Order F21-01

INSURANCE CORPORATION OF BRITISH COLUMBIA

Lisa Siew
Adjudicator

January 4, 2021

CanLII Cite: 2021 BCIPC 01
Quicklaw Cite: [2021] B.C.I.P.C.D. No. 01

Summary: An applicant requested the Insurance Corporation of British Columbia (ICBC) provide access, under the *Freedom of Information and Protection of Privacy Act* (FIPPA), to records about an ICBC telephone line used to support law enforcement agencies. ICBC withheld information under s. 15(1)(l) claiming the disclosure of the withheld information could reasonably be expected to harm the security of its communications system. The adjudicator determined that ICBC did not prove s. 15(1)(l) applied to the information at issue and required ICBC to disclose that information to the applicant.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, s. 15(1)(l).

INTRODUCTION

[1] An applicant requested access to records from the Insurance Corporation of British Columbia (ICBC) under the *Freedom of Information and Protection of Privacy Act* (FIPPA). The applicant requested the "privacy impact assessment" and "the policies, procedures and operations manual" for "the ICBC police line."[1] The applicant describes the ICBC police line as a phone number or hotline that the police call to obtain information from ICBC about drivers and insurance policy holders.

[2] ICBC informed the applicant that a privacy impact assessment was not completed for the operation of ICBC's police line. It provided the applicant with a copy of the procedure and operations manual, but withheld a small amount of information under s. 15(1)(l) (harm to the security of any property or system).

[1] Applicant's access request by email dated March 20, 2015.

[3] The applicant requested the Office of the Information and Privacy Commissioner (OIPC) review ICBC's decision to refuse access to the withheld information. Mediation did not resolve the issues in dispute and the matter was forwarded to inquiry. Both parties provided inquiry submissions and ICBC's submissions include pre-approved *in camera* materials.

PRELIMINARY MATTER

[4] In his submission, the applicant claimed for the first time that it was in the public interest, under s. 25 of FIPPA, for ICBC to disclose the withheld information because "it is in the public interest to know that a public body is carelessly holding and disclosing personal information."[2] Section 25 requires a public body to disclose information without delay, if disclosure is clearly in the public interest or the information is about a risk of significant harm to, among other things, public safety. This section applies despite any other provision of FIPPA.

[5] The applicant also claimed that ICBC was in violation of s. 6 of FIPPA. Under s. 6(1) public bodies are required to make every reasonable effort to respond without delay to each applicant openly, accurately and completely. The applicant says ICBC failed to tell him, in its written response to his access request, which FIPPA exception was being relied on to withhold the information at issue.

[6] The applicant further alleges ICBC failed to conduct a privacy impact assessment. To support this allegation, the applicant provided a copy of an OIPC document titled, *Early notice and Privacy Impact Assessments to the OIPC under the Freedom of Information and Protection of Privacy Act (Updated July 2012)*. This document provides guidance and instructions to public bodies who are planning a "data-linking initiative" or a "common or integrated program or activity."[3]

[7] ICBC objects to the applicant raising these additional matters at this late stage, noting that s. 15 is the only issue set out in the notice of inquiry. ICBC says the applicant has made no attempt to explain why ss. 6 and 25 are being raised for the first time at this point in the inquiry. ICBC also clarifies that its police support line is not a "data-linking initiative" since there is no "linking" or "combining" of its database with any other public body or agency database. Relying on previous OIPC orders, ICBC submits that these additional matters ought to be disregarded since a party is not entitled to introduce a new issue at the inquiry stage unless permission is granted from the OIPC, which ICBC says was not granted in this case.

---

[2] Applicant's submission at para. 11.
[3] Schedule 1 of FIPPA defines both these terms.

[8] None of the additional issues now being raised by the applicant were identified in the OIPC investigator's fact report or in the notice of inquiry. Previous OIPC orders have consistently said parties may raise new issues at the inquiry stage only if they request and receive permission to do so.[4] The applicant did not seek permission to add these additional matters to the inquiry or explain why he should be permitted to do so at this late stage. There is also nothing in the materials before me that suggests s. 25 may be engaged or that the public body was required, under FIPPA, to conduct a privacy impact assessment.

