore, I need only consider s. 21(1) where it is the only exception claimed: a Ministry of Health Security Dashboard and issue log;[36] and portions of two other pages.[37]

[31] The relevant parts of s. 21(1) of FIPPA in this case read as follows:

> 21(1) The head of a public body must refuse to disclose to an applicant information
>
> (a) that would reveal
>
> (i) trade secrets of a third party, or
> (ii) commercial, financial, labour relations, scientific or technical information of or about a third party,
>
> (b) that is supplied, implicitly or explicitly, in confidence, and
>
> (c) the disclosure of which could reasonably be expected to
>
> (i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,
> (ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
> (iii) result in undue financial loss or gain to any person or organization, …

[32] Previous orders and court decisions have established the principles for determining whether s. 21(1) applies.[38] All three parts of the s. 21(1) test must be met in order for the information in dispute to be properly withheld. First, Deloitte must demonstrate that disclosing the information at issue would reveal one or more of the following: trade secrets of a third party; or commercial, financial, labour relations, scientific or technical information of, or about, a third party. Next, it must demonstrate that the information was supplied, implicitly or explicitly, in confidence. Finally, it must demonstrate that disclosure of the information could reasonably be expected to cause one or more of the harms set out in s. 21(1)(c).

---

[36] All of pages 285-297, phase 4.
[37] Small amounts of information on pages 8 and 153, phase 6.
[38] See, for example, Order 03-02, 2003 CanLII 49166 (BCIPC), Order 03-15, 2003 CanLII 49185 (BCIPC), and Order 01-39, 2001 CanLII 21593 (BCIPC).

[33] I find below that s. 21(1) does not apply. This is because, while I find that s. 21(1)(a) applies, I find that s. 21(1)(b) does not. I also find that Deloitte has not established a reasonable expectation of harm under s. 21(1)(c).

Section 21(1)(a) – type of information

[34] Deloitte said that the information in dispute is its trade secrets, as well as its technical and commercial information. The Ministry and the applicant did not address this issue.

[35] **Commercial information**: In Deloitte's view, the records were prepared as part of a commercial enterprise and can be considered to contain commercial information. Deloitte said that the records contain information on the financial cost breakdown associated with carrying out the data security review services.[39]

[36] FIPPA does not define "commercial" information. However, previous orders have held that "commercial information" relates to commerce, or the buying, selling, exchanging or providing of goods and services. The information does not need to be proprietary in nature or have an actual or potential independent market or monetary value.[40]

[37] The withheld information pertains to the projects Deloitte carried out as part of its work for the Ministry, steps Deloitte proposed to take and issues that it identified as needing resolution.[41] I am satisfied that this information consists of commercial information of or about Deloitte, because it relates to commerce, or the buying, selling, exchanging or providing of goods and services. I find that s. 21(1)(a)(ii) applies to the information at issue in these pages. In light of this finding, I need not consider if the information is also Deloitte's trade secrets or technical information of or about Deloitte.

Supply in confidence – s. 21(1)(b)

[38] The next step is to determine whether the information at issue was "supplied, implicitly or explicitly, in confidence." The information must be both "supplied" and supplied "in confidence."[42] Deloitte said it supplied the information in dispute explicitly in confidence.[43] The Ministry and the applicant did not address this issue.

---

[39] Deloitte's initial submission, p. 5.
[40] See Order 01-36, 2001 CanLII 21590 (BC IPC) at para. 17, and Order F08-03, 2008 CanLII 13321 (BC IPC) at para. 62.
[41] The dashboard and issue log (pages 285-297, Phase 4); a phrase in a description of Deloitte's approach to a ministry security model (page 8, phase 6); and a table describing an approach to a problem (page 153, phase 6).
[42] See, for example, Order F17-14, 2017 BCIPC 15 (CanLII), at paras. 13-21, Order 01-39, 2001 CanLII 21593 (BC IPC), at para. 26, and Order F14-28, 2014 BCIPC 31 (CanLII), at paras. 17-18.
[43] Deloitte's initial submission, pp. 5-6.

[39] **Supply:** It is clear from the records themselves that Deloitte provided the information at issue to the Ministry. For example, Deloitte's name appears on the first page and the footers of each slide presentation. Its name also appears in the reports in which Deloitte documents its progress on various projects for the Ministry. There is no evidence that the information at issue was the product of negotiations between the Ministry and Deloitte. I accept that this information was "supplied" to the Ministry for the purposes of s. 21(1)(b).

[40] **In confidence:** A number of orders have discussed examples of how to determine if third-party information was supplied, explicitly or implicitly, "in confidence" under s. 21(1)(b), for example, Order 01-36:[44]

> [24] An easy example of a confidential supply of information is where a business supplies sensitive confidential financial data to a public body on the public body's express agreement or promise that the information is received in confidence and will be kept confidential. A contrasting example is where a public body tells a business that information supplied to the public body will not be received or treated as confidential. The business cannot supply the information and later claim that it was supplied in confidence within the meaning of s. 21(1)(b). The supplier cannot purport to override the public body's express rejection of confidentiality.
> …
>
> [26] The cases in which confidentiality of supply is alleged to be implicit are more difficult. This is because there is, in such instances, no express promise of, or agreement to, confidentiality or any explicit rejection of confidentiality. All of the circumstances must be considered in such cases in determining if there was a reasonable expectation of confidentiality. The circumstances to be considered include whether the information was:
>
> 1. communicated to the public body on the basis that it was confidential and that it was to be kept confidential;
> 2. treated consistently in a manner that indicates a concern for its protection from disclosure by the affected person prior to being communicated to the public body;
> 3. not otherwise disclosed or available from sources to which the public has access;
> 4. prepared for a purpose which would not entail disclosure.

[41] Deloitte said that it provided the information to the Ministry with the "express expectation that [it] would be held in confidence." Deloitte said that it has consistently held the information in confidence and the information is not available to the public or its competitors.[45]

---

[44] Order 01-36, 2001 CanLII 21590 (BC IPC).
[45] Deloitte's initial submission, pp. 5-6.

[42] There is no indication in the material before me that Deloitte supplied the information at issue "in confidence" to the Ministry. Deloitte's reports and other deliverables contain no explicit markers of confidentiality.[46] I also note that the Ministry said nothing about whether the information at issue was supplied "in confidence."

[43] In addition, the contracts themselves do not support Deloitte's confidentiality argument. Deloitte pointed to Article 5 of the contracts in support of its position. However, this provision addresses Deloitte's obligation to keep confidential any information it received from the Ministry. This article says nothing about whether Deloitte and the Ministry agreed that Deloitte was supplying its reports, presentations and other deliverables "in confidence." Deloitte has not, in my view, established that the information at issue was supplied, explicitly or implicitly, "in confidence," for the purposes of s. 21(1)(b).

Conclusion on s. 21(1)(b)

[44] I find that the information at issue was "supplied" but that it was not supplied "in confidence." This means that s. 21(1)(b) does not apply.

Reasonable expectation of harm – s. 21(1)(c)

[45] Given my findings above, I need not consider whether s. 21(1)(c) applies. For completeness, however, I will consider whether Deloitte has established a reasonable expectation of harm on disclosure of the information in dispute.

[46] **Harm to competitive position - s. 21(1)(c)(i):** Deloitte's arguments on harm did not address the information in dispute under s. 21(1). Rather, Deloitte addressed information that is no longer in dispute, that is, information that the Ministry has already disclosed[47] or which the applicant has agreed may be withheld.[48]

[47] Deloitte said its competitors could use the information in dispute to "compete unfairly or undercut Deloitte in providing these specialized services." Deloitte said it has "devoted considerable time, energy, expertise, and resources to developing these processes, costs and personnel choices to be able to provide the highest level of service to a targeted clientele." Deloitte added that disclosure of the information "could interfere significantly with its contractual relationships with current and potential clients by revealing cost structures and

[46] The statement of work says that it is "private and confidential" but the Ministry has disclosed this record in full.
[47] For example, its "personnel choices," expertise of its staff, processes and proposals, which appear in its statement of work.
[48] For example, its hourly rates and negotiations on rates.

personnel choices that would allow our competitors to use this opportunity to compete or undermine Deloitte."[49]

[48] Deloitte did not explain who its competitors were nor how they could use the information in dispute to do the things it fears. The dashboard, which is part of a report, lists a number of steps Deloitte was to accomplish, along with timelines. The information in the dashboard appears innocuous and, moreover, echoes information in other parts of the report that the Ministry has disclosed. It is not clear how disclosure of similar information, which, even at the time of this inquiry, was several years old, could cause harm to Deloitte's competitive position and Deloitte did not explain.

[49] The issue log, also part of the report, sets out a number of issues that Deloitte identified, their severity, information on how they were or would be resolved and relevant dates. This information, again, several years old, relates specifically to this project and appears innocuous. It is not clear how competitors could use it to harm Deloitte's competitive position in the future and Deloitte did not explain.

[50] I have the same comments about other information in dispute.[50] For instance, Deloitte is concerned about disclosure of information that refers to one of its methods and is of a promotional character.[51] Deloitte is also concerned about the disclosure of a diagram that sets out an approach to a problem and contains what appear to be generic headings.[52] Deloitte did not explain how this information might be unique, creative or proprietary, or how it might be useful to others. I do not see how Deloitte's competitors could use the information to harm its competitive interests and Deloitte did not explain.

[51] **No longer supply - s. 21(1)(c)(ii):** Deloitte said it is in the public interest for public bodies to be able to solicit and receive proposals such as those in the records. It said that professionals are more likely to provide information of this nature when they have the confidence to know their materials will not be disclosed outside the public body. In Deloitte's view, disclosure of the "confidential information could undermine the relationship of confidence between the Ministry and its external professional advisors. Professional advisors might not feel confident in providing advice … when it could be disclosed to the world at large, along with confidential personal rates and banking information, pursuant to an access request." Deloitte argued that it is "important to foster confidence so that public bodies like the Ministry can retain third party consultants for expert professional advice and services."[53]

---

[49] Deloitte's initial submission, page 6. All quotes come from this page.
[50] A term (p. 8, phase 6) and a diagram (page 153, phase 6).
[51] Page 8, phase 6.
[52] Page 153, phase 6.
[53] Deloitte's initial submission, pages 6-7.

[52] As noted above, Deloitte's arguments relate to information that is not at issue. Deloitte did not specifically address the dashboard, issue log and other information at issue. It is not clear how disclosure of this information could reasonably be expected to cause the harm Deloitte fears and Deloitte did not explain.

[53] **Undue loss or gain - s. 21(1)(c)(iii):** Deloitte said disclosure of the type of information of concern could result in "material loss to Deloitte in the manner described above." It said that the loss of its proprietary information would result in unfair gains to its competitors who could use the information to their competitive advantage "at the expense of organizations that devoted resources to develop their expertise and rates." Deloitte said that its "competitive position would be significantly and irreparably prejudiced and Deloitte would experience undue loss." Deloitte said its competitors could use the information to undercut and underbid it in future RFPs, causing serious harm to Deloitte's commercial interests. It added that disclosure of the negotiated rates would fundamentally undermine its ability to negotiate with government entities and private clients for any future engagements.

[54] Previous orders have said that the ordinary meaning of "undue" financial loss or gain under s. 21(1)(c)(iii) includes excessive, disproportionate, unwarranted, inappropriate, unfair or improper, having regard for the circumstances of each case. For example, if disclosure would give a competitor an advantage – usually by acquiring competitively valuable information – effectively for nothing, the gain to a competitor will be "undue."[54]

[55] Deloitte did not explain how disclosure of the specific information at issue here could result in undue loss to it or undue gain to its (unspecified) competitors. Deloitte also did not quantify any such loss or gain. It is not clear how disclosure of the information at issue could reasonably be expected to cause the harm Deloitte fears and Deloitte did not explain.

Conclusion on s. 21(1)(c)

[56] Deloitte has not, in my view, provided objective evidence that is well beyond or considerably above a mere possibility of harm, which is necessary to establish a reasonable expectation of harm under s. 21(1)(c).[55] Its evidence does not establish a direct link between the disclosure and the apprehended harm or that the harm could reasonably be expected to ensue from disclosure. Therefore, I find that s. 21(1)(c) does not apply to the information in dispute. Deloitte has

[54] See, for example, Order 00-10, 2000 CanLII 11042 (BC IPC) at pp. 17-19. See also Order F14-04, 2014 BCIPC 31 (CanLII) at paras. 60-63, for a discussion of undue financial loss or gain in the context of a request for a bid proposal.
[55] *Community Safety*, at para. 54.

not, in my view, met its burden of proof and I find, therefore, that s. 21(1) does not apply to the information at issue.

CONCLUSION

[57] For reasons given above, I make the following orders:

1. Under s. 58(2)(c) of FIPPA, I confirm that the Ministry is authorized to withhold the information it withheld under s. 15(1)(l), subject to item 2(a) below.

2. Under s. 58(2)(a), I require the Ministry to disclose the following:

    (a) the term and its acronym that the Ministry withheld under s. 15(1)(l) on pages 1-39, Phase 6; and

    (b) the information annotated with s. 21(1) on pages 285-297, Phase 4, and on pages 8 and 153, Phase 6.

[58] Under s. 59(1) of FIPPA, I require the Ministry to give the applicant access to the information in item 2 of the previous paragraph by December 23, 2019. The Ministry must concurrently copy the OIPC Registrar of Inquiries on its cover letter to the applicant, together with a copy of the records. For clarity, I have highlighted in yellow the information I am ordering disclosed in a copy of the relevant pages that accompany the Ministry's copy of this order.

November 8, 2019

ORIGINAL SIGNED BY

Celia Francis, Adjudicator

OIPC File No.: F14-59804