Order F21-59

# BRITISH COLUMBIA HYDRO AND POWER AUTHORITY

Jay Fedorak
Adjudicator

November 19, 2021

CanLII Cite: 2021 BCIPC 68
Quicklaw Cite: [2021] B.C.I.P.C.D. No. 68

**Summary:** An applicant requested the emails that a certain contracted employee of the BC Hydro and Power Authority (BC Hydro) sent or received over a period of three days. BC Hydro refused to disclose information in the responsive records under s. 15(1)(l) (harm the security of a computer system) and s. 22 (unreasonable invasion of third-party personal privacy). The adjudicator found that s. 22(1) applied to some of the information at issue and ordered BC Hydro to withhold the information. The adjudicator found that s. 15(1)(l) did not apply to the records and ordered BC Hydro to disclose the remaining information.

**Statutes Considered:** *Freedom of Information and Protection of Privacy Act*, ss. 15(1)(l), 22(1), 22(2)(a), 22(2)(f), 22(3)(a), 22(3)(d), 22(3)(f), 22(4)(e).

## INTRODUCTION

[1] A journalist (applicant) made a request under the *Freedom of Information and Protection of Privacy Act* (FIPPA) to BC Hydro and Power Authority (BC Hydro) for the emails that a certain contracted employee sent or received over a period of three days. BC Hydro responded in July 2017 providing a list of all emails and copies of some of the emails. It severed some of the information in the list and in some of the information in the emails. It indicated that it was withholding the information in dispute under s. 15(1)(l) (harm the security of a computer system) and s. 22(1) (unreasonable invasion of third-party personal privacy). It withheld most of the emails in their entirety.

[2] The applicant requested a review by the Office of the Information and Privacy Commissioner (OIPC) of BC Hydro's decision to withhold the information under ss. 15(1)(l) and 22(1).

[3] Mediation by the OIPC did not resolve the matter and the applicant requested it proceed to an inquiry.

## ISSUE

[4] The issues in this inquiry are:

1. Whether s. 15(1)(l) authorizes BC Hydro to withhold information; and

2. Whether s. 22(1) of FIPPA requires BC Hydro to withhold information.

[5] Under s. 57(1) of FIPPA, BC Hydro has the burden of proving that s. 15(1)(l) applies to the information withheld. Under s. 57(2) of FIPPA, the applicant has the burden of proving that disclosure of the information in dispute would not be an unreasonable invasion of third-party personal privacy under s. 22(1) of FIPPA.[1]

## DISCUSSION

[6] **Background –** In August 2015, a windstorm caused widespread power cuts throughout British Columbia. An unprecedented number of customers attempted to obtain information about the disruption of service through a BC Hydro website, and this caused the site to crash. The systems that support the website generated over 1000 emails in response to the crash.

[7] **Information at Issue –** The information in dispute is the personal information of some of BC Hydro's employees and customers in addition to information about the software programs that BC Hydro uses to manage its website. This information is contained in 1,347 emails of 1665 pages that a contracted employee sent and received over three days. Most of the emails in question were system-generated relating to the crash of the website.

[8] In its submission to this inquiry, BC Hydro provided a list of all emails but copies of only some of the emails. It did not indicate why it had produced just the list and excluded most of the emails that were responsive to the request, rather than providing all the responsive records.

[9] When the Registrar of Inquiries notified BC Hydro that it had not delivered many of the records, BC Hydro responded that this failure to produce all the responsive records was owing to an oversight. It provided the remaining records

[1] However, the public body has the initial burden to show that the information it is withholding under s. 22(1) is personal information: Order 03-41, 2003 CanLII 49220 (BC IPC) at paras. 9-11.

after having applied the exceptions to disclosure line by line. It also requested an opportunity to provide additional submissions regarding the content of the emails that originally it had failed to produce. The Registrar of Inquiries granted the request and invited the applicant to respond to the submissions. Along with its supplemental submission, BC Hydro also provided to the applicant, for the first time, a copy of the severed records that it had previously failed to produce.