[9] With regards to s. 6, where an applicant complains that a public body has not performed a duty under FIPPA, the OIPC requires the applicant to raise the issue with the public body first, prior to making a complaint to the OIPC. The applicant is required to give the public body an opportunity to respond and attempt to resolve the complaint. There is no evidence that the parties first attempted to resolve this matter between themselves. Additionally, once the OIPC has accepted a complaint, it is usually investigated and resolved by a case review officer or an investigator and not at a formal inquiry.[5]

[10] For all these reasons, I decline to add the additional issues raised by the applicant at this late stage to this inquiry.

ISSUE

[11] Given my findings above, the only issue I must decide in this inquiry is whether ICBC is required to withhold the information at issue under s. 15(1)(l) of FIPPA. Section 57(1) places the burden on ICBC, as the public body, to prove the applicant has no right of access to the withheld information.

DISCUSSION

Background

[12] ICBC is a provincial Crown corporation that provides basic and optional auto insurance to BC motorists. It also issues driver licences, vehicle licences and registration, and identification cards. Through these services, ICBC collects and holds the personal information of millions of individuals who have driver licences, insurance policies, insurance claims, voluntary identification cards, and BC Services Cards.[6]

[13] The phone line that is central to this inquiry is referred to by ICBC as the "Police Support Line." This support line is described as a dedicated phone line

[4] See for example, Order F19-41, 2019 BCIPC 46 at para. 5.
[5] Order F18-11, 2018 BCIPC 14 at para. 6 and Decision F08-02, 2008 CanLII 1647 (BC IPC) at para. 38.
[6] This background information about ICBC is found in the OIPC's *Audit and Compliance Report F17-01* at p. 1. The report was noted in the applicant's submission at para. 17.

operated by ICBC employees that is used solely by municipal, provincial and federal law enforcement agencies for making enquiries relating to vehicle information such as descriptions and registration numbers. It is also used by these agencies to obtain information about the registered owner of a vehicle such as their name, date of birth, address and driver's licence information.

[14] ICBC explains that the support line receives calls that may be general in nature or related to an emergency such as a threat of homicide or an abduction. ICBC says the support line annually receives thousands of calls from law enforcement agencies requesting information. It identifies three categories of information commonly requested by law enforcement agencies: (1) telephone numbers; (2) addresses; and (3) insurance policy information.

Record and information in dispute

[15] The record at issue is a four-page document which describes the procedures used by ICBC employees for the operation of the Police Support Line.[7] ICBC disclosed most of the record and only withheld a small amount of information on page two of this record under s. 15(1)(l). ICBC explains that the withheld information is an additional tool used by ICBC employees to ensure that callers to the Police Support Line are, in fact, a member of a law enforcement agency.[8]

[16] To be clear, the withheld information reveals what the ICBC employee is specifically instructed to request from the caller if they are unable to provide other verifying information. The ICBC employee asks the caller to provide this information as part of the vetting process. The question on its own, however, does not reveal the actual correct answer. The caller is expected to answer with a specific type of information that verifies that they are a legitimate member of a law enforcement agency. I will refer to this information as the "vetting information." ICBC submits that the disclosure of the withheld information would allow someone to obtain the vetting information.

Section 15(1)(l) – harm to a communications system

[17] Section 15(1)(l) of FIPPA provides that a public body must refuse to disclose information if the disclosure "could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system or a communications system."

[18] Based on the wording of s. 15(1)(l), the questions to be answered in this inquiry are as follows:

[7] Affidavit of ICBC's senior legal counsel at para. 3.
[8] *Ibid* at para. 9.

1. Is the Police Support Line a system, in particular, a communications system?

2. If the Police Support Line is a communications system, could disclosure of the withheld information reasonably be expected to harm the security of that system?

