Order F25-26

DISTRICT OF SUMMERLAND

Emily Kraft
Adjudicator

March 27, 2025

CanLII Cite: 2025 BCIPC 32
Quicklaw Cite: [2025] B.C.I.P.C.D. No. 32

Summary: The applicant made a request under the *Freedom of Information and Protection of Privacy Act* (FIPPA) to the District of Summerland (District) for access to certain email communications sent or received by a number of named individuals. The District withheld the information in dispute in this inquiry under s. 15(1)(l) (harm to the security of a property or system) of FIPPA. The adjudicator found that s. 15(1)(l) applied to the information in dispute and confirmed the District's decision to withhold it.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s. 15(1)(l)

INTRODUCTION

[1] Under the *Freedom of Information and Protection of Privacy Act* (FIPPA), an individual (applicant) requested that the District of Summerland (District) provide him with access to certain email communications sent or received by a number of named individuals.

[2] The District provided the applicant with 657 pages of responsive records but withheld some information under ss. 3 (scope of FIPPA), 13 (advice or recommendations), 14 (solicitor-client privilege), 15(1)(l) (harm to the security of a property or system), 21 (harm to third-party business interests), and 22 (unreasonable invasion of third-party personal privacy) of FIPPA.

[3] The applicant requested that the Office of the Information and Privacy Commissioner (OIPC) review the District's decision. During mediation by the OIPC, the District released additional information to the applicant. Also, the applicant decided that he was only requesting a review of the District's decision to withhold information under ss. 15(1)(l) and 22(1) on two pages of responsive

records (pages 134 and 516). Mediation did not resolve the remaining issues and the matter proceeded to this inquiry.

[4] In his submission for this inquiry, the applicant stated that a different public body[1] had already provided him with access under FIPPA to the information withheld under s. 22(1) on page 134 of the records. He attached an unredacted copy of this record to his submission. It is not clear to me why the applicant is using FIPPA's review and inquiry processes to obtain access to information that he was already given access to under FIPPA. Regardless, in light of the applicant's submission, the District reconsidered its application of s. 22(1) to the information on page 134 and released that information to the applicant during this inquiry.[2] Since that information was the only information in dispute under s. 22(1), I conclude s. 22(1) is no longer an issue in this inquiry.

PRELIMINARY MATTER

Mediation material

[5] In his submission for this inquiry, the applicant discussed and attached the OIPC investigator's opinion that was provided during mediation. The District says that this is mediation material and that I should not consider it.[3]

[6] In support of its position, the District quotes the following portion of the OIPC's *Instructions for Written Inquiries*:

> "Mediation material" refers generally to communications that relate to offers or attempts to resolve the matter during mediation. The Commissioner will not consider mediation materials in reaching a decision and issuing an order. To preserve the integrity of the "without prejudice" nature of the mediation process, a party may not, without the written consent of the other parties, refer to or include in its submissions any mediation materials, including any opinions or recommendations an investigator expressed during mediation. However, it is permissible to refer to information which is not mediation material, for instance an investigator's decisions about the issues and the scope of the records that will proceed to inquiry, or an investigator's decision in complaints. Parties may include information about such factual outcomes in their submissions.[4]

[7] I find that the investigator's opinion that was attached and discussed in the applicant's submission is clearly mediation material and the District objects to it

[1] The Provincial Agriculture Land Commission.
[2] District's reply submission at para 6 and email dated March 11, 2025.
[3] District's reply submission at paras 3-5.
[4] https://www.oipc.bc.ca/documents/guidance-documents/1658 at pp 6-7.

being introduced into the inquiry. I will not consider this material when making my decision.[5]

ISSUE

[8] The issue I must decide in this inquiry is whether the District is authorized under s. 15(1)(l) to refuse to disclose the information in dispute.

[9] Under s. 57(1), the District has the burden of proving that it is authorized to refuse to disclose the information in dispute under s. 15(1)(l).

DISCUSSION

Background

[10] The parties provided very little background information about their dispute in their inquiry submissions. I understand that the applicant is a resident of the District, and that he and his neighbour are involved in an ongoing legal dispute.[6] Some of the responsive records are related to that legal dispute.

Information in dispute

[11] The only information in dispute is a file path that appears in an email between two District employees.[7] The District is withholding this information under s. 15(1)(l).

Section 15(1)(l) - harm to the security of a property or system

[12] Section 15(1)(l) says that a public body may 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.

[13] The standard of proof for s. 15(1)(l) is a reasonable expectation of probable harm, which is "a middle ground between that which is probable and that which is merely possible."[8] In order to meet that standard, a public body

---

[5] For a similar approach, see Order F24-62, 2024 BCIPC 72 at para 14.
[6] Affidavit of Corporate Officer at para 6.
[7] Page 516 of the records. I note that the copy of this page that was initially provided to the OIPC also contains some information that was withheld under s. 22(1) as well as some information for which no FIPPA exception was cited. I wrote to the District about this matter and it clarified that the information withheld under s. 22(1) was disclosed to the applicant during mediation (District's letter dated January 18, 2024 and attachments). Also, the District clarified that the information for which no FIPPA exception was cited is a number that was added to the record during the District's sorting process and then removed so as to not cause confusion to the applicant. Accordingly, the only information in dispute on page 516 is the file path.
[8] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at para 54.

"must provide evidence 'well beyond' or 'considerably above' a mere possibility of harm."[9]

Parties' submissions

District's initial submission

[14] The District says that the information withheld under s. 15(1)(l) is a file path to District materials stored on an internal server.[10] It says that disclosure of this information could reasonably be expected to harm the security of a computer system.

[15] In support of its submission, the District provided an affidavit from its manager of information technology (IT Manager), who oversees the District's cybersecurity. The IT Manager says that the District has previously been a victim of a successful external cyber attack against its website. The IT Manager says that, as a cybersecurity measure, the District limits the disclosure of internal District file paths to District staff only. He says that disclosing the file path would reveal the structure of the District's internal systems, which could:

- Provide an attacker with information to allow them to target specific locations;
- Allow an attacker to create more convincing phishing emails or social engineering attempts by referencing a specific and accurately named District file path; and
- Aid an attacker in attempting brute force attacks on specific District systems or exploit known vulnerabilities in the system structure.[11]

[16] The District also cites OIPC Orders F15-12[12] and F20-20[13] in support of its position that s. 15(1)(l) applies.

[17] In Order F15-12, the adjudicator determined that s. 15(1)(l) applied to a file path to a secure file transfer location where files were stored by government security investigation staff. The adjudicator found that disclosing that information could harm the security of the secure file transfer system by revealing information about where files are stored, making the system more vulnerable to a security breach.[14]

[18] In Order F20-20, the adjudicator found that s. 15(1)(l) applied to a web link to an externally accessible site containing sensitive information. The public body

---

[9] *Ibid*.
[10] District's initial submission at para 10.
[11] Affidavit of IT Manager at para 7.
[12] 2015 BCIPC 12.
[13] 2020 BCIPC 23.
[14] 2015 BCIPC 12 at para 68.

in that case provided evidence from its senior manager of cybersecurity who deposed that there had been several hacking attempts against the public body and that the public body relied on numerous layers of protection against hackers, including limiting disclosure of the web link. The adjudicator accepted that the web link to a secure location for documents was related to the security of a computer system and found that the evidence provided by the public body demonstrated that disclosure could reasonably be expected to harm the security of the location of sensitive documents.[15]

Applicant's response submission

[19] The applicant says that the District's submissions about s. 15(1)(l) are vague and speculative and that the District has not met its burden of proof.

