Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Order F17-54

CITY OF VANCOUVER

Chelsea Lott
Adjudicator

November 15, 2017

CanLII Cite: 2017 BCIPC 59
Quicklaw Cite: [2017] B.C.I.P.C.D. No. 59

Summary: A journalist requested that the City of Vancouver disclose its contract with a company for voting software and voter data storage. The City disclosed the contract except for the physical location of computer servers and their corporate operators under s. 15(1)(l) (harm to security of property or system). The adjudicator held that the City was not authorized to withhold the information.

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

Authorities Considered: B.C.: Order F14-45, 2014 BCIPC 48 (CanLII); Order F15-03, 2015 BCIPC 3 (CanLII); Order F11-14 2011 BCIPC 19 (CanLII); Order F09-13, 2009 CanLII 42409 (BC IPC).

Cases Considered: *Prassad v. Canada (Minister of Employment and Immigration)*, [1989] 1 SCR 560 (SCC); *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 (CanLII).

INTRODUCTION

[1] This inquiry involves the request by a journalist for access to a contract between the City of Vancouver (City) and Comprint Systems Inc. doing business as DataFix (DataFix). The City provided the applicant with a copy of the contract but withheld portions pursuant to ss. 15(1)(l) (harm to security of property or system) and 21(1) (harm to third party business interests) of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

[2] The applicant requested the Office of the Information and Privacy Commissioner (OIPC) review the City's decision. During mediation, the City released further information to the applicant, but continued to rely on s. 15(1)(l) to withhold information in the contract. Therefore, the applicant requested that the matter proceed to an inquiry. The City and the applicant provided submissions for the inquiry.

ISSUE

[3] The issue to be decided in this inquiry is whether the City is authorized to refuse to disclose the requested information under s. 15(1)(l) of FIPPA. Section 57 of FIPPA provides that the burden is on the City to prove that the applicant has no right of access to the information it is withholding.

DISCUSSION

Preliminary matter – late submissions

[4] The applicant did not provide his response submissions until six weeks after his deadline to respond and did so only when prompted by the Registrar of Inquiries.[1] The City points out that its request for a time extension to provide its own submissions was rejected by the OIPC.[2] The City submits that the applicant should have been held to the same standard. It says that in the circumstances, I should not accept the applicant's late submissions.

[5] The OIPC has the discretion to control its own procedures subject to any restrictions imposed by FIPPA and procedural fairness.[3] The timelines for submissions are set by the Registrar of Inquiries. Parties should respect the timelines and not assume that they can be disregarded with impunity. However, the City does not point to any actual prejudice that it suffered due to the applicant's delay. The City had an opportunity to respond to the applicant's submissions. In addition, the applicant's delay has been to his own prejudice because it has delayed the outcome of this inquiry which he requested. As a result, I deny the City's request.

Background - DataFix

[6] DataFix provides election data management services to municipalities across Canada.[4] Its software provides election officials with electoral information

[1] City of Vancouver Director of Access to Information affidavit at Exhibit B.
[2] *Ibid* at Exhibit A.
[3] See *Prassad v. Canada (Minister of Employment and Immigration)*, [1989] 1 SCR 560 (SCC) at p. 568-569.
[4] DataFix affidavit at paras. 2-3.

including the ability to correct voter lists and to access voter counts needed for electoral planning.[5]

[7] In 2014, the City and DataFix entered into an agreement for DataFix to provide voting software and to store voter data for the City's municipal election (the Contract).[6]

Information in dispute

[8] The City has disclosed the entirety of the Contract to the applicant except for the locations of the primary and backup servers that stored voter data during the term of the Contract and the names of the companies that operated those servers.

Section 15(1)(l)

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

> 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

[10] Section 15(1)(l) requires that the specified harm "could reasonably be expected to" occur. The appropriate standard of proof for provisions containing this test was set out by the Supreme Court of Canada in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)* as follows:

> 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": *Merck Frosst*, at para. 94, citing *F.H. v. McDougall*, 2008 SCC 53 (CanLII), [2008] 3 S.C.R. 41, at para. 40.[7]

[5] *Ibid* at para. 4.
[6] *Ibid* at paras. 4-5.
[7] 2014 SCC 31 (CanLII) at para. 54.

[11] I will apply the above approach to determine if the City is authorized to withhold information pursuant to s. 15(1)(l).

[12] The City says that disclosing information about the facilities which house servers would harm the security of the facilities and servers because it would:

1) remove a layer of the defence in depth strategy;
2) make these facilities targets for criminal activity;
3) open the facilities to social engineering attacks; and
4) allow attackers to compare the security precautions for the primary and backup servers and target the location thought to be less secure.[8]

[13] In my view, this list indicates that the harm which DataFix is ultimately trying to prevent is unlawful access to the facilities and servers. DataFix's list describes ways unlawful access would be facilitated by disclosing the location of the facilities.

[14] The City relies on affidavit evidence from the Chief Technology Officer of DataFix. DataFix states that voter data is "highly sensitive" and a target for criminal activity.[9] It says that stolen voter data could be used to interfere with ongoing or future elections.

[15] DataFix explains that it has a multi-layered approach to secure voter data which relies on physical and technical security approaches, which it terms a "defence in depth strategy."[10] DataFix states that removing one of its security approaches would "decrease the overall security level."[11] DataFix explains that keeping the server location confidential between it and its customer is a security measure.[12]

[16] DataFix's believes that the following mischief could occur by disclosing the information:

> …These addresses have stringent physical security precautions but, for a dedicated attacker, knowledge of the address could provide additional means to initiate social engineering attacks focusing on employees at these facilities. Additionally, knowing the addresses of both the primary and back-up servers would allow an attacker to compare the security precautions at both locations and target the location determined to be less secure.[13]

[17] The City relies on previous orders which have held that s. 15(1)(l) applies to information which would allow or assist third parties to gain unauthorized

[8] City initial submissions at para. 17(F).
[9] DataFix affidavit at para. 6.
[10] *Ibid.*
[11] *Ibid*.
[12] *Ibid* at para. 7.
[13] DataFix affidavit at para. 9.

access to a computer system or weaken the security of a computer system.[14] However, in my view, those orders are distinguishable. In Order F14-45, the information consisted of:

> …the names of databases and systems, user IDs, passwords, identifiers associated with the level/role/access authorization for obtaining specific data, system URLs that reveal details about a database, user account names, and the identifiers or names for various database tables that would enable one to query the databases for specific types of data….[15]

[18] In Order F15-03, the information was described as being about a computer system's operational information, specifically network configuration, security settings, and protocols for internal and remote communications.[16] In both orders, the adjudicators concluded the information would help potential computer hackers attack a computer system. Neither of those orders dealt with the physical location of servers.

[19] I note that the physical location of servers, as well as their names and model numbers, were found in Order F11-14 to not be subject to s. 15(1)(l).[17]

[20] In order for s. 15(1)(l) to apply, there must be evidence of a connection between disclosure of the information and the anticipated harm, that is well beyond or considerably above a mere possibility. In my view, the evidence in this case does not meet that threshold.

[21] It is uncertain whether voter data will continue to be held on these servers. The voter data which was obtained pursuant to the Contract is no longer stored on the servers identified in the Contract. The information was destroyed following the 2014 election in accordance with the terms of the Contract.[18] DataFix has other data storage facilities, but states that it expects to use the same server facilities again, and (at the time of submissions) it was in negotiations with the City for an agreement to support a municipal by-election.[19] However, there is no certainty that DataFix will use the same servers in the future or that the City will contract with DataFix for future elections.

[22] The City argues that knowledge of the locations could make employees at these facilities targets of "social engineering attacks." However, the City does not explain what it means by social engineering attacks or how knowing the identity of employees at these facilities would enable those attacks.

---

[14] Order F14-45, 2014 BCIPC 48 (CanLII) at para. 33; Order F15-03, 2015 BCIPC 3 (CanLII) at paras. 17-18.
[15] Order F14-45, *supra* at para. 33.
[16] Order F15-03, *supra* at para. 16.
[17] 2011 BCIPC 19 (CanLII) at para. 22.
[18] DataFix affidavit at para. 9.
[19] DataFix affidavit at para. 8.

[23] The City also argues that the facilities where the servers are physically located could become targets for criminal activity. They do not say what they mean by this, but I assume it to mean that the building could be unlawfully accessed and this could result in mischief, vandalism or theft. It states that criminals could compare security precautions between the primary and backup server facilities and target the less secure location. The assertions by DataFix, without more, do not convince me that disclosing the locations would measurably decrease the physical security of the facilities. Further, DataFix describes the facilities as having stringent physical security precautions. I do not accept that disclosing their physical locations would make unlawful access considerably more likely than a mere possibility.

[24] There is a strong public interest in transparency in relation to contracts involving public services delivered by private contractors and the risk of harm under s. 15(1)(l) must be sufficient to outweigh that public interest.[20] The City has not satisfied me that the security of the primary and backup server facilities or the server computer system itself could reasonably be expected to be harmed by disclosure of their location or the names of the companies which operate them. Therefore, I find the City is not authorized to refuse the applicant access to this information pursuant to s. 15(1)(l).

CONCLUSION

[25] For the reasons given above, pursuant to s. 58 of FIPPA:

I require the City to give the applicant access to the information it has withheld under s. 15(1)(l) of FIPPA by December 29, 2017. The City must concurrently copy the OIPC Registrar of Inquiries on its cover letter to the applicant, together with a copy of the records.

November 15, 2017

ORIGINAL SIGNED BY

Chelsea Lott, Adjudicator

OIPC File No.: F15-60677

[20] Order F09-13, 2009 CanLII 42409 (BC IPC) at para. 15.