[19] The standard of proof applicable to harms-based exceptions like s. 15(1)(l) is whether disclosure of the information could reasonably be expected to cause the specific harm. The Supreme Court of Canada has described this standard as "a reasonable expectation of probable harm" and "a middle ground between that which is probable and that which is merely possible."[9] There needs to be a reasonable basis for believing the harm will result and the standard does not require a demonstration that harm is probable.[10] The public body need not show on a balance of probabilities that the harm will occur if the information is disclosed, but it must demonstrate that disclosure will result in a risk of harm that is well beyond the merely possible or speculative.[11]

[20] The determination of whether the standard of proof has been met 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 the "inherent probabilities or improbabilities or the seriousness of the allegations or consequences."[12] Previous OIPC orders have said general speculative or subjective evidence will not suffice.[13] Further, it is the release of the information itself which must give rise to a reasonable expectation of harm.[14] The public body must prove there is a clear and direct connection between the disclosure of the specific information at issue and the alleged harm.[15]

ICBC's submission

[21] ICBC submits the Police Support Line qualifies as a communications system under s. 15(1)(l). It notes that the term "system" is not defined in FIPPA,

---

[9] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at para. 54, citing *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3 at paras. 197 and 199.
[10] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII) at para. 59 and *British Columbia Hydro and Power Authority v British Columbia (Information and Privacy Commissioner)*, 2019 BCSC 2128 (CanLII) at para. 93.
[11] *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3 at para. 206.
[12] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at para. 54.
[13] For example, Order F08-03, 2008 CanLII 13321 (BC IPC) at para. 27.
[14] *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner),* 2012 BCSC 875 at para. 43.
[15] *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3 at paras. 197 and 219. Order F08-03, 2008 CanLII 13321 (BC IPC) at para. 27.

but it says the non-exhaustive examples under s. 15(1)(l) include a computer system and a communications system.[16] It also relies on Order F15-32 and Order F17-23 which found a teleconference phone line qualifies as a communications system.[17] I understand ICBC is arguing that the Police Support Line is similar enough to a teleconference line that it should be considered a communications system.

[22] ICBC also relies on Order F15-32 and Order F17-23 to establish that disclosing the withheld information would harm the security of its dedicated phone line. In Order F15-32, the adjudicator found that disclosing teleconference numbers, ID numbers and passwords would create a real risk of unauthorized individuals potentially accessing the public body's teleconferences.[18] In Order F17-23, the adjudicator was satisfied that the disclosure of the conference call ID numbers could reasonably result in someone gaining access to confidential government teleconference calls.[19] ICBC argues that the withheld information about the Police Support Line is sufficiently analogous to the teleconference ID numbers that were withheld in these previous orders and, therefore, s. 15(1)(l) should also apply to the information at issue.

[23] ICBC submits that it withheld the disputed information due to a real and substantial possibility of harm to the integrity of the Police Support Line. ICBC describes the harm as the real possibility of unauthorized access to the personal information in its databases and the weakening of its vetting process. ICBC explains that, before it gives the caller the information they seek, the ICBC employee must obtain and record the caller's name, badge number or regimental number, employee number (if a dispatcher), and the police file number. If the caller can provide those details, the ICBC employee will provide the requested information. However, if a caller is unable to provide those details, the ICBC employee will move on to verify the identify of the caller by asking for the vetting information.

[24] ICBC provided an affidavit from its senior legal counsel in support of its position. ICBC's senior legal counsel explains that the vetting information allows ICBC employees to ensure that a caller to the line who cannot give other identifying information is, in fact, a member of a law enforcement agency before any personal information is released to them.[20] ICBC's legal counsel says if someone who is not a member of a law enforcement agency obtained access to the vetting information, then it would be possible for them to impersonate a law

[16] ICBC's initial submission at para. 25.
[17] ICBC's initial submission at paras. 25-26, citing Order F15-32, 2015 BCIPC 35 and Order F17 23, 2017 BCIPC 24.
[18] 2015 BCIPC 35 at para. 12. The adjudicator was also satisfied with *in camera* evidence of additional harm described by the public body's Chief Information Officer.
[19] 2017 BCIPC 24 at paras. 69 and 73.
[20] Affidavit of senior legal counsel at paras. 10-11.

