

Order F22-12

# **ISLANDS TRUST**

Jay Fedorak Adjudicator

March 2, 2022

CanLII Cite: 2022 BCIPC 14 Quicklaw Cite: [2022] B.C.I.P.C.D. No. 14

**Summary:** An applicant requested records relating to a bylaw complaint against his property. The Islands Trust (Trust) disclosed records to the applicant but withheld some information under s. 15(1) (harmful to law enforcement) and s. 22(1) (unreasonable invasion of privacy). The adjudicator found that the Trust had correctly applied ss. 15(1) and 22(1).

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

# INTRODUCTION

[1] A property owner (applicant) made a request under the *Freedom of Information and Protection of Privacy Act* (FIPPA) to the Islands Trust (Trust) for records relating to a bylaw complaint involving his property. He requested a copy of the original complaint, photographs, bylaw officer notes and any reports that the planner had made. The Trust responded by disclosing records while withholding some of the information under s. 15(1)(d) (harm to law enforcement) and s. 22(1) (unreasonable invasion of privacy).

[2] The applicant subsequently requested the Office of the Information and Privacy Commissioner (OIPC) review the Trust's decision to withhold the information under ss. 15(1)(d) and 22(1).

[3] Mediation failed to resolve the matter and the applicant requested that it proceed to an inquiry. The Trust subsequently disclosed further records to the applicant and applied s. 14 (solicitor-client privilege) to some of the information. After the OIPC issued the Notice of Inquiry, the Trust disclosed further information and ceased to rely on s. 14.

### ISSUES

[4] The issues to be decided in this inquiry are:

- 1. Whether s. 15(1)(d) authorizes the Trust to withhold information; and
- 2. Whether s. 22(1) requires the Trust to withhold information.

[5] Under s. 57(1) of FIPPA, the Trust has the burden of proving that s. 15(1)(d) applies to the information withheld. Under s. 57(2) of FIPPA, the applicant has the burden of proving that the disclosure of the information in dispute would not be an unreasonable invasion of the personal privacy of the third parties under s. 22(1) of FIPPA.<sup>1</sup>

### DISCUSSION

[6] **Background –** The Trust received information that the applicant was about to cut down and remove some trees from his property. Bylaw officers subsequently visited the property on multiple occasions and spoke with the applicant. These conversations were adversarial in nature. The applicant expressed objections to the presence of the bylaw officers on his property.

[7] **Records at issue –** The records at issue include the bylaw complaint consisting of emails and attachments (seven pages) and a bylaw officer's notes (one page). The information at issue consists of passages in the records that the Trust submits could identify third parties.

### Section 15(1) – harm to law enforcement

- [8] The relevant provision of s. 15(1) is 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
    - •••
    - (d) reveal the identity of a confidential source of law enforcement information.
- [9] FIPPA defines "law enforcement" as follows

### "law enforcement" means

- (a) policing, including criminal intelligence operations,
- (b) investigations that lead or could lead to a penalty or sanction being imposed, or

<sup>&</sup>lt;sup>1</sup> 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, 2002 BCIPC 49220 (CanLII), paras 9-11.

(c) proceedings that lead or could lead to a penalty or sanctions being imposed.

[10] The Trust submits that bylaw enforcement officials compiled the information in the records during an investigation into alleged bylaw infractions.<sup>2</sup> It asserts that the investigation is ongoing and that it requires the assistance of the complainant. It believes that the complainant would cease to assist the investigation, if it disclosed the identity of the complainant to the applicant.<sup>3</sup>

[11] The Trust submits that it treats in confidence all reports of alleged bylaw infractions. It states this explicitly on its website, where it commits to protecting the confidentiality of any information that individuals provide concerning a reported infraction. It also promises to use this information solely for the purpose of investigating the complaint.<sup>4</sup>

[12] It states that the name and email address of the complainant appear multiple times in the records. It adds it has withheld other information in the records that, if disclosed, would enable the applicant to infer the identity of the complainant.<sup>5</sup>

[13] The applicant submits that he knows the identity of the complainant and that, therefore, there is no justification for continuing to withhold the information in the record. He includes in his submission the name and email address of a third party whom he believes to be the complainant. He also submits that it is not plausible for a bylaw investigation to still be ongoing relating to these complaints. They concern activities that took place several years ago and, according to him, the legal timeline for issuing Bylaw Violation Warning Notices or Bylaw Violation tickets has expired. To date, he had not received notices, tickets or stop work orders for any of the alleged violations. He does acknowledge receiving tickets for other violations that occurred after the Trust received the complaint at issue.<sup>6</sup>

### Analysis

[14] To assess whether disclosure of the information at issue would reveal the identity of a confidential source of law enforcement information in accordance with s. 15(1)(d), I must determine the following:

- 1. Whether the information in dispute relates to law enforcement;
- 2. Whether disclosure would reveal the identity of the source of law enforcement information; and

<sup>&</sup>lt;sup>2</sup> The Trust's initial submission, para. 24.

<sup>&</sup>lt;sup>3</sup> The Trust's initial submission, paras. 25 and 27.

<sup>&</sup>lt;sup>4</sup> The Trust's initial submission, para. 29.

<sup>&</sup>lt;sup>5</sup> The Trust's initial submission, paras. 32-33.

<sup>&</sup>lt;sup>6</sup> Applicant's response submission, pp. 1-3, Appendix, pp. 3 and 5.

3. Whether the source is a confidential source.

### Does the information in dispute relate to law enforcement?

[15] The Trust submits that the information at issue relates to ongoing investigations under the following bylaws:

- 1. Salt Spring Island Land Use Bylaw No. 355 (1999)
- 2. Salt Spring Island Official Community Plan Bylaw No. 434 (2008)
- Salt Spring Island Local Trust Area Soil Removal and Deposit Regulation Bylaw No. 418 (2008)<sup>7</sup>

[16] The Trust submits that the Salt Spring Island Local Trust Committee (Trust Committee) enacted these bylaws. The Trust Committee is a form of local government for Salt Spring Island whose statutory authority is the *Islands Trust Act* (ITA).<sup>8</sup> The Trust Committee forms part of the Trust.

[17] The ITA s. 16 gives the Trust Committee the authority to approve bylaws. The ITA s. 28 gives the Trust Committee the authority to enforce its bylaws with the same powers as a regional district board under the Local Government Act (LGA).

[18] The Trust submits that the Trust Committee instituted the bylaws at issue in accordance with its authorities to create bylaws under the ITA and the LGA.<sup>9</sup>

[19] The Trust provides evidence from its Legislative Services manager and FOI Head that the bylaw investigations at issue remain active.<sup>10</sup>

[20] The applicant does not contest the validity of the bylaws. He questions, however, whether the Trust properly enforced the bylaws.<sup>11</sup>

[21] The issue I must determine is whether the information relates to law enforcement. It is clear that it relates to matters subject to a municipal bylaw. The next question is whether the enforcement of the bylaws at issue in this case constitute "law enforcement". The relevant provision in the definition of "law enforcement" is whether the enforcement of the bylaws constitute an investigation that leads or could lead to a penalty or sanction being imposed.

[22] The information relates to the removal of trees from the applicant's property and the sifting of soil. There is reference in Bylaw No. 355 s. 4.4.5 to a possible requirement for a permit prior to removing vegetation from a property. There is also a reference to requirements for vegetation screens in s. 3.4. I note

<sup>&</sup>lt;sup>7</sup> The Trust's supplemental submission, p. 2.

<sup>&</sup>lt;sup>8</sup> Islands Trust Act [RSBC1996] Chapter 239.

<sup>&</sup>lt;sup>9</sup> The Trust's supplemental submission, p. 3.

<sup>&</sup>lt;sup>10</sup> Appendix to the Trust's supplemental submission.

<sup>&</sup>lt;sup>11</sup> Applicant's supplemental submission, p.1.

that s. 2.5.1 of the bylaw stipulates that "every person who commits an offence against this Bylaw is liable, upon summary conviction, to a fine and penalty not exceeding five thousand dollars and the costs of prosecution". The Trust has demonstrated that the investigations at issue relate to bylaws that the Trust Committee approved under its statutory authority. It has identified the relevant bylaws.

[23] Therefore, an investigation of Bylaw No. 355 could lead to a penalty being imposed and qualifies as "law enforcement" under FIPPA. Whether the bylaw actually applies in this case is not relevant. It is enough that the investigations relate to possible violations of the bylaw.

[24] The applicant's questioning of the credibility of bylaw enforcement does not invalidate the bylaws at issue or the fact that the complainant provided their personal information as part of an investigation of the bylaw. The information relates to removal of trees and treatment of soil. The bylaws at issue relate to these matters.

[25] Therefore, I find that the information relates to matters subject to a bylaw, which qualifies as law enforcement. My finding is consistent with previous Orders that have found that investigations in complaint-based regulatory and other types of law enforcement and bylaw enforcement proceedings constitute "law enforcement".<sup>12</sup>

# Would disclosure reveal the identity of the source of law enforcement information?

[26] It is clear from the face of the records at issue that the complainant sent communications to an official of the Trust and an employee of the Ministry of Environment of the Government of British Columbia. The purpose of these communications was to report evidence and allegations of activities that were relevant to matters concerning Trust bylaws. Trust officials subsequently commenced an investigation and visited the site. As I have found bylaw enforcement in this case to constitute law enforcement for the purposes of FIPPA, I find that the complainant is a source of law enforcement information.

[27] The information at issue includes the name and other identifying information about the complainant, as well as contextual information that could enable the applicant to infer the identity of the complainant. Therefore, disclosure of this information would reveal the identity of the complainant who is a source of law enforcement information.

<sup>&</sup>lt;sup>12</sup> The Trust's initial submission, para. 23, Order 00-01, 2000 BCIPC 9670 (CanLII). See also Order F21-40, 2021 BCIPC 48 (CanLII).

## Is the source confidential?

[28] The Trust has provided evidence that it treats bylaw complaints in confidence. The applicant does not refute this point, other than to indicate that he believes he already knows the identity of the complainant. As noted above, he identifies the name and the email address of the person he believes to be the complainant and asserts that there is no longer a need for confidentiality and the Trust should disclose the information in the record.

[29] The mere fact that the applicant states that he knows the identity of the complainant does not affect the application of s. 15(1)(d). The issue is whether there was an understanding of confidentiality between the public body and the source of law enforcement information. In this case the Trust has demonstrated that it receives bylaw complaints in confidence.

[30] Therefore, the complainant in this case qualifies as a confidential source of bylaw enforcement.

# Conclusion on s. 15(1)(d)

[31] I have found that the information at issue relates to law enforcement. As the details of the information that the complainant provided to the Trust relates to law enforcement, the complainant qualifies as a source of law enforcement information. Finally, I have found that the complainant was a confidential source.

[32] The Trust withheld the name and email address of the complainant and I find that s. 15(1)(d) applies to that information. The Trust withheld other information on the grounds that disclosure of that information would enable the applicant to infer the identity of the complainant. I agree that disclosure of the information withheld could enable the applicant to infer the identity of the complainant to infer the identity of the complainant, so s. 15(1)(d) applies. For example, some of the details the complainant provided would reveal information associated with the complainant, as would the names of the individuals who were copied on the emails of the complaints.

[33] As I have found that s. 15(1)(d) applies to all of the information withheld, I do not need to make a finding with respect to s. 22(1). Nevertheless, I will make a finding, as s. 22(1) is a mandatory exception.

## Section 22(1) – unreasonable invasion of privacy

[34] The proper approach for the application of s. 22(1) of FIPPA has been the subject of analysis in previous Orders. Order F15-03 provides a clear and concise description of this approach, 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 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.<sup>13</sup>

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

### Step 1 – Is the information "personal information"?

[36] 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."<sup>14</sup>

[37] The Trust submits that the information at issue is personal information and not contact information. The applicant disagrees. He states that none of the information at issue is personal information. He asserts that the names and email addresses of all third parties constitute contact information. He also states that while disclosure of the information at issue would reveal the identity of the complainant, the fact that he already knows the identity of the complainant means that the information is not personal information.<sup>15</sup>

[38] The fact that the applicant believes that he already knows the identity of the complainant does not change the personal nature of the information. The name and address of an identifiable individual are personal information, unless they constitute contact information. In this case, the names and email addresses at issue do not constitute contact information. Such information constitutes contact information only where it enables the individual to be contacted at a place of business. All of the email addresses at issue are personal email addresses, not business email addresses being used for business purposes.

[39] Therefore, I find that the information at issue is recorded information about identifiable individuals and not contact information in accordance with s. 22(1). Consequently, I find it to be personal information. I also find the contextual information withheld could reasonably be expected to identify the complainant and therefore constitutes his personal information.

<sup>&</sup>lt;sup>13</sup> F15-03, 2013 BCIPC 3, para. 58.

<sup>&</sup>lt;sup>14</sup> FIPPA provides definitions of key terms in Schedule 1.

<sup>&</sup>lt;sup>15</sup> Applicant's response submission, first attachment, p. 1.

Step 2 – Does s. 22(4) apply?

[40] Neither of the parties raise the application of s. 22(4). I cannot find any of the provisions of the subsection that might apply. Therefore, I find that s. 22(4) does not apply in this case.

Step 3 – Does s. 22(3) apply?

- [41] The relevant provision reads as follows:
  - **22** (3) A disclosure of personal information is presumed to be an unreasonable invasion of the personal privacy of a third party if
    - (b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or continue the investigation

[42] The Trust asserts that s. 22(3)(b) applies in this case. It submits that the personal information at issue was collected as part of an investigation into a possible violation of law. In support, it cites Order 01-12, which held that the meaning of the term "law" in s. 22(3)(b) included local government bylaw enforcement. Therefore, it argues, disclosure is presumed to be an unreasonable invasion of the personal privacy of the third parties.

[43] The applicant does not contest the application of s. 22(3).

[44] As I noted above, the records relate to a complaint that initiated an investigation into a possible contravention of a bylaw. I have found that this investigation qualifies as law enforcement for the purposes of FIPPA.<sup>16</sup> Therefore, I find that the personal information at issue was collected as part of an investigation into a possible violation of law, in accordance with s. 22(3)(b). The disclosure of this information is presumed to be an unreasonable invasion of the personal privacy of the third parties.

Step 4 – Do the relevant circumstances in s. 22(2) rebut the presumption of unreasonable invasion of privacy?

- [45] 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 of the relevant circumstances, including whether

<sup>&</sup>lt;sup>16</sup> See above, paras. 15-25.

(a) The disclosure is desirable for the purposes of subjecting the activities of the government of British Columbia or a public body to public scrutiny

[46] The applicant believes that the email addresses in the complaint records belong to employees of the Trust. He asserts that, as employees, disclosure of their names and email addresses would not harm their personal privacy. He also submits that the disclosure of their names and email addresses are desirable for holding the Trust publicly accountable. He does not, however, explain how this disclosure would foster public scrutiny of the Trust.<sup>17</sup>

[47] The Trust made no comment on this provision in its submissions.

[48] The applicant has not persuaded me that this provision is a relevant circumstance in this case. The names and email addresses may not refer to employees of the Trust. The email addresses at issue are personal email addresses, unlike those of the recipients of the emails. In any event, the applicant has failed to demonstrate how disclosure of those names would assist the public in holding the Trust accountable. He does not explain what issue of accountability is at stake and how the mere disclosure of the name and email addresses of these third parties would assist the public in holding the Trust accountable.

[49] Therefore, I find that s. 22(2)(a) is not a relevant consideration in this case.

[50] **Other relevant circumstances –** The applicant submits that, as he already knows the identity of the complainant, there is no reason for the Trust to withhold the information at issue. The Trust responds that whether or not he knows the identity of the complainant, disclosure of the information is equivalent to disclosing the personal information at issue to the world. Therefore, it submits that it must protect the personal information from disclosure to other individuals.<sup>18</sup>

[51] Previous BC Orders have established that the fact the applicant already knows the personal information at issue can be a relevant circumstance weighing in favour of disclosure.<sup>19</sup> Nevertheless, this would only apply in cases where there is evidence that the applicant has definitive knowledge of personal information, such as having had access to the same information in another form or having submitted the information themselves. It does not apply when applicants are merely speculating about the identity of the individual whose information is at issue. The applicant has not demonstrated that he has definitive knowledge of the identity of the complainant in this case. He has merely provided an unsupported assertion.

<sup>&</sup>lt;sup>17</sup> Applicant's response submission, p. 3.

<sup>&</sup>lt;sup>18</sup> The Trust's reply submission, para. 3.

<sup>&</sup>lt;sup>19</sup> See for example, Order F21-40, Order F17-02, 2017 BCIPC 2 (CanLII), Order F20-26, 2020 BCIPC 31 (CanLII).

[52] Therefore, I find that the applicant's purported knowledge of the identity of the complainant is not a relevant circumstance in this case.

# Conclusion on s. 22(1)

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

[54] I have found that the personal information in dispute was collected and is identifiable as part of an investigation into a possible violation of law in accordance with s. 22(3)(b). Its disclosure is presumed to be an unreasonable invasion of the personal privacy of third parties.

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

[56] In conclusion, I find that that s. 22(1) applies to the information and disclosure would be an unreasonable invasion of the complainant and other third parties' privacy.

# CONCLUSION

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

- 1. I confirm the decision of the Trust to withhold the information at issue under s. 15(1).
- 2. I require the Trust to withhold under s. 22(1) the personal information that it withheld under s. 22(1).

March 2, 2022

ORIGINAL SIGNED BY

Jay Fedorak, Adjudicator

OIPC File No.: F19-81091