Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F11-03

BRITISH COLUMBIA HYDRO AND POWER AUTHORITY

Elizabeth Denham, Information and Privacy Commissioner

December 19, 2011

Quicklaw Cite: [2011] B.C.I.P.C.D. No. 43
CanLII Cite: 2011 BCIPC No. 43
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/IR-F11-03.pdf

TABLE OF CONTENTS

EXECUTIVE SUMMARY

[1] There is considerable public concern about British Columbia Hydro and Power Authority's ("BC Hydro") initiative to replace meters currently in use with smart meters.

[2] BC Hydro is presently replacing the electro-mechanical and digital meters of its more than 1.8 million customers with new smart meters. Rather than measuring electricity consumption on a monthly or bi-monthly basis, as is currently the case, smart meters will provide BC Hydro with hourly information about customers' electricity consumption. As a result, analysis of our household consumption information may reveal more information about our daily lives.

[3] The Government of British Columbia passed a new *Clean Energy Act* in April 2010 that, among other things, requires BC Hydro to install smart meters across the province by the end of 2012 and a smart grid by the end of 2015. The intention is to ensure energy self-sufficiency at low rates through "a renewed commitment to smart meters and smart grids that will allow ratepayers to better manage their electricity use and save on power bills by taking advantage of new electricity pricing programs aimed at encouraging conservation and smart use of electricity during off-peak periods".[1] At this time, however, BC Hydro has said that it is not implementing a rate differential whereby the price of electricity is lower during off-peak hours. The British Columbia Utilities Commissioner would have to review and approve any new or modified rates.

[4] The media and citizens of British Columbia have raised various concerns about BC Hydro's Smart Meter and Infrastructure Initiative ("SMI"). The Office of the Information and Privacy Commissioner ("OIPC") received complaints and correspondence from approximately 600 individuals expressing privacy and security concerns, which prompted the Information and Privacy Commissioner ("Commissioner") to initiate this investigation. British Columbians are concerned about whether BC Hydro will properly protect information about their electricity consumption and whether the organization will improperly share their consumption information with third parties.

[5] Public concerns also include the cost of installing smart meters and their potential health risks. However, this report focuses on BC Hydro's obligations under the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), examining only privacy and security impacts of BC Hydro's new technology and

[1] Backgrounder, "New Act sets the Foundation for Three Areas of Priority", Government of BC, April 28, 2010.

the resulting increase in BC Hydro's ability to collect information about British Columbians' household activities.

[6] This report is limited to the roll-out of BC Hydro's SMI project to date. Although it makes some reference to the future state of SMI, the investigation focuses on the project's compliance with FIPPA in its current state and the privacy management framework in place to ensure ongoing consideration of privacy and security as the project continues to be implemented.

[7] The Commissioner found that BC Hydro is complying with FIPPA regarding the collection, use, disclosure, protection, and retention of personal information and that BC Hydro has taken reasonable steps to put in place an effective privacy management framework. However, the Commissioner found that BC Hydro is not complying with the requirement to notify customers of the purposes for collecting the personal information in relation to the SMI project, the legal authority for the collection, and providing the contact information for a person within BC Hydro who can answer questions regarding the collection.

[8] This report makes a series of recommendations[2] to address BC Hydro's noncompliance with the requirement to notify and to improve the organization's privacy and security governance. BC Hydro has committed to put in place action plans to address these recommendations. The OIPC will continue to monitor the SMI project to ensure that BC Hydro complies with the recommendations.

[9] As the SMI project moves forward, BC Hydro will offer its customers choices as to how they wish to implement features of the SMI project in their homes. The Commissioner advises customers to carefully consider the privacy implications of their choices with regard to the products they will purchase to try to reduce their electricity consumption.

PART I PURPOSE AND SCOPE OF THIS REPORT

INTRODUCTION

[10] British Columbia Hydro and Power Authority ("BC Hydro") is in the process of replacing the electro-mechanical and digital meters of its more than 1.8 million customers with new smart meters. Rather than measuring electricity consumption on a monthly or bi-monthly basis, as is currently the case, smart meters will provide BC Hydro with hourly information about its customers' electricity consumption. As a result, analysis of our household consumption information may reveal more information about our daily lives.

[2] See Appendix B for complete list of recommendations.

[11] The media and citizens of British Columbia have raised various concerns about smart meters. Our office received complaints and correspondence from approximately 600 individuals expressing privacy and security concerns, which prompted us to initiate this investigation. The citizens of British Columbia are concerned as to whether BC Hydro will properly protect their electricity consumption information and are worried that BC Hydro will improperly share their consumption information with third parties.

