



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2012-001

September 27, 2012

Town of La Scie

Summary:

On January 19, 2012 the Office of the Information and Privacy Commissioner received a Privacy Complaint under the *Access to Information and Protection of Privacy Act* (“*ATIPPA*”) filed collectively by two individuals regarding the Town of La Scie (the “Town”). The Complainants stated that their personal information had been sent to one of the Complainants by a Town employee via a private message on a social media website (“Facebook”). The message was sent using the employee’s personal Facebook account. The Complainants alleged that their personal information was not adequately protected pursuant to section 36; was improperly used pursuant to section 38; and was improperly disclosed pursuant to section 39.

The Commissioner found that the disclosure of the Complainants’ personal information was not contrary to the *ATIPPA* as the message was sent only to the Complainants. The Commissioner found that the Facebook message was a use of the Complainant’s personal information and that the method by which this use was carried out (i.e. Facebook) did not meet the limitations set out in section 38(2) or standard of necessity required by sections 38(1)(a) and 40(b) of the *ATIPPA* and, consequently, amounted to an improper use of personal information. Finally, the Commissioner found that the personal information had not been adequately protected. The Commissioner also provided commentary on the use of social media by public bodies and concluded that outside of community matters, announcements and notices, social media websites should not be used by public bodies to collect, use or disclose personal information regardless of the mechanism of delivery. The Commissioner recommended that the Town create and implement policies and practices regarding the use of social media and ensure that privacy training is provided to all Town employees.

Statutes Cited:

Access to Information and Protection of Privacy Act, S.N.L. 2002 c. A-1.1, as amended, ss. 2(o), 36, 38(1), 38(2) and 40(b).

BACKGROUND

[1] On January 19, 2012 this Office received a Privacy Complaint on behalf of two individuals in respect of the Town of La Scie (the “Town”). The Complainants stated that their personal information had not been adequately protected, had been improperly used and had been improperly disclosed contrary to sections 36, 38 and 39 respectively of the *ATIPPA*.

[2] The Complainants described their complaint as follows:

Personal financial information was emailed to us via a Town of La Scie employee’s personal facebook account.

[3] On January 24, 2012 this Office contacted the Town to inquire into the policies, procedures and practices employed by the Town regarding the protection, use and disclosure of personal information and the circumstances surrounding the Complaint. The response received by this Office on January 30, 2012 from the Town confirmed that the Complainants were, in fact, contacted by a Town employee via Facebook; however, it was the opinion of the Town that this was not an improper collection, use or disclosure of personal information. The Town explained that the employee was “doing her job...trying to contact a customer...and we had no phone number.”

[4] The Town also explained:

[I]n the matter of Face Book that is password protected because the letter was written in the “in box” [where only the people with the password could read it. The letter [...] has been deleted and we will not be using a personal account anymore we have an account set up for the Town of La Scie.

[5] The Town also provided documentation in support of its position including a letter to the Complainants which indicates:

The Privacy Act Commissioner was contacted and he informed us that using face book either personal or the Town’s was not an invasion of your privacy.

and a note outlining the Town's conversations with a Privacy Analyst with the Department of Justice which states "*he informed me that we were not invading her privacy in any way because it was not being seen by the public.*" This conversation did not, in fact, occur with any member of my Office as stated by the Town but rather with an employee of the Department of Justice ATIPP Office; I will discuss this further below.

II DISCUSSION

[6] There are three issues to be determined in this investigation:

- i. Has a disclosure occurred which is contrary to the provisions of the *ATIPPA*?
- ii. Was the Complainants' personal information used by the Town in a manner which is authorized by the *ATIPPA*?
- iii. Was the Complainants' personal information protected by reasonable security arrangements?

[i] Has a disclosure occurred which is contrary to the provisions of the *ATIPPA*?

[7] Section 2(o) of the *ATIPPA* defines "personal information" as follows:

- (o) *"personal information" means recorded information about an identifiable individual, including*
 - (i) *the individual's name, address or telephone number,*
 - (ii) *the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,*
 - (iii) *the individual's age, sex, sexual orientation, marital status or family status,*
 - (iv) *an identifying number, symbol or other particular assigned to the individual,*
 - (v) *the individual's fingerprints, blood type or inheritable characteristics,*

- (vi) *information about the individual's health care status or history, including a physical or mental disability,*
- (vi) *information about the individual's educational, financial, criminal or employment status or history,*
- (viii) *the opinions of a person about the individual, and*
- (ix) *the individual's personal views or opinions;*

[8] The Facebook message, which was sent only to the Complainants, contains the personal information of the Complainants – names and information about the Complainants' financial and employment status and history. There is no evidence that the information was disclosed to parties other than the Complainants. I am therefore satisfied that no disclosure contrary to the provisions of the *ATIPPA* has occurred.

[ii] Was the Complainants' personal information used by the Town in a manner which is authorized by the *ATIPPA*?

[9] Section 38 of the *ATIPPA* states:

38. (1) A public body may use personal information only

- (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 40 ;*
- (b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or*
- (c) for a purpose for which that information may be disclosed to that public body under sections 39 to 42 .*

(2) The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

[10] Pursuant to section 38(1)(a) of the *ATIPPA* the use of personal information must be for the purpose for which that information was obtained or for a use which is consistent with that purpose in accordance with section 40. Section 40(b) makes a use consistent where such use is necessary to operate a legally authorized program of the public body:

40. *A use of personal information is consistent under section 38 or 39 with the purposes for which the information was obtained or compiled where the use*
[...]

(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

[11] As stated above, the Facebook message from the Town employee contained the personal information of the Complainants. This is a clear use of the Complainants' personal information. However, there was no need to communicate the personal information via Facebook. The Town had other methods for contacting the Complainants (e.g. mailing address). I have therefore determined that there has been an improper use of personal information because the Town chose to use a less than secure means of sending the Complainants' personal information when another more secure means was available. The choice to do so does not meet the standard of necessity required by section 40(b).

[12] Furthermore, even if Facebook was the only means available for the Town to contact the Complainants all that needed to be communicated was a request for the Complainants to contact the Town. This does not meet the limitation set out in section 38(2) and is also contrary to the Town's statutory obligations under the *ATIPPA*.

[13] Finally it is important to also note that in order to contact the Complainants the Town employee performed a search within Facebook using the name of one of the Complainants. There was no means for the Town to verify that the account to which the message was sent was, in fact, an account belonging to the Complainant; the information could easily have been sent to the account of a person with the same name. Additionally, the Complainant did not give permission to the Town to be contacted this way and there was no indication or confirmation that the Complainant actually had a Facebook account.

[iii] Was the Complainants' personal information protected by reasonable security arrangements?

[14] Section 36 of the *ATIPPA* states:

36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[15] Facebook is a social media website that is accessible from any computer or device which is capable of accessing the internet. In this sense, the use of Facebook by the Town employee may be akin to the removal of personal information from the Town office. This is further exacerbated by the use of the employee's own personal account to engage in this communication. From this perspective, the information must be protected in the same manner as used by other public bodies which allow for the removal of personal information from their facilities. When we have been asked to examine instances of these circumstances in the past, this Office prescribed multi-layered security arrangements such as encryption and clear policies and procedures. Other than a single password, Facebook itself does not offer any other method of protecting an individual's account. It is up to each individual account holder to bolster his/her computer security as a whole (e.g. securing their server, implementing layers of passwords, creating user computer accounts, etc.). Regardless, even where these arrangements are in place, it is the position of this Office that Facebook, and other social media websites should not be used by public bodies to collect, use or disclose personal information.

[16] It was disturbing and surprising to learn that a Town employee felt it was appropriate to use her own personal Facebook account to send personal information about private matters to citizens. Also, the Town's lack of policies surrounding communications with its citizens is disconcerting. The Town does not appear to have concerns about its use of personal information on social media websites. The Town has indicated that since this occurrence, it has created a Facebook account specifically for the Town, itself, rather than for its employees and it intends to use this account to carry out any communications it deems necessary.

[17] I feel the need to stress that the use of Facebook and other social media websites by public bodies for the purpose of communicating personal information is a practice this Office discourages. For the various security and identification issues outlined above, there is no way to ensure that personal information is properly protected on these websites. If an individual requests that

communications with a public body be carried out in this manner, the public body must first satisfy itself that the identity of the Facebook account holder is confirmed, and furthermore that express consent be obtained from the individual acknowledging that the privacy of the communication cannot be guaranteed. This applies regardless of whether the communication is sent from a personal Facebook account or a public body Facebook account. The Town's implied belief that the practice of communicating with individuals using a Town Facebook account rather than an individual employee account will prevent this issue from arising in the future is incorrect.

[18] There are numerous examples of privacy authorities in Canada and around the world, as well as the courts, dealing with the aftermath of people's assumptions about how private Facebook really is. Facebook is a great tool for municipalities to inform people about festivals, application deadlines, respond to inquiries about operating hours of facilities, etc., but it is not a means for municipalities to use or disclose personal information. No personal information should be collected, used or disclosed by a public body in any context via social media except as described above, and the collection and use of personal information through Facebook should be done minimally and only in compliance with the *ATIPPA*.

[19] Finally, I must address the Town's assertion that it spoke with the "The Privacy Act Commissioner" and a "Privacy Analyst" and was told that the relevant use of Facebook was not an invasion of privacy as the relevant information was not seen by the public. There exists, within the provincial Department of Justice, an Access to Information and Protection of Privacy Office. That office is charged with overseeing the implementation and coordination of the *ATIPPA* by providing education, training, leadership and advice to public bodies and their coordinators in respect of interpretation and administration of the *ATIPPA* and developing policy and procedures to be implemented and maintained in each public body. The ATIPP Office exists separately and distinctly from this Office - the Office of the Information and Privacy Commissioner. The Office of the Information and Privacy Commissioner is charged with upholding and overseeing compliance with the *ATIPPA*. At no time prior to the initiation of this Review did the Town communicate with this Office in relation to this matter.

[20] While the alleged statement of the ATIPP Office that the Complainants' personal information was not disclosed to the public is correct, there has in fact been a violation of the *ATIPPA*. The use of the Complainants' personal information went beyond what was necessary and the use of Facebook for this purpose meant that there were inadequate security measures in place. Both of these actions are contrary to the provisions of the *ATIPPA*.

III CONCLUSION

[21] I have reached the following conclusions:

1. The information contained in the Facebook message contained the Complainants' personal information. However, there is no evidence that the information was disclosed to parties other than the Complainants. Consequently, no disclosure contrary to the *ATIPPA* has occurred.
2. In respect of the use of the personal information, however, the mechanism by which the information was conveyed and the amount of information conveyed were inappropriate to achieve the desired purpose. The Town had other methods to contact the Complainants and communicate the information effectively and securely. Consequently, the Town did not meet its statutory obligations under sections 38(2) and 40 of the *ATIPPA*.
3. Facebook and any other form of social media are an inappropriate means to communicate and use personal information by public bodies. While the website may be password protected, there is no ability to ensure that other people cannot access the information once it is sent. Furthermore, the possibility to accidentally convey the information is very real (i.e. posting to a "wall" or other public forum instead of privately.) Finally, there are no means by which to confirm that the recipient of the disclosure is, in fact, the intended recipient. Facebook does not check nor is it able to confirm the identities of account holders in this manner. It is possible for someone to create an account in the name and likeness of someone else without consent. This is another means by which a private message could be inappropriately disclosed.

4. The divulgence of information from the Town to the Complainants was indeed the result of inadequate security arrangements and a failure by the Town to meet its statutory obligations under section 36 of the *ATIPPA*. The Town did not adequately protect the Complainants' personal information and, in fact, still believes the means by which the information was disclosed was reasonably secure. The actions of the Town employee were intentional and reasonable security measures coupled with further education, training and understanding of the purpose of those arrangements and the purpose of the *ATIPPA* could have prevented this situation.

IV RECOMMENDATIONS

[22] Based on the possibility of a serious privacy breach, and the lack of concern and apprehension on the part of the Town in using social media to communicate personal information, I recommend that the Town undertake further privacy training so that its employees and the members of Council can appreciate and understand the importance of the protection of privacy and the seriousness, significance and gravity of privacy breaches. The Town must also attempt to educate itself on the proper use of social media in the municipal context. The action which gave rise to this Complaint was intentional and may have been prevented had the individual involved had a better appreciation of privacy under the *ATIPPA*.

[23] Furthermore, I recommend that the Town insist that the employee remove from her personal Facebook account all personal information of all citizens compiled in the course of conducting work on behalf of the Town, including the personal information of the Complainants. This process should also be carried out by any other Town employee who has the personal information of other individuals contained within their Facebook account in connection with their duties with the Town.

[24] Finally, I recommend that the Town develop and implement policies and procedures governing its use of social media.

[25] The Town is requested to please respond to these recommendations within 30 days of receiving this Report.

[26] Dated at St. John's, in the Province of Newfoundland and Labrador, this 27th day of September, 2012.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador

