Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MR16-6

Innisfil Hydro Distribution Systems Limited (InnPower)

December 5, 2017

Summary: The Office of the Information and Privacy Commissioner of Ontario (IPC) was contacted by Innisfil Hydro Distribution Systems Limited (Innpower) to report a privacy breach under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). Innpower informed the IPC that the laptop of one of its contractors had been stolen from a university library and that the laptop contained the unencrypted personal information of its customers. Given that the unencrypted personal information was disclosed by way of a theft, the disclosure was not consistent with section 32 of the *Act*. This report finds that Innpower responded adequately to the breach.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56, as amended,* sections 2(1) and 32.

BACKGROUND:

[1] The Office of the Information and Privacy Commissioner of Ontario (IPC) was contacted by Innisfil Hydro Distribution Systems Limited (Innpower) to report a privacy breach under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). Innpower informed the IPC that the laptop of one of its contractors had been stolen from a university library and that the laptop contained the unencrypted personal information of its customers.

[2] Because Innpower had authorized the contractor to provide services to Innpower customers on its behalf, Innpower remained responsible for the safety and security of

its customers' personal information that was stored on the contractor's laptop.

[3] The personal information of Innpower customers on the stolen laptop consisted of names, addresses, copies of electricity bills, energy consumption information, and any type of energy assessment that had been completed. Innpower confirmed that the information on the laptop did not include any customers' financial or banking information.

[4] Innpower initially reported to the IPC that the stolen laptop contained the unencrypted personal information of 123 customers and one of its own employees. It later learned, however, that only nine of the 123 affected customers were Innpower customers. Further, the employee information contained on the stolen laptop consisted of business contact information for the employee and not his personal information.

ISSUES:

[5] The following issues were identified as arising from this investigation:

1. Is the information at issue "personal information" as defined by section 2(1) of the *Act*?
2. Was the disclosure of the information at issue in accordance with section 32 of the *Act*?
3. Has Innpower responded adequately to the breach?

DISCUSSION:

1. Is the information "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part:

> "personal information" means recorded information about an identifiable individual, including:
>
> > (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
> >
> > (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> (e) the personal opinions or views of the individual except where they relate to another individual,
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and
>
> (h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[6] For the purposes of the analysis that follows, I find that the contactor was an agent of Innpower, as it was an organization who was acting on Innpower's behalf, by providing services to its customers. Innpower agrees with this finding.

[7] According to Innpower, the contractor's laptop contained the following customer information: names, addresses, copies of electricity bills, energy consumption information, and any type of energy assessment that had been completed. Innpower confirmed that the information on the laptop did not include any customers' financial or banking information.

[8] Based on the information set out above, I find that the information at issue qualifies as "personal information" as set out under section 2(1) of the *Act*. Innpower does not dispute this finding.

2. Was the disclosure of the personal information in accordance with section 32 of the *Act*?

[9] Section 32 of the *Act* prohibits the disclosure of personal information unless one of the listed exceptions applies. In reporting this breach to the IPC, and throughout this investigation, Innpower has stated that the disclosure of its customers' personal information through theft of the unencrypted laptop was not in accordance with the *Act*. I agree and find that the disclosure of unencrypted personal information on the stolen laptop was not in accordance with section 32 of the *Act*.

3. Has Innpower responded adequately to the breach?

[10] When responding to a breach, there are a number of steps that the IPC recommends, including containment, notification, investigation and remediation.

[11] In response to this breach, Innpower immediately contacted security at the university campus where the laptop was stolen to report the theft and also filed a police report.

Notification

[12] In February 2016, Innpower provided written notification to the nine customers whose personal information had been breached. The IPC was also contacted and notified.

[13] As part of this investigation, I have reviewed a copy of the notification letters that Innpower sent to its affected customers. The information contained in these letters included details about the breach, including that the theft had been reported to the police, and that both the IPC and the Privacy Commissioner of Canada had been notified. These letters also provided affected customers with details about the type of personal information that was contained on the stolen laptop and the name and title of a senior staff member to contact if they had any additional questions. Innpower's letters also stated that it has implemented additional privacy measures in response to the breach.

Privacy Policies & Practices

[14] The privacy policy that Innpower had in place at the time of the breach stated that it "shall protect personal information with security safeguards appropriate to the sensitivity of the information". This policy also stated that the methods of protection of personal information that Innpower uses should include, "technological security, such as, the use of passwords and encryption."

[15] Innpower has confirmed that there are confidentiality clauses in all of its contracts with third-party companies whose employees have access to customers' personal information. Innpower has also stated that it requires its contractors to sign non-disclosure agreements.

[16] Innpower informed the IPC that the stolen laptop had two layers of password protection in place, but that the personal information stored on it was not encrypted. At the time of the breach, Innpower did not have a specific policy in place regarding the encryption of mobile devices.

Under the *Act*, section 3 of Regulation 823[1] states:

> Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

[17] By their very nature, mobile devices, such as a laptops and smart phones, are vulnerable to loss and theft. It is for this reason, together with the requirement under section 3 of Regulation 834 for an institution's head to put in place reasonable measures to protect records in his or her institution, that any personal information stored on mobile devices should be well secured. As stated in a 2012 Investigation Report by British Columbia's Information and Privacy Commissioner[2]:

> All information security procedures should recognize that the physical characteristics of these electronic devices require more extensive security protection, including encryption, when storing personal information on them. Mere password protection of a device does not create the same level of security as encryption.

[18] In the IPC's 2014 guidance document, *Safeguarding Privacy on Mobile Devices*[3], this organization stated: "Make sure that access to (personally identifiable information) on your mobile device is protected by strong login passwords and encryption."

[19] Through Innpower's response to the breach, it has gained a better understanding of the risks of personal information stored on mobile devices and appreciates that passwords alone are not enough to protect personal information. As a result, Innpower has created and implemented a Mobile Device Encryption Policy. It has also committed to asking its current contactors to encrypt their mobile devices. Going forward, Innpower will address the issue of mobile encryption with its contractors by including this requirement in all future contracts where the contactor will have access to the personal information of its customers.

[20] At the time of the breach, Innpower did not have a Privacy Breach Protocol in place. In response to the breach, however, it has created a Privacy Breach Protocol, which has been rolled out to all of its staff. This protocol sets out the definition of a privacy breach and outlines the steps that are to be taken in response to a breach, including containment, investigation, notification, and taking steps to prevent a similar breach from occurring in the future.

[21] On the issue of privacy training, all staff are now required to review Innpower's

---

[1] RRO 1990, Reg 261, s 3.
[2] https://www.oipc.bc.ca/investigation-reports/1246
[3] https://www.ipc.on.ca/wp-content/uploads/Resources/safeguarding-privacy-on-mobile-devices-e.pdf

privacy policies at the time of hire, and then annually thereafter. Innpower electronically monitors and follows up with all staff to ensure these reviews are completed.

[22] Based on my review, I am satisfied that Innpower has responded adequately to this breach.

CONCLUSIONS:

1. The information at issue is "personal information" as defined by section 2(1) of the *Act*.

2. The disclosure of the personal information was not in accordance with section 32 of the *Act*.

3. Innpower has responded adequately to the breach and accordingly, it is unnecessary for me to make any recommendations.

Original Signed by: December 5, 2017

Trish Coyle
Investigator