enforcement official and obtain personal information from the Police Support Line.[21]

[25] ICBC explains that it is attempting to safeguard the integrity of the Police Support Line and prevent any unauthorized access or disclosure of personal information in accordance with its obligations under FIPPA. ICBC says it is statutorily required under s. 30 of FIPPA to protect personal information in its custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[26] ICBC submits that reasonable security standards include developing appropriate policies and procedures relating to personal information protection, as it has done with its vetting process. ICBC claims that it is reasonably foreseeable that disclosing the withheld information would compromise the integrity of its authentication system for the Police Support Line.

[27] ICBC also believes that it would suffer other harms if the withheld information was disclosed. ICBC says it would be prejudiced by the disclosure because it would be forced to take a particular course of action which it describes *in camera*. It says disclosing the withheld information would also require it to notify all law enforcement agencies, change its policies and procedures, retrain its employees and require "other operational undertakings."[22]

Applicant's submission

[28] The applicant rejects ICBC's claim that s. 15(1)(l) applies to the withheld information and says it is not a violation of s. 15 for the full record to be disclosed. The applicant cites a number of past OIPC orders that determined s.15(1)(l) did not apply to the information at issue. The applicant submits those orders establish that s. 15(1)(l) does not apply in the following circumstances:

- When the public body fails to establish a clear connection between the release of the information and a risk of harm.[23]

- When a public body's assertions about a potential security risk are implausible given the non-sensitive nature of the information and the availability of other security measures.[24]

[21] Affidavit of senior legal counsel at para. 12.
[22] ICBC's initial submission at para. 36.
[23] Order F08-13, 2008 CanLII 41151 (BC IPC); Order F17-54, 2017 BCIPC 59 (CanLII).
[24] Order F18-41, 2018 BCIPC 44 (CanLII).

- Where a public body fails to provide sufficient evidence that a person masquerading as a legitimate user could use the information in dispute to gain unauthorized access to an information system.[25]

[29] In particular, the applicant cites the following from Order F10-25 about a public body's burden to establish that disclosing the information at issue could reasonably be expected to result in unauthorized access:

> …It is of course always theoretically possible that criminals will use all sorts of publicly available information in a dishonest fashion to illegally access confidential information. In my view, that possibility, by itself, is not sufficient to refuse to disclose information. There must be something more that ties a special risk to a particular context so as to meet the "reasonable expectation" test….[26]

[30] The applicant also questions the lack of any appropriate safeguards in ICBC's verification process to prevent a well-rehearsed fraudster from using illegally obtained or fabricated information to successfully bypass the verification system. The applicant says ICBC's evidence does not indicate whether the phone line operator verifies or checks the information that the caller provides to authenticate their identity.

[31] The applicant also relies on four news articles to show "numerous cases of the wrongful access and use of information from databases in BC."[27] One article discusses how a reporter pretended to be a mall security officer to obtain details about a potential security incident. Another article discusses how a person paid an ICBC employee to provide them with the personal information of their victims by using licence plate information.

[32] The applicant argues that the public is interested in knowing whether a public body is "carelessly holding and disclosing personal information."[28] The applicant says the public has a right to know and understand how the Police Support Line is administered. The applicant argues that "if ICBC and police agencies have poor controls – and the record reflects that – then that is no defence in these proceedings."[29]

ICBC's response submission

[33] ICBC notes that the news stories of privacy breaches that the applicant mentions only serve to highlight its concerns regarding the disclosure of the

[25] Order F10-25, 2010 BCIPC 36 (CanLII).
[26] Order F10-25, 2010 BCIPC 36 (CanLII) at para. 20.
[27] Applicant's submission at para. 12.
[28] *Ibid* at para. 11.
[29] *Ibid* at para. 19.

withheld information. ICBC says that it recognizes its responsibility for ensuring the security of the personal information in its custody and control. It submits that it is evident from its submissions that "there are safeguards put in place to ensure that only those individuals who can accurately identify themselves as law enforcement by reference to, among other things, the severed information may obtain personal information from the ICBC Police Support Line."[30]

[34] ICBC also distinguishes the previous OIPC orders cited by the applicant. It discusses each order and explains how the circumstances and the information differ from what is at issue here. For instance, ICBC submits that the risk of unauthorized access in the present case is not remote as it was in Order F10-25 or speculative like it was in Orders F15-32 and F17-23. ICBC says the information at issue in this case is not general or non-descript information where it is unlikely that the security risk will arise.[31] ICBC describes the information that it is trying to protect as the sensitive personal information in its databases, including the driver's licence numbers and addresses of various individuals.[32]

[35] ICBC explains that the vetting information is necessary to identify a member of a law enforcement agency in certain circumstances. It says the withheld information "is itself, a form of prevention of unauthorized access" and that "there is no other security measure that ICBC could take absent creating and distributing a different piece of information."[33] It submits that the limited distribution of this information makes it a useful security safeguard; therefore, it is necessary to protect this information.

Analysis and findings

Is the Police Support Line a communications system?

[36] FIPPA does not define the term "system," but s. 15(1)(l) recognizes that a computer system or a communications system qualifies as a "system" under s. 15(1). Past orders have found that a "system" includes a video surveillance system and a public transportation system.[34] In Order F16-52, Adjudicator Whittome considered the ordinary meaning of the word "system" as defined in the English Oxford dictionary and concluded that "a series of clear security principles or procedures could comprise a security 'system' under s. 15(1)(l)."[35]

[30] ICBC's response submission at para. 8.
[31] *Ibid* at para. 11.
[32] *Ibid* at para. 13.
[33] *Ibid* at para. 13.
[34] Order F15-72, 2015 BCIPC 78 at para. 27, citing Order F08-03, 2008 CanLII (BCIPC) at para. 43 and Order F09-13, 2009 CanLII 42409 (BC IPC) at para. 13-17.
[35] Order F16-52, 2016 BCIPC 58 (CanLII) at para. 37.

[37] The term "communications system" is also not defined in FIPPA. But, I note that the English Oxford dictionary defines the word "communications" to include "the imparting or exchanging of information by speaking, writing, or using some other medium" and a "means of sending or receiving information, such as phone lines or computers".[36] Further, as noted by ICBC, past orders have accepted that a teleconferencing system qualifies as a communications system.[37]

[38] I am satisfied the Police Support Line qualifies as a communications system under s. 15(1)(l). The Police Support Line allows members of law enforcement agencies to request and receive information from ICBC employees through a dedicated phone line. I, therefore, conclude the Police Support Line is a communications system for the purposes of s. 15(1)(l), considering the ordinary meaning of the words "communications" and "system" and taking into account the types of processes and activities that have previously qualified under this exception.

Is there a reasonable expectation of probable harm to the system?

[39] For the reasons to follow, I find ICBC has not provided sufficient evidence to establish that disclosing the withheld information could reasonably be expected to harm the security of its Police Support Line. ICBC submits that the disclosure of the withheld information would allow someone to obtain the vetting information, thereby, allowing an unauthorized individual to impersonate a member of a law enforcement agency and access the personal information in its databases. ICBC also argues disclosing the withheld information would compromise its vetting process because it would reveal one of its security safeguards and it would be difficult to find a suitable replacement.

[40] ICBC's arguments about the risk of harm are based on the assumption that an unauthorized individual (i.e. someone not associated with a law enforcement agency) armed with advanced knowledge of what information is required for ICBC's vetting process could reasonably be expected to locate, obtain and use that information to gain access to the personal information in ICBC's databases. Therefore, in order to establish that the alleged harm could reasonably be expected to result from disclosing the withheld information, there needs to be some evidence as to the likelihood that someone who is not a member of a law enforcement agency could find or obtain the vetting information.

[41] This reasoning also applies to ICBC's claims that the disclosure of the withheld information would weaken its vetting process. Any alleged compromise of ICBC's vetting process is contingent on the likelihood of someone being able to obtain the vetting information. ICBC also submits that disclosing the withheld information would require it to undergo the time and effort to find a suitable

[36] *Oxford English Dictionary*, online: https://en.oxforddictionaries.com.
[37] For example, Order F15-32, 2015 BCIPC 35 (CanLII) at para. 12.

replacement, as well as the update of its procedures and the retraining of its staff. However, ICBC would only need to undertake those activities if it could reasonably be expected that someone who is not a member of a law enforcement agency could locate or obtain the vetting information.

[42] ICBC's submissions do not explain how someone who is not a member of a law enforcement agency could locate and obtain the vetting information. It is also not apparent from the materials before me how this would be possible and I am not going to speculate. For instance, ICBC does not discuss the public availability or the ease with which the vetting information can be found or obtained. As a result, I find ICBC has not established a clear and direct connection between the disclosure of the withheld information and the alleged harm.

[43] ICBC also does not explain how someone could locate or obtain the phone number to call the Police Support Line. The record itself says "if the caller does not know the secure line number for police support calls, they should get the number from their commanding officer, the Canadian Police Information Centre (CPIC) Headquarters in Vancouver, or a BC Detachment, if they are from an out of province police department."[38] The applicant also provided a news article that claims the ICBC phone number is changed every six months. ICBC does not discuss or mention this fact. ICBC also does not address the likelihood of a potential wrongdoer bypassing these security measures, which ensures the secure phone number is only disclosed to authorized individuals. Without more, it is unclear how a potential wrongdoer could obtain the phone number to the secured phone line.

[44] I also find the cases cited by ICBC about teleconferencing are distinguishable from the present circumstances. The information at issue in those cases was the actual teleconference and ID numbers and passcodes used to access the public body's teleconference phone system. In this case, as previously noted, the withheld information is not the actual, specific information that a caller must provide to verify the legitimacy of their identity. Put another way, if the information at issue was a teleconference access ID number, ICBC is not withholding the actual ID number as was the case in Order F15-32 and Order F17-23. Instead, ICBC is arguing that even knowing the general type of information needed to pass its vetting process could reasonably be expected to harm the security of its communications system.

[45] Previous orders have found that it is "always theoretically possible that criminals will use all sorts of publicly available information in a dishonest fashion to illegally access confidential information"; therefore, something more is needed "that ties a special risk to a particular context so as to meet the 'reasonable

[38] Record in dispute at p. 1.

expectation' test".[39] In the present case, ICBC does not discuss or provide evidence, even on an *in camera* basis, to show whether the vetting information is publicly available.

[46] Further, simply knowing that a caller must provide the vetting information does not result in a reasonable expectation that they will then be able to impersonate a member of a law enforcement agency and successfully obtain personal information from ICBC's databases. In order to establish that the anticipated harm is well beyond or considerably above a mere possibility, there has to be some evidence about the likelihood an illegitimate caller will be able to find or obtain the vetting information, as well as obtain the secure phone number to the Police Support Line. In my view, the evidence in this case does not meet that threshold. As a result, I conclude ICBC is not authorized to withhold the information at issue under s. 15(1)(l).

CONCLUSION

[47] For the reasons given above, under s. 58 of FIPPA, I make the following order:

1. ICBC is not authorized to refuse access to the information that it withheld under s. 15(1)(l).

2. ICBC must disclose this information to the applicant and concurrently copy the OIPC registrar of inquiries on its cover letter to the applicant, along with a copy of the relevant record.

[48] Under s. 59 of FIPPA, ICBC is required to give the applicant access to the information it is not authorized to withhold by February 16, 2021.

January 4, 2021

ORIGINAL SIGNED BY

Lisa Siew, Adjudicator

OIPC File No.: F15-61425

[39] Order F10-25, 2010 BCIPC 36 (CanLII) at para. 20.