[12] There has also been a great deal of public concern regarding the anticipated cost of $930 million for BC Hydro's Smart Meter and Infrastructure Initiative ("SMI") and BC Hydro's overall business plan for the SMI project. Many citizens are also concerned about the potential health risks associated with smart meters' wireless technology. These issues are not within the Office of the Information and Privacy Commissioner's ("OIPC") mandate and we do not address them in this report.

[13] In this report, we will examine only the privacy and security impacts of BC Hydro's new technology and the resulting increase in the organization's ability to collect information about the household activities of British Columbians. This investigation focuses on BC Hydro's obligations under the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

[14] The Government of British Columbia passed a new *Clean Energy Act* in April 2010 that, among other things, requires BC Hydro to install smart meters across the province by the end of 2012. This measure is intended to ensure energy self-sufficiency at low rates through "a renewed commitment to smart meters and smart grids that will allow ratepayers to better manage their electricity use and save on power bills by taking advantage of new electricity pricing programs aimed at encouraging conservation and smart use of electricity during off-peak periods".[3] At this time, however, BC Hydro has said that it is not implementing a rate differential whereby the price of electricity is lower during off-peak hours.

[15] BC Hydro states that one of its major objectives for the SMI project is to provide customers with more information about their electricity consumption along with tools to help them manage their electricity use more efficiently. BC Hydro anticipates the SMI project will lead to reduced electricity consumption from its customers as well as improved power outage management and an increased ability to detect and reduce electricity theft.

[3] Backgrounder, "New Act sets the Foundation for Three Areas of Priority", Government of BC, April 28, 2010.

[16] This report is limited to the roll-out of BC Hydro's SMI project to date. It is an ongoing project and, while there are some references to the future state of SMI, our investigation is focused on the project's compliance with FIPPA in its current state and the privacy management framework in place to ensure ongoing consideration of privacy and security as the project continues to be implemented. Our office will continue to monitor future phases of the SMI project.

INVESTIGATION PROCESS

[17] Since July 2011, the OIPC received more than 600 complaints and correspondence from citizens regarding smart meters. We advised BC Hydro by letter dated July 28, 2011 that, pursuant to s. 42(1)(a) of FIPPA, we were investigating BC Hydro's SMI project to ensure compliance with privacy and security requirements of FIPPA.

[18] In August 2011, the OIPC provided BC Hydro with an extensive list of questions and requested copies of related documentation. We received a response from BC Hydro dated September 1, 2011. We subsequently contacted BC Hydro on numerous occasions with further questions. The OIPC also made a site visit to BC Hydro on September 22, 2011 to ask further questions and to perform an independent verification of select components of BC Hydro's privacy and security framework that have been implemented at this point.

[19] As part of our investigation, the OIPC conducted research on smart meters and the smart grid with a view to better understand the SMI project as well as how other jurisdictions in Canada and around the world are addressing the privacy and security issues.

APPLICATION OF FIPPA

[20] BC Hydro is a public body listed under Schedule 2 of FIPPA and is therefore subject to FIPPA. The Commissioner has a statutory mandate to monitor compliance of public bodies with FIPPA to ensure the purposes of the legislation are achieved. The purposes, as stated in s. 2(1) of FIPPA, are to make public bodies more accountable to the public and to protect personal privacy by, among other things, preventing the unauthorized collection, use or disclosure of personal information by public bodies.

[21] Our investigation of BC Hydro's SMI project was conducted pursuant to the statutory authority of the Commissioner under s. 42(1)(a) of FIPPA to conduct investigations and audits to ensure compliance with FIPPA.

BACKGROUND

Overview of BC Hydro

[22] BC Hydro is a provincial Crown Corporation established under the *Hydro and Power Authority Act*. BC Hydro is the primary provider of electricity to most of the province and the vast majority of the residents of British Columbia. In addition, BC Hydro supplies electricity to the province's commercial and industrial sector.

[23] BC Hydro's purposes are set out in the *Hydro and Power Authority Act*.[4] It must generate, manufacture, supply, acquire and dispose of power and related products. BC Hydro is also responsible for supplying and acquiring services related to these purposes.