[20] The applicant notes that in Order F20-20, the public body in that case provided evidence that there had been numerous hacking attempts against it. The applicant says that unlike in Order F20-20, in this case, the District provided no evidence of previous cyber attacks on its internal server. He says there is a significant difference between an external cyber attack on the District's website and a cyber attack on its internal server. The applicant also says that the District provided no evidence about whether file paths were attacked or compromised in its previous cyber attack.

[21] The applicant also says that the file path at issue does not reveal where confidential documents are stored and therefore disclosing it would not pose a security risk.

[22] Finally, the applicant notes that pages 145 and 176 of the responsive records contain other file paths that were not redacted.[16]

District's reply submission

[23] In reply, the District says that evidence of a prior attack on internal computer systems is not a requirement for the application of s. 15(1)(l). It says that the absence of prior internal breaches is indicative of successful security measures, rather than the non-existence of threats to cybersecurity.

[24] The District acknowledges that pages 145 and 176 of the records include file paths that it says were inadvertently left unredacted. However, it says that inadvertent disclosure of those file paths does not adversely impact the District's ability to withhold similar information. It cites Order 03-35,[17] where former Commissioner Loukidelis found that the inadvertent disclosure of some information did not completely negate the risk of harm under s. 17(1) that could

[15] 2020 BCIPC 23 at para 86.
[16] Applicant's response submission at paras 15-23.
[17] 2003 CanLII 49214 (BC IPC) at paras 22-34.

reasonably be expected to result from disclosure of the fully and accurately constituted information. The District says that the risk of harm created by the inadvertent disclosure of certain file paths in this case does not negate the further risk of harm that would be created by disclosing an additional file path.[18]

Analysis and findings

[25] For the reasons that follow, I am satisfied that s. 15(1)(l) applies to the information in dispute.

[26] First, I find that the District's internal server qualifies as a "computer system" under s. 15(1)(l). Previous OIPC orders have reached the same conclusion.[19]

[27] Additionally, I accept the IT Manager's evidence that disclosing the file path would reveal information about the structure of the District's internal systems, which could allow a hacker to target specific locations in the District's server or create more convincing phishing or social engineering attempts. I find this evidence to be logical, and there is no evidence that contradicts it. I am therefore satisfied that disclosure of the file path could reasonably be expected to harm the security of the District's internal server.[20]

[28] Contrary to what the applicant seems to suggest, the District does not need to provide evidence of previous hacking attempts against its internal server or evidence that file paths have been exploited in previous hacking attempts in order to prove a reasonable expectation of probable harm. The District only needs to show that there is a reasonable basis for believing that harm will result; it does not need to prove on a balance of probabilities that the harm will in fact occur.[21] In my view, the District has met its burden in this case.

[29] I acknowledge that the District disclosed other file paths to materials stored on its internal server on pages 145 and 176 of the records. However, based on my review of these file paths, I find that they are different from the file path withheld on page 516. The file path withheld on page 516 reveals the name of another location on the server where it appears a different category of materials are stored. Therefore, its disclosure would provide additional information to a potential hacker about the structure of the District's internal systems.

---

[18] District's reply submission at paras 12-19.
[19] For instance, Order F21-35, 2021 BCIPC 43 at para 89.
[20] For a similar finding, see Order F17-23, 2017 BCIPC 24 at para 72.
[21] *British Columbia Hydro and Power Authority v British Columbia (Information and Privacy Commissioner),* 2019 BCSC 2128 at para 93; *Burnaby (City) v British Columbia (Information and Privacy Commissioner)*, 2023 BCSC 948 at para 64; *Merck Frosst Canada Ltd. v Canada (Health),* 2012 SCC 3 at para 196.

[30] Considering all this, I am satisfied that s. 15(1)(l) applies to the file path on page 516 of the records.

CONCLUSION

[31] For the reasons given above, under s. 58 of FIPPA, I confirm the District's decision to refuse to disclose the information in dispute under s. 15(1)(l).

March 27, 2025

ORIGINAL SIGNED BY

Emily Kraft, Adjudicator

OIPC File No.: F23-94193