### *Section 15(1)(l) – harm to a computer system*

[10] The relevant provision of s. 15(1) is as follows:

> 15 (1) The head of the 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 communications system.

[11] In this case, to rely on s. 15(1) BC Hydro must establish that disclosure of the information could reasonably be expected to harm its computer system. The "reasonable expectation of harm" standard is "a middle ground between that which is probable and that which is merely possible."[2] There is no need to show, on a balance of probabilities, that the harm will occur, if the information is disclosed, but the public body must show that the risk of harm is well beyond the merely possible or speculative.[3]

[12] BC Hydro asserts that it is reasonable to conclude that the disclosure of names of the systems, in combination with the other system-generated information that it has already disclosed, could threaten the security of those and other systems. It also argues that disclosure of the email addresses and other information of its customers would pose the same threat. With the support of an affidavit from its Manager, Cybersecurity Planning and Operations (Manager), BC Hydro explains that it manages the delivery of electricity to its customers using electronic systems, and these systems are connected to the website. Therefore, BC Hydro submits the relevant risk relates not only to the website but to the entire BC Hydro network, which could lead to a breach of customer data and disruption of the supply of electricity.[4]

[13] BC Hydro deposes that its systems have been subject to numerous attempted hacks and that it works continuously to protect its systems. It argues that the ability of a hacker to conduct a successful attack relates directly to the amount of information that the hacker possesses about the system. BC Hydro

---

[2] *Merck Frosst Canada Ltd. v. Canada (Health),* 2012 SCC 3 at para. 201.
[3] *Ibid* at para. 206. See also *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at paras. 52-54.
[4] BC Hydro's initial submission, para. 15.

uses layers of protection to prevent cyber attacks and keeps information about its systems as confidential as possible. This information is available to BC Hydro staff on a need-to-know basis. BC Hydro submits that a hacker could use information about the systems to identify potential weaknesses in those systems that the hacker could exploit to improve the chance of a successful attack.[5]

[14] To demonstrate the veracity of the existing threat, BC Hydro notes that one of its subsidiaries, Powertech Labs Inc, was subject to a ransomware attack in 2021. BC Hydro submits that a successful attack into BC Hydro's website could result in disruption of its systems by malicious code or suffering a denial-of-service attack or theft of customer data. For these reasons, the British Columbia Utilities Commission (BCUC) issued a bulletin in 2021 directing BC Hydro to mitigate its exposure and be vigilant in protection of its information and computer systems from cyberattacks.[6]

[15] The applicant highlights that the incident at issue occurred in 2015 and suggests that it is reasonable to conclude that BC Hydro has updated its systems since then. They assert that this would negate any risk of harm of the disclosure of this dated information at issue.[7] BC Hydro responds that, while there have been modifications to its systems since 2015, the same systems are still in place.[8]

### *Analysis*

[16] BC Hydro argues that disclosure of the name of its systems or the email addresses of its customers would increase the chance that unauthorized individuals could enter its systems. It submits that it has provided sufficient evidence to support its position through the affidavit of the Manager. BC Hydro asserts that it has provided arguments that disclosing information about the programs it uses would assist a hacker in identifying weaknesses that the hacker could exploit in ways that would increase the chance of a successful attack. BC Hydro submits that these arguments establish a direct connection between the disclosure of the information at issue and the anticipated harm.[9]

[17] Nevertheless, the evidence of the Manager is vague. He has not explained how this could happen, or how likely that would be. He has acknowledged that one of BC Hydro's subsidiaries has been the subject of a ransomware attack. However, he has not demonstrated how much the risk of a successful attack would increase because of disclosure of the names of the systems or customers at issue. BC Hydro is asking me to conclude that

[5] BC Hydro's initial submission, paras. 13-14.
[6] Affidavit of Manager, para. 18.
[7] Journalist's response submission, para. 5.
[8] BC Hydro's reply submission, para. 3.
[9] BC Hydro's reply submission, paras. 5-8.

disclosure could trigger a series of unknown events that ultimately could lead to unauthorized access to its systems. I find its submission consists of speculation unsupported by explanation or persuasive evidence.

[18] BC Hydro has provided a hypothesis that the disclosure of simply the name of a program or an email address of a customer will increase the risk of harm to its systems to a level sufficient to trigger the application of s. 15(1)(l). It has made a general assertion that any information about a system can give an individual assistance in conducting a successful attack. The affidavit evidence is equally vague. Moreover, UBC has not explained how knowing the name of a program or the email address of a customer would add anything to what a hacker may or may not know about how to break into a specific system or how knowing this information would otherwise make the system easier to infiltrate.

[19] The best I can discern from this is that BC Hydro is saying there are different programs available for it to use and they have different vulnerabilities of which some hackers would be aware. In which case, it might save such hackers time in probing the vulnerabilities of BC Hydro's systems to know which programs they were dealing with. This suggests that BC Hydro's systems have critical vulnerabilities that an experienced hacker would be able to exploit eventually given enough time. In addition, I believe BC Hydro to be saying that knowing the email address of a customer could assist the hacker in gaining access to the customer's account, which the hacker could use as an entry point into the larger system. Given my finding below that s. 22(1) applies to these email addresses, I do not need to make a finding with respect to s. 15(1)(1) about them. Therefore, my comments apply only to the other information BC Hydro has withheld.

[20] The appropriate legal test requires evidence of a connection between the disclosure of the information and the anticipated harm and for this connection to be rational and logical. BC Hydro did not explain the differences in the programs available for it to use or how knowledge about them can facilitate a successful attack, for example, by identifying the technical vulnerabilities and how hackers can exploit them. It submits that once the attacker has entered one system, they could find their way into others. However, it has not explained how in a technical sense this might occur in the circumstances of this case.

[21] These circumstances mirror those in Order F10-39 and Order F10-25[10]. In those cases, the adjudicators found that, while the disclosure of the name of software or a server might possibly assist a hacker in designing an attack that could result in unauthorized access to the systems, the mere possibility itself does not meet the appropriate test. There must be more that ties the disclosure of the information to a reasonable expectation that the envisaged harm will occur.

[10] Order F10-39, 2010 BCIPC 59 (CanLII); Order F10-25, 2010 BCIPC 36 (CanLII).

There must be an explanation of precisely how the disclosure of the information at issue would render these systems vulnerable to an attack.

[22] I note that the decision of Order F10-39 was upheld on judicial review.[11] Mr. Justice Bracken found that the adjudicator, as noted above, applied the appropriate test:

> [58] I am satisfied the Adjudicator's finding that the Ministry failed to establish a clear and direct connection between the disclosure of the withheld information and the alleged harm, falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and law.
>
> [59] There is an intelligible basis in the reasons for the decision. The Adjudicator informed the Ministry precisely what it lacked: concrete factors to demonstrate there was a reasonable expectation that sensitive government information would be "hacked" or otherwise compromised should the information in question be released.

[23] The fact patterns and arguments are almost identical here. BC Hydro has failed to elucidate the "concrete factor" necessary to establish that disclosure of the information at issue could reasonably be expected to cause its systems to be hacked or otherwise compromised. It has not established that the risk of harm in this case is more than speculative. Saying that disclosure might help hackers to identify vulnerabilities in the system is not enough without explaining what those vulnerabilities are and how hackers can exploit them.

[24] Moreover, from my review of the records at issue there is nothing apparent that is indicative of the risk of harm that BC Hydro envisages.

[25] Therefore, for the reasons above, I find that s. 15(1)(l) does not apply to the information about BC Hydro's information systems.

### *Section 22 – harm to third-party personal privacy*

[26] The proper approach to the application of s. 22(1) of FIPPA has been the subject of analysis in previous Orders. A clear and concise description of this approach is available in Order F15-03, where the adjudicator stated the following:

> This section only applies to "personal information" as defined by FIPPA. Section 22(4) lists circumstances where s. 22 does not apply because disclosure would not be an unreasonable invasion of personal privacy. If s. 22(4) does not apply, s. 22(3) specifies information for which disclosure

[11] *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner),* 2012 BCSC 875.

> is presumed to be an unreasonable invasion of a third party's personal privacy. However, this presumption can be rebutted. Whether s. 22(3) applies or not, the public body must consider all relevant circumstances, including those listed in s. 22(2), to determine whether disclosing the personal information would be an unreasonable invasion of a third party's personal privacy.[12]

[27] I have taken the same approach in considering the application of s. 22(1) here.

*Step 1: Is the information "personal information"?*

[28] Under FIPPA, "personal information" is recorded information about an identifiable individual, other than contact information. "Contact information" is "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual."[13]

[29] BC Hydro submits that the information at issue is personal information about identifiable individuals and that it is not contact information.

[30] I find that some of the information is medical information about identifiable employees and, therefore, it constitutes personal information.

[31] BC Hydro also applied s. 22(1) to profile IDs and email addresses of some of its customers and the BC Hydro account number of a third party working to resolve problems with the website. While not all email addresses include identifiable names, they are the email addresses associated with personal BC Hydro accounts. The information is clearly information about identifiable individuals and not contact information. I find that the information at issue is personal information in accordance with s. 22(1).

*Step 2: Does s. 22(4) apply?*

[32] BC Hydro argues that none of the provisions in s. 22(4) apply in this case. The applicant cites s. 22(4)(e) with respect to information about the position, functions or remuneration of a member of a public body. However, they provide no argument as to how this provision applies in this case.

[33] The information at issue about BC Hydro employees consists solely of the reasons for the absence of individuals. This does not constitute information about the position or functions of that individual. Therefore, s. 22(4)(e) does not apply.

---

[12] Order F15-03, 2015 BCIPC 3 (CanLII), at para. 58.
[13] FIPPA provides definitions of key terms in Schedule 1.

[34] The parties do not raise any other provision of s. 22(4) and none of them appear to me to apply. Therefore, I find that none of the information falls within s. 22(4).

*Step 3. Does s. 22(3) apply?*

[35] The relevant provisions read as follows:

> 22 (3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
>
> > (a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation,
> >
> > …
> >
> > (d) the personal information relates to employment, occupational or educational history,
> >
> > …
> >
> > (f) the personal information describes the third party's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness.

[36] BC Hydro asserts that some of the information at issue relates to employment history, as it consists of information about absences from work. This includes information inserted in an employee's signature block.[14] The applicant does not contest this point.

[37] Having reviewed the record, I agree with BC Hydro's description of the information at issue. I find that s. 22(3)(d) applies and that disclosure of the information at issue would be presumed to be an unreasonable invasion of the third party's personal privacy.

[38] In its reply submission, BC Hydro also raises, for the first time, the application of s. 22(3)(a) with respect to absences for medical reasons. While the information does not reveal specific diagnoses, it does include medical history and medical treatment information. Having reviewed the information at issue, I agree with BC Hydro that some of the information relates to medical history. I note that BC Hydro has released the information about there being a medical appointment but withheld the name of the individual to whom the reference to that appointment refers.

[39] I find that s. 22(3)(a) also applies and that disclosure of some of the information at issue would be presumed to be an unreasonable invasion of the third party's personal privacy.

---

[14] BC Hydro's initial submission, paras. 28-29.

[40] In its additional submission, BC Hydro submits that s. 22(3)(f) applies to the customer account information of a third party, including their balance owing.

[41] I find that s. 22(3)(f) applies to the customer account information of the third party because it reveals their financial information.

*Step 4: Do the relevant circumstance in s. 22(2) rebut the presumption of invasion of privacy?*

[42] The relevant provisions are these:

> 22 (2) In determining under subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether
>
> > (a) for the purpose of subjecting the activities of the government of British Columbia to public scrutiny.
> >
> > …
> >
> > (f) the personal information has been supplied in confidence,

[43] **Section 22(2)(a) public scrutiny –** The purpose of s. 22(2)(a) is to provide that, where disclosure of records would promote accountability of a public body, this may in some cases support a finding that the release of third party personal information would not constitute an unreasonable invasion of personal privacy.[15]

[44] The applicant cites s. 22(2)(a) as a relevant circumstance in this case. They assert that because the email box at issue belongs to a contractor to BC Hydro, disclosure of all the information in their email box is necessary for the purpose of scrutinizing the activities of BC Hydro.[16] They do not describe how disclosure about the absences from work of other employees or the email addresses of customers would serve the purpose of holding BC Hydro to public scrutiny. BC Hydro points out that the information at issue is not about the contractor to whom the applicant refers.

[45] For s. 22(2)(a) to apply, the disclosure must have the potential to serve the public purpose of scrutiny of the activities of the public body. I see no evidence before me that an individual's occasional absences from work is an important issue or any other reason why disclosure would serve the purpose of subjecting BC Hydro to public scrutiny. The same applies with respect to the email addresses of its customers.

---

[15] Order F05-18 2005 BC IPC 24734 (CanLII), para. 49.
[16] Journalist's response submission, para. 9.

[46] Therefore, I find that s. 22(2)(a) is not a relevant circumstance in this case arguing in favour of disclosure.

[47] **Section 22(2)(f) supplied in confidence –** BC Hydro asserts that the employees and customers concerned provided their information at issue in confidence. It is information that the employees sent to other employees to inform them about their absences, and they did so in confidence.[17]

[48] BC Hydro has not provided evidence to support its position that the employees supplied this information in confidence. For example, with respect to the information in the employee's signature block, it has not provided proof that the employee only used this signature block for communications with colleagues. There is no confirmation that this information was never disclosed outside of their circle of colleagues. Nor is there any indication from the employee that he was providing this information in confidence.

[49] With respect to the email addresses of the customers, BC Hydro has not provided evidence to support its contention that the customers provided their information in confidence.

[50] Therefore, I have insufficient evidence to satisfy me that this information was supplied in confidence. I find that s. 22(2)(f) is not a relevant factor in this case.

[51] **Other relevant circumstances –** When BC Hydro provided severed versions of the missing documents, it applied s. 22(1) to profile IDs and email addresses of some of its customers and the BC Hydro account number of a third party working to resolve problems with the website.

[52] Previous orders have found that personal contact information of individuals, such as telephone numbers and email addresses, is their personal information and that information relates to their private lives.[18] As the information relates to their private lives, I find this is a circumstance that favours withholding the information.

***Conclusion on s. 22(1)***

[53] The parties do not argue the application of any other relevant circumstances in this case, and I find that none apply here.

[17] BC Hydro's initial submission, para.31.
[18] See for example F09-23, 2009 BCIPC 10 (CanLII) and F21-03, 2021 BCIPC 3 (CanLII).

[54] I found above that the information in dispute constitutes personal information. I have found that none of the provisions in s. 22(4) apply that would have excluded the application of s. 22(1).

[55] I find that some of the personal information constitutes the employment history of the third parties, in accordance with s. 22(3)(d) and that its disclosure is presumed to be an unreasonable invasion of third-party personal privacy. I also find that some of the information constitutes medical history in accordance with s. 22(3)(a) and the disclosure of the identity to whom that refers is presumed to be an unreasonable invasion of privacy.

[56] I find that the personal email addresses of customers and the account number and balance of one customer is information that relates to their private lives, which favours withholding the information.

[57] I find that none of the relevant factors in s. 22(2) apply to rebut the presumption that disclosure would be an unreasonable invasion of privacy. I also find that the applicant did not make a case that disclosure of this personal information would not be an unreasonable invasion of privacy.

[58] In conclusion, I find that s. 22(1) applies to the personal information at issue and BC Hydro must withhold it.

## CONCLUSION

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

1. Under s. 58(2)(a), subject to item 2 below, I require BC Hydro to give the applicant access to all the information it withheld under s. 15(1)(l).

2. Under s. 58(2)(c), I require BC Hydro to refuse access, under s. 22(1), to the personal information it withheld under s. 22(1).

[60] Pursuant to s. 59(1) of FIPPA, BC Hydro must comply with this order by December 31, 2021.

November 19, 2021.

**ORIGINAL SIGNED BY**

Jay Fedorak, Adjudicator

OIPC File No.: F17-71234