Legislative Requirements for the SMI Project

[24] Sections 17(2) and (3) of the *Clean Energy Act*, when read in conjunction with the Smart Meters and Smart Grid Regulation made under that Act, explicitly require BC Hydro to install and put into operation smart meters and related equipment for its customers by the end of the 2012 calendar year. Section 17(4) of the Act and s. 4(1) of the Regulation require BC Hydro to install and put into operation a smart grid by the end of the 2015 calendar year.

[25] Under the Regulation, smart meters must be capable of recording measurements of electricity "at least as frequently as in 60-minute intervals".[5] Smart meters must also be capable of "transmitting information to and receiving information from an in-home feedback device".[6] In-home feedback devices include devices known as in-home displays, programmable thermostats and energy management systems. Some of these devices display the measurements of electricity supplied to a premises in real-time and, where configured to do so, the cost of that electricity.

[4] See s. 12(1.1).
[5] Smart Meters and Smart Grid Regulation, s. 2(d).
[6] Ibid., s. 2(g).

Smart Grids and Smart Meters

[26] Today's electricity grid is designed to support the one-way flow of electricity – from a central source to customers. The smart grid refers to the modernization of the current electrical grid to enable the two-directional flow of information and electricity. This two-directional flow provides the utility with more information about the use, voltage, and power quality of the electricity transmitted across the electricity grid. It also provides customers with more information as to how much electricity they use and when they use it. Smart grids start with automated smart meters and continue with automation of the rest of the power delivery system (*i.e.,* the grid). Devices on power lines, and at substations (transmission and distribution grid level), can be remotely monitored and controlled by the power supplier.

[27] Smart meters are one of many components that make up the smart grid. They provide two-way communication between the customer and BC Hydro, capturing the amount of electricity consumed on an hourly basis and reporting that hourly consumption to BC Hydro three times per day. Smart meters can automatically record and report electricity consumption information. Smart meters can also identify consumer consumption in far greater detail than a conventional meter and communicate that information back to the electricity distributor for monitoring of the electricity grid and customer billing purposes.

[28] BC Hydro states that it expects the SMI project will result in such operational efficiencies as:

- **Faster power outage restoration** – Smart meters will provide automated and instant notification of power outages. This will enable BC Hydro to restore power more quickly and to ensure all affected residences have power restored. At present, BC Hydro relies on notification from its customers of a power outage. Such notification will not be necessary once the smart grid is operational.

- **Reduced electricity theft** – BC Hydro believes it will be able to better identify energy diversions, reducing theft and mitigating safety issues for the public and BC Hydro employees. At present, BC Hydro estimates that the cost of energy theft is more than $100 million per year.[7]

[7] See Fact 3 at http://www.bchydro.com/news/press_centre/media_updates/smart_meter_facts.html.

ISSUES

[29] The issues in this investigation are:

1. Does BC Hydro have authority to collect personal information for the SMI project and has BC Hydro properly notified its customers about this collection? [ss. 26 and 27(2) of FIPPA]

2. Does BC Hydro have authority for its intended uses of its customers' personal information in the SMI project? [s. 32 of FIPPA]

3. Does BC Hydro have authority for its intended disclosures of personal information in the SMI project? [s. 33 of FIPPA]

4. Has BC Hydro taken reasonable steps to protect personal information within the SMI project? [s. 30 of FIPPA]

5. Does BC Hydro retain its customers' personal information in accordance with FIPPA? [s. 31][8]

[30] This report will also include an examination of BC Hydro's privacy management framework as it relates to the SMI project.

PART II SMART METERS AND SMART GRIDS

BC HYDRO'S SMI PROJECT

[31] BC Hydro is implementing the SMI project in phases. Each phase advances the project and introduces new hardware, software and process components. In the initial phase, which started in July 2011, BC Hydro began deployment of smart meters and related system components and updated some legacy software applications. Although BC Hydro started installing smart meters in July of this year, meter-readers are still going house-to-house to collect electricity consumption data for the purposes of billing. BC Hydro informs us that this practice will continue until at least the spring of 2012 when it will start to switch customers to billing from the automated meter reads. BC Hydro anticipates it will continue to manually read some customers' meters throughout 2012, until it has fully deployed the metering system.

[8] The relevant portions of ss. 26, 27, 30, 31, 32, 33 and 33.2 of FIPPA are set out in Appendix A.

[32] BC Hydro has configured smart meters to automatically collect household electricity consumption data on an hourly basis. This information will be transmitted from the smart meter to BC Hydro three times per day.

[33] The second phase, which started in October 2011, includes the implementation of the meter data management system ("MDMS"), which will collect and store the information collected from the smart meters.

[34] In the third phase, expected to begin in the spring of 2012, the MDMS will be in production and BC Hydro anticipates that customers will be able to access their hourly consumption data through the BCHydro.com customer portal.

[35] As part of the third phase, in the spring of 2013**,** BC Hydro anticipates that customers will be able to purchase compatible in-home feedback devices[9] to allow them to access more detailed consumption information if they so choose. In-home feedback devices will allow customers to see real-time energy usage as well as the projected billing resulting from their usage. This may help customers determine the impact on their electricity consumption of such things as unplugging an appliance or turning off a light. BC Hydro believes that in-home feedback devices will show customers how electricity consumption relates to cost and customers will consume less electricity as a result. BC Hydro states that it will not have access to such real-time consumption information.

[36] Future releases will include the introduction of load forecasting and theft detection.

[37] A challenge in this investigation has been that the full functionality of the SMI project is not yet in place. We have, however, attempted to gain as much insight as possible from BC Hydro about functional possibilities of the SMI project. BC Hydro informed us that:

- BC Hydro has no immediate plans to introduce time-of-use billing. Time-of-use billing involves charging different rates for electricity at different times of day. The goal of time-of-use billing is to offer financial incentives to encourage consumers to reduce electricity consumption during peak hours. By moving electricity usage to off-peak hours, utility providers can lower costs by limiting the building and operation of peak generating facilities. Peak generating facilities provide BC Hydro with the capacity to cover the highest peak demand during the day. BC Hydro states that if it considers introducing time-of-use billing in the future, it will only do so "after extensive public consultation and an independent

[9] BC Hydro informed us that in-home feedback devices are consumer products and not part of BC Hydro's distribution infrastructure. BC Hydro will not be selling these products, but may offer customers a rebate to help offset the cost.

regulatory review".[10] The British Columbia Utilities Commission would have to review and approve any new or modified rates.

- BC Hydro will collect information about in-home feedback devices to ensure the device selected by the customer is compatible with and can receive detailed aggregate consumption information from the meter. BC Hydro will not have access to the in-home feedback device and will not collect any information about or from individual appliances.

- BC Hydro plans to introduce functionality to notify customers (via email, text message, etc.) when they are close to reaching consumption targets. Customers would have to first consent to receiving such alerts.

- Individuals who own electric vehicles may, in the future, be able to purchase electricity from the smart grid for their vehicle and sell electricity back to the grid when the vehicle is not in use.

[38] The OIPC will continue to monitor these, and any other future developments of the SMI project, to help ensure that BC Hydro addresses the privacy and security risks.

Recommendation 1
As BC Hydro introduces new elements to the smart grid, or increases the functionality of existing elements of the grid, it should continue to complete privacy impact assessments in each instance and provide it to the OIPC for review and comment before implementation.

OTHER JURISDICTIONS

[39] Many other jurisdictions in Canada and around the world are either contemplating the introduction of smart meters and the smart grid or are further along than BC Hydro with implementation. We will look at Ontario and California and compare them, where appropriate, with how BC Hydro is implementing smart meters.

[10] See Fact 2 at www.bchydro.com/news/press_centre/media_updates/smart_meter_facts.html.

[40] Ontario adopted its smart meter policy in 2004 and is the first jurisdiction in North America to equip every home and small business with a smart meter.[11] As of October 31, 2011, more than 4.7 million smart meters have been installed in Ontario. As is the case in British Columbia, these meters report consumption data on an hourly basis.[12]

[41] California has moved forward with full-scale deployment of smart meters. There are four major electricity utilities in California that have installed millions of smart meters. Some of these meters report consumption data every 15 minutes, while most report consumption data on an hourly basis.

[42] Ontario and California have both introduced time-of-use billing to some of their customers, whereas to date BC Hydro has stated that it has no intention to introduce this style of billing. As of October 31, 2011, utilities in Ontario had switched more than 3.4 million customers to time-of-use billing.[13]

[43] The Information and Privacy Commissioner of Ontario worked with Ontario's largest electricity companies—Hydro One Inc. and Toronto Hydro—to ensure they were embedding strong privacy and security protections in Ontario's smart grid right from the start and at each step in the development of the smart grid. These steps include ensuring the electricity companies thoroughly addressed privacy and security in smart grid requirements, business process analysis and architectural designs.

[44] The introduction of smart meters in Ontario has been a much smoