OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2024-001

March 27, 2024

Department of Environment and Climate Change

Summary: The Complainant filed a privacy complaint under the *Access to Information and Protection of Privacy Act, 2015* alleging that the Department of Environment and Climate Change had breached their privacy by disclosing their personal information without their consent when the Department copied a third party on an email to the Complainant. The Complainant submitted that this was contrary to the *Act.* The Commissioner found that the Department had breached the Complainant's privacy, commented on the assessment of risk arising from the breach and remedial measures taken by the Department, and made recommendations for improvement.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, SNL 2015, c A-1.2, sections 2 and 68.

BACKGROUND

[1] The Complainant filed a privacy complaint under the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) against the Department of Environment and Climate Change. In the complaint, the Complainant described how they had made an inquiry to the Department about certain environmental data related to a project in Newfoundland. An employee of the Department had replied to them in response to these inquiries, enclosing a substantial package of reports and other correspondence relating to the environmental data and to measures taken both by the third party proponent of the project and by government. That email was copied to an employee of the third party business, as well as to other government employees. The complaint is about the disclosure to the employee of the third party business.

[2] Our Office conducted an investigation of the complaint, and concluded that there had been a privacy breach. We asked the Complainant for further information in order to conduct a risk assessment. The Complainant did not provide a great deal of further information. Therefore, this Report is based on those facts that we have gathered and the conclusions that we consider reasonable, based on the information before us.

[3] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 44(4) of *ATIPPA, 2015*.

ISSUES

[4] There are three main subjects to be discussed in this Report:

1. Whether the actions of the Department constituted a breach of the Complainant's privacy;
2. The assessment of risk to the Complainant resulting from any breach; and
3. Whether the Department has taken remedial measures to prevent further breaches.

DECISION

Determination of Privacy Breach

[5] The email sent by the employee to the Complainant, and copied to the employee of the third party business, contained the following information:

- the Complainant's first and last names;
- the Complainant's email address;
- the fact the Complainant had made one or more inquiries about environmental data related to the third party's project and about measures taken; and
- the fact the Department had provided the Complainant with the response and attachments.

[6] The first issue, whether the actions of the Department constituted a privacy breach, is not in dispute. *ATIPPA, 2015* defines personal information in section 2(u) as recorded information about an identifiable individual, including the individual's name, address, or telephone number, and the individual's personal views or opinions. It is clear that the information disclosed was the Complainant's personal information.

[7] From that email message, a reader would know the Complainant's name and email address, and could deduce that they had some interest in the project and in the environmental data related to it. In addition, in the body of the email, the Department employee refers to the Complainant's "concerns with the project" although those concerns are not described.

[8] The *Act* goes on to provide, in section 68, that a public body may disclose an individual's personal information only in specifically limited circumstances, including, for example, with the individual's consent, for the purpose for which it was collected, or in compliance with the law. We have concluded that none of the circumstances listed in section 68 applies in the present case, and the Department agrees with that assessment. The Complainant's personal information was therefore disclosed in contravention of the *Act.*

[9] Section 64(4) of the *Act* requires a public body to file a privacy breach report with our Office detailing the nature of the breach and the remedial measures taken. The Department did so.

Assessment of Risk

[10] An important part of a privacy breach investigation is the assessment of risk to the individual resulting from the breach. Depending on the circumstances and the nature of the information that is improperly disclosed there may, for example, be a risk of embarrassment, of identity theft, or of other kinds of harm. Having concluded that the disclosure was a privacy breach, our next step is to determine the nature and extent of the risk. In making that assessment, there are several questions to be asked:

- What are the different kinds of risks that might be expected to flow from the particular breach?
- What is the severity of the impact that each kind of risk might be expected to have, if it happened?
- In each case, what is the likelihood that each kind of risk will actually happen?

[11] Once we have done that kind of assessment, we can identify measures that may need to be taken by the public body or by the individual to prevent serious risks from happening to the individual whose privacy has been breached, or at least to mitigate the effects. In addition, this can help to identify measures that should be taken by the public body to prevent or at least to reduce the likelihood of the breach happening again.

[12] It is difficult to complete a reliable risk assessment without detailed information. That is why we will ask a complainant for any additional information that they can provide that could help us determine the nature and extent of a risk resulting from a privacy breach. In their complaint and submissions, the Complainant has made a number of statements about the risk to which the Complainant states they are exposed.

[13] First, the Complainant is concerned that the Department has forwarded their concerns about the project directly to the third party business, or that the Department forwarded their "complaint against the project" to the third party. However, in our investigation we have found no evidence that was the case. The communication that the Department copied to the employee of the third party business was a new, freestanding email, not a reply to the Complainant's previous correspondence. It did not contain any complaint or any other communication from the Complainant attached to it, nor did it contain the Complainant's views or opinions, or any evidence that a complaint had been made beyond noting the

Complainant's "concerns with the project". It appears, therefore, that the personal information disclosed in this privacy breach was limited to what is summarized above.

[14] In their submission, the Complainant asks how many of their previous emails may have been forwarded by the Department to the third party proponent of the project. This is obviously a relevant question. However, there is no evidence that this was done on any other occasion. The Complainant subsequently made an access request for that information and the records provided to the Complainant and to our Office would appear to confirm that the only individuals to whom any of his other messages were copied were internal to government, and those disclosures appear to be appropriate.

[15] In their complaint and submissions, the Complainant states the disclosure has jeopardized the safety of their family and property. This is an extremely serious concern and in many cases might merit not only a complaint to our Office but also a police investigation. The Complainant, however, has not enlarged upon the basis for that concern. In our investigation we have not seen any evidence that would lead us to conclude that the Complainant's personal safety or that of their family or their property is likely to be at risk of harm as a result of the disclosure.

[16] That is not to say there is no risk at all. We cannot draw that conclusion. We have to be aware of the social context and we recognize that individuals or groups who have concerns about the impact, on their community or their property, of a significant commercial or industrial development have a right to inquire about such projects and to express those concerns. However, in speaking out, they may find themselves feeling quite vulnerable.

[17] If people engage in advocacy of a public nature, they may fear the reaction of those who are involved with the venture or otherwise stand to gain from it. They may also fear that government or other public bodies will somehow treat them unfairly in retribution for their actions. Whether these fears are well-founded, or simply subjective, may not be known until much later, but there is certainly a power imbalance at play under such circumstances.

[18] It is important that citizens be able to advocate to government decision-makers and regulators without fear of their identity being exposed in the community or exposed to corporate interests who support a project they may oppose. It must be the individuals themselves who decide when or if they wish to identify themselves, and under what circumstances. In a democratic society, privacy is essential for the same reason that governments and law enforcement should not use surveillance and facial recognition to identify people taking part in a lawful protest.

[19] However, based on the information before us, it appears that the kinds of risks in the present case would be limited to discomfort or embarrassment. It is not apparent that the disclosure of the specific information involved in this case could materially contribute to more serious risks such as identity theft or another kind of serious harm such as the Complainant has suggested.

[20] Therefore, again based on the information before us, we can only conclude that the severity of any harm resulting from this breach would be relatively low.

[21] Finally, we cannot make any prediction about how likely the occurrence of any harm would be, apart, of course, from the subjective discomfort that has clearly been experienced already by the Complainant.

Remedial Measures

[22] In every privacy breach investigation, one of our main goals is remedial: to help the public body find better ways of protecting people's privacy so that similar breaches do not happen in future. In the present case, it appears from all the evidence before us that it was an isolated occurrence.

[23] The Department advised that in the process of collecting the information to respond to the Complainant's inquiry, its employee who was processing the inquiry had email correspondence with the employee of the third party business, and then mistakenly included that individual on the reply to the Complainant. We are satisfied that it was an unconscious mistake, rather than a conscious misapplication of an existing policy or practice. We conclude

that the Department has learned from this mistake, and that Departmental staff have a heightened awareness of the need to be very careful, to avoid improperly or accidentally disclosing information about individuals to others who have no need to know it.

[24] In conclusion, we find that copying the email intended for the Complainant to the third party business' employee did constitute a privacy breach. On the evidence we have been able to gather, that breach has a relatively low risk of serious harm. We find that the Department has responded appropriately to the privacy breach, and that the remedial measures taken by the Department are reasonable and appropriate.

RECOMMENDATIONS

[25] Under the authority of section 76(2) of the *Access to Information and Protection of Privacy Act, 2015* I recommend that the Department of Environment and Climate Change review its existing policies and practices regarding the collection, use, protection and disclosure of personal information, and continue to improve staff awareness of privacy principles and practices in their daily work.

[26] As set out in section 78 of *ATIPPA, 2015*, the head of the Department of Environment and Climate Change must give written notice of his or her decision with respect to these recommendations to the Commissioner and any person who was sent a copy of this Report within 10 business days of receiving this Report.

[27] Dated at St. John's, in the Province of Newfoundland and Labrador, this 27th day of March, 2024.

Michael Harvey
Information and Privacy Commissioner
Newfoundland and Labrador