Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. MR09-35

Toronto Hydro Corporation

Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9188
TTY: 416-325-7539
http://www.ipc.on.ca

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **MR09-35**

INVESTIGATOR: **Mark Ratner**

INSTITUTION: **Toronto Hydro Corporation**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

DISCUSSION:

Summary of Commissioner-Initiated Investigation

On July 24, 2009, Toronto Hydro (Hydro) notified the Information and Privacy Commissioner/Ontario (IPC) of a privacy breach involving unauthorized access to their customer account billing records. Hydro advised the IPC that, on July 20, 2009, it discovered abnormal activity on its web-based electronic billing (e-bill) system. Specifically, it appeared that an unauthorized party was automating the creation and activation of new e-bill accounts on the site, and was also able to override password protections and access existing accounts. As a result, the unauthorized party was able to access electronic copies of the most recent bills of Hydro customers. I refer to this incident as the "e-bill breach".

Upon discovery, Hydro immediately shut down the e-bill component of its website and began an internal investigation. According to their log files, approximately 179,000 Hydro customer accounts had been subject to the unauthorized access. Due to the nature of the incident, Hydro believed that the unauthorized party most likely had access to a complete list of all Toronto Hydro account numbers. There are approximately 640,000 Hydro customers.

Based on the information provided by Hydro, the IPC immediately opened a privacy investigation file and initiated an investigation under the *Municipal Freedom of Information and Protection of Privacy Act*. Our investigation is focused on two related issues:

- the factors contributing to the e-bill breach; and

- the way in which the 640,000 Hydro account numbers were obtained.

Background Information

During the course of the investigation, IPC staff met with Hydro on a number of occasions and Hydro provided its position on the matter in writing. The following is based on information supplied by Hydro.

Hydro explained that the e-bill system was designed to permit Hydro customers to receive their Hydro bill electronically, rather than through the mail. Customers who were interested in this service were able to create and activate an e-bill account through a link on Hydro's web site. Once the e-bill account was activated, customers would be able to view their most recent Hydro bill over the internet by downloading a Portable Document Format (PDF) image of the bill.

At the time of the e-bill breach, it was possible for customers to sign up for the e-bill system by entering their Hydro account number. After entering the account number, the user would then be prompted to create a user name and password, and provide an e-mail address. An e-mail confirmation would be sent to any customers who signed up for the e-bill system. At the time of the e-bill breach, there were no measures in place to authenticate the user's connection with the account number entered.

Hydro explained that the only information that can be obtained from the e-bill system is the information contained on a Hydro customer's bill, which includes the customer's account number, meter number, the customer's name and address, electricity charges for the billing period, amount of the last bill, the amount of the previous bill, and any outstanding amount due.

Hydro further stated that the e-bill breach appeared to have been the result of an automated process, run in parallel, resulting in the compromise of more than 179,000 e-bill accounts over a two-day (weekend) period. The process then allowed the party to access the PDF images of the bills of Hydro customers whose accounts had been breached. Hydro noticed the breach because of suspicious activity on its e-bill system.

Hydro advised that, due to the sequencing of the account numbers employed by the exploit, it was likely that the unauthorized party had somehow gained access to a complete list of the account numbers of all Hydro customers.

Remedial steps taken by Hydro

In order to address these incidents, Hydro confirmed that it was taking a number of steps. In addition to notifying the IPC, Hydro indicated that it had provided the Toronto Police Service (the Police) with details about the incident. Hydro also explained that it had launched an internal investigation into the matter, and stated that it had retained an external IT investigator to assist with its investigation. Hydro explained that the IT investigator would be mandated to:

- Examine Hydro's information systems to determine the cause and extent of unauthorized access to the e-bill system; and

- Determine the method by which the customer account numbers were obtained by a third party.

Hydro also stated that it would be notifying the public, including all Hydro customers of the privacy breach.

On July 23, 2009, Hydro sent a letter to all of its customers advising that the name, address, account number and amount of the last bill of some of its customers had come into the possession of a third party that was not associated with Toronto Hydro.

The letter advised customers of Hydro's concern that some of the information obtained may be used to fraudulently contact customers in order to obtain further personal information or money. The letter cautioned that customers should not provide any personal information in response to such calls, and should report the calls to Hydro's Customer Care department. The letter also stated that Hydro was taking the matter seriously, was launching an investigation, and was notifying the appropriate authorities. The letter was signed by Hydro's President and CEO.

In addition to the letter, on July 28, 2009, Hydro issued a press release, which contained information similar to that contained in the letter.

Hydro also informed the IPC that it has disabled the process through which users were able to set up e-bill accounts online. While customers with existing e-bill account profiles would still be able to view their bills online, customers are not able to create new e-bill accounts.

Hydro indicated that, at some point in the future, it would be removing the restriction on the creation of new e-bill accounts. When this restriction is removed, in conjunction with recommendations made by the IT investigator, Hydro stated that it intends on implementing a new procedure for creating e-bill accounts. The specific measures recommended by the IT investigator are addressed below.

Results of the Investigation

As noted above, the IPC's investigation centred on two separate, but related incidents: (1) the e-bill breach, and (2) the original compromise of the account numbers of Hydro customers. I will address the results of each investigation in detail below.

E-bill breach

As discussed above, the e-bill breach came to Hydro's attention as a result of unusual and suspicious activity on Hydro's e-bill portal system. Hydro investigated further and discovered that a party had been using an automated process to create and activate new e-bill accounts and to gain unauthorized access to Hydro account information. In total, approximately 179,000 unauthorized accounts had been set-up over the preceding two days.

Hydro's investigation revealed that the party was able to create and activate multiple unauthorized e-bill accounts simultaneously via rapid and simultaneous automated processes, and took steps to disguise its tracks and to avoid traceability.

Upon further investigation, Hydro was able to connect the unauthorized access attempts with an IP address linked to a Toronto-area computer. This information was provided to the Police, who executed a search warrant in the home connected to the IP address.

As a result of the search warrant, the Police seized a computer. The Police reviewed the computer's hard drive. Based on their findings, the Police proceeded to arrest the owner of the computer in connection with the e-bill breach.

Hydro advised our office that the Police investigation into this matter is continuing. According to Hydro, the Police are not aware of any subsequent use of the e-bill information.

As a result of its investigation into the matter, the external IT investigator retained by Hydro concluded that there were certain weaknesses in the log-in procedures to the e-bill system that allowed the unauthorized access to occur once the third party had access to the account numbers. As a result, the IT investigator recommended the following:

- Separate the creation of User IDs and passwords from their use;
- Passwords should be unique, complex and alpha numeric;
- E-mail address verification should be part of the account activation process;
- Before e-bill accounts are activated, an 'activation code' process should be implemented, with the activation code being provided to the customer via an alternate channel, such as postal mail; and
- To ensure the "liveness" of users, deployment of 'CAPTCHA' technology is warranted (*i.e.*, requiring users to enter characters appearing in a text box).

Compromise of Hydro Account Numbers

As discussed above, Hydro believed that the unauthorized party likely had access to a complete list of all Hydro account numbers. There are approximately 640,000 current Hydro customers. Hydro proceeded to investigate the way these account numbers, which were used to facilitate unauthorized access, may have been obtained by the third party.

After investigating, the external IT investigator concluded that there had not been an external security breach to Hydro's Customer Information System (CIS).

In order to determine how account numbers may have been obtained, the IT investigator considered which parties would have had access to these account numbers, and investigated whether a service provider could have been responsible for the breach. After investigating, the IT investigator concluded that a service provider could not have been the party responsible for the breach.

Hydro therefore focussed its investigation on potential internal sources of the breach. In doing so, Hydro instructed the IT investigator to address the circumstances surrounding the potential unauthorized disclosure of customer account numbers. In order to define the scope of this investigation, the IT investigator identified all of the Hydro employees that had the ability to access, and potentially extract, the complete list of Hydro account numbers.

The external IT investigator imaged the computer hard drives of each of the employees. The hard drives were examined for evidence that these employees had accessed, extracted, or printed the complete list of Hydro account numbers.

Based on its examination, the IT investigator concluded that there was no evidence that any of the computers that were subject to examination had been used to extract the complete list of Hydro account numbers.

The following issues were identified as arising from the investigation:

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,
>
> …
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the 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,
>
> …
>
> (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
>
> … .

This investigation concerns two separate privacy incidents: the e-bill breach, and the earlier compromise of Hydro account numbers. I will therefore consider whether the records at issue in both of these incidents contained personal information.

E-bill breach

The records that were accessible through the e-bill breach were electronic copies of customer bills in PDF format. Approximately 179,000 customer bills were accessed by the outside party. I have reviewed a sample copy of the record and note that it contains the customer's name, account number, address, amount charged for current billing period, amount charged for previous billing period, and amount of electricity used.

I am satisfied that the information contained in the record clearly qualifies as "personal information" under the *Act*.

Compromise of Hydro Account Numbers

As discussed above, Hydro has concluded that the e-bill breach was facilitated, in part, by an earlier compromise of the account numbers of all Hydro customers. The Toronto Hydro account number is a number that is unique for every Toronto Hydro customer.

The test to determine whether a given record contains personal information is whether it is reasonable to expect that an individual may be identified if the information is disclosed [Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 (C.A.)].

In this case, the disclosure of customer account numbers most likely enabled the party to access PDF copies of the bills, which included the names and addresses of customers. Therefore, the disclosure of the account numbers facilitated the disclosure of the identity of Hydro customers. Accordingly, I am satisfied that, in the circumstances of this case, it is reasonable to expect that an individual may be identified as a result of the improper disclosure of the customer account number.

I further note that subsection (c) of the definition of personal information states that personal information includes "any identifying number, symbol or other particular assigned to the individual …" In this case, a Hydro account number is an identifying number that is assigned to an individual, namely, the Hydro account holder in question.

Based on all of the above, I am satisfied that a Hydro account number qualifies as personal information.

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

Section 32 of the *Act* sets out a number of circumstances under which an institution may disclose personal information. None of these circumstances are present in this case, as personal information was disclosed inadvertently. Accordingly, I conclude that both the disclosure of the copies of the customer bills through the e-bill breach as well as the disclosure of the account numbers was not in accordance with the *Act*.

Did Hydro have adequate security measures in place at the time of the e-bill breach?

Section 3(1) of Ontario Regulation 823 made pursuant to the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

This provision requires that institutions implement measures to protect records in their custody. As there are two separate, but related matters under investigation in this case, I will address the security measures that were in place at the time of the incidents.

E-bill breach

At the time of the e-bill breach, Hydro stated that it had the following security measures in place:

- Intrusion detection and intrusion prevention systems which monitor and stop outside intrusion to Hydro's network;
- Firewalls;
- De-militarized zones;
- Web security tools designed to stop unauthorized access to restricted web pages;
- 24 hour, 7 day a week monitoring of its network; and
- Incident Management and response process teams

As discussed above, Hydro has explained that at the time of the incident, customers were able to set up e-bill accounts by entering a valid customer account number. Once the account number had been entered, the customer would be prompted to create a user identification and password. After completing this process, a customer would be able to view their bill online.

Hydro has stated that the Hydro bill information for Hydro customers is retained in a secure archived repository behind a protective firewall.

Hydro explained that, in some cases, the unauthorized party was able to override existing e-bill account protections and obtain control of the online accounts for those customers.

As noted above, in response to the e-bill breach, Hydro suspended the creation of new e-bill accounts. Hydro explained that when the system becomes active again, it will introduce additional security measure to prevent accounts from being set up through the use of automated processes. These additional measures include the requirement that users enter an activation code, which would be sent through the mail. In addition, the customers signing up for e-bill accounts would be required to manually enter characters in a special box which would prevent sign-up by automated scripts.

Compromise of Hydro Account Numbers

It is Hydro's position that account numbers may have been obtained through its internal Customer Information System (CIS). With respect to the CIS, Hydro has stated:

> Access to the system involves multiple levels of approval and is granted on a need to use basis to Toronto Hydro employees. The need for access for each employee is reviewed on an annual basis as part of Toronto Hydro's access governance practices. Toronto Hydro also has in place a mandatory Security Awareness Program which educates employees on an annual basis about security risks and policies and internal procedures to mitigate potential risks to information and systems.

Hydro has further stated that it is in the process of introducing a new CIS in early 2010, and that the new CIS will incorporate enhanced security protections.

Analysis

I have reviewed the information provided by Hydro regarding the security measures in place at the time of the e-bill breach, and I note that Hydro did have measures in place to protect the security of customer information. I further note that upon learning of the incident, Hydro took appropriate remedial steps to address the privacy breach. As discussed above, Hydro had intrusion detection systems in place at the time of the incident, and Hydro was able to identify the fact that an automated process had been employed, and that customer information had been potentially compromised.

However, notwithstanding the existence of these security measures, our investigation as well as the external IT investigation has revealed security shortcomings in some aspects of Hydro's security systems in place at the time of the e-bill breach.

When the e-billing function was set-up, it was designed to facilitate access by Hydro customers. The primary shortcoming is that Hydro permitted users to create e-bill account profiles by simply entering a valid account number. At the time of the e-bill breach, Hydro had not implemented measures to authenticate that the user accessing the system was the actual account holder, and had not adequately safeguarded against the potential deployment of automated processes. I am pleased that Hydro has acknowledged these shortcomings and has committed to improving security at the profile creation stage for its e-bill system.

In addition, I further note that, in some cases, the unauthorized user was able to exploit vulnerabilities in the e-bill software that allowed for passwords to be overridden, which permitted the unauthorized user to assume effective control over the account. Hydro has committed to correcting the flaw in the e-bill software coding before permitting the creation of new e-bill accounts.

With respect to intrusion detection, I note that in this case, the e-bill breach took place over a period of two days, and was only discovered when Hydro noticed unusual activity relating to the creation of new e-bill account profiles.

Based on this incident, I am of the view that Hydro should implement more robust intrusion detection mechanisms in the e-billing function than those that were in place at the time of the unauthorized access. Specifically, Hydro should implement additional mechanisms to detect and limit unusual online account activities, including repeated login attempts, multiple new account creation, account overrides, password resets, as well as the re-use of identifiers, such as e-mail addresses or IP addresses. Such steps can be implemented through logging and audit measures as well as enhancements to existing intrusion detection and prevention systems.

I also note that there are shortcomings with respect to Hydro's CIS, which is set up to allow certain employees to access account information for all customers. Although Hydro has stated that access to the CIS is only granted on a need-to-know basis, in my view, it is incumbent upon Hydro to critically examine the number of employees that have the permission to access customer account information of **all** customers in one list.

In addition, Hydro has also acknowledged that its CIS does not have a comprehensive audit function, which is troubling, and limits the ability of Hydro to investigate instances of improper access to customer account information.

Based on the security shortcoming identified above, I conclude that Hydro did not have adequate security measures in place at the time of the e-bill breach.

Conclusions

I have reached the following conclusions based on the results of my investigation:

1. The information disclosed as a result of the e-bill breach is "personal information" as defined under section 2(1) of the *Act*.

2. Individual customer account numbers are "personal information" as defined under section 2(1) of the *Act*.

3. The personal information disclosed as a result of the e-bill breach was not disclosed in accordance with section 32 of the *Act*.

4. Hydro had not implemented adequate security measures as required under section 3(1) of Regulation 823, made pursuant to the *Act*.

Other matters: The future of power provision requires SmartPrivacy

As discussed above, this investigation report has described shortcomings with respect to the design of Hydro's information security systems. As we progress into the future, it is incumbent that utilities such as Hydro ensure that privacy is built into all information technology systems to reduce the risk of similar incidents occurring in the future. One emerging technology is what is known as the "Smart Grid".

The provision of power is currently evolving to further increase energy conservation and efficiency. Infrastructure that includes smart meters are helping electrical providers move towards a "smarter" electrical grid that seeks to curb greenhouse gas emissions and reduce consumers' energy bills. A feature of this modernized electrical grid, or "Smart Grid," is the potential to collect much more detailed information on individual energy consumption use and patterns within the most private of places—our homes.

Instead of measuring energy use at the end of each billing period, smart meters will provide this information at much shorter intervals. This will increase the level of personal information detail available as well as the instances of collection, use and disclosure of personal information. Electric utilities and other providers may in the future have access to information about what customers are using, when they are using it, and what devices are involved. An electricity usage profile could become a source of behavioural information on a granular level. The privacy and security issues surrounding the future of power provision are therefore extremely important.

Our office recently published a paper on how to address Smart Grid privacy and security concerns titled *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*. SmartPrivacy represents a broad arsenal of protections, encapsulating everything necessary to ensure that all of the personal information held by an organization is appropriately managed. Privacy by Design is its *sine qua non*—those who fail to envision privacy requirements early in the development of technology, business practices or physical space and infrastructure will be less likely to provide comprehensive protection, despite the presence of the other elements.

The reason I highlight the Smart Grid in this investigation report is because the Smart Grid is only in its early stages of development, which is the perfect time to build SmartPrivacy into the Smart Grid. Security and privacy issues consistently appear where personal information is involved, such as in the provision of online features including the e-bill system, and will also be front and center regarding the Smart Grid. Consumer control of electricity consumption and consumer control of their personal information must go hand in hand. Doing so will ensure that consumer confidence and trust is gained, and that participation in the Smart Grid contributes to the vision of creating a more efficient and environmentally friendly electrical grid, as well as one that is protective of privacy. This will result in a positive sum (win-win) outcome, where both environmental efficiency and privacy may coexist.

Recommendations:

1. Hydro should implement measures identified by the IT investigator to enhance security at the e-bill account creation stage. The specific measures identified are:

    - Separate the creation of User IDs and passwords from their use;
    - Passwords should be unique, complex and alpha numeric;
    - E-mail address verification should be part of the account activation process;
    - Before e-bill accounts are activated, an 'activation code' process should be implemented, with the activation code being provided to the customer via an alternate channel, such as postal mail; and

- To ensure the "liveness" of users, deployment of 'CAPTCHA' technology is warranted (*i.e.*, requiring users to enter characters appearing in a text box).

2. Hydro should take appropriate measures to prevent, limit, and to otherwise detect the ability of employees to query and obtain complete Hydro customer lists through the CIS.

3. Hydro should put in place robust access controls and audit capabilities for all instances of access to customer account information among Hydro employees.

4. Hydro should put in place additional mechanisms to detect and limit unusual online account activities, including repeated login attempts, multiple new account creation, account overrides, password resets, and the re-use of identifiers, such as e-mail addresses or IP addresses. These measures can be implemented through logging and audit measures as well as enhancements to existing intrusion detection and prevention systems.

5. Hydro should repair—with a high degree of confidence—the e-bill software coding that allowed the unauthorized override of the password protections of existing e-bill account holders, and assume effective control of accounts. Toronto Hydro's remedial actions and degree of confidence shall be submitted to the IPC for approval.

6. On a quarterly basis, Hydro should provide a report to the IPC regarding policy and information technology systems enhancements and improvements designed to protect customer privacy. Given the increasing amount of customer personal information that will be collected by Hydro, this report should include updates on customer service program improvements including the introduction of Smart Meters and steps taken to link to the "Smart Grid".

By June 1, 2010, the institution should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations.

Original signed by: March 1, 2010

Mark Ratner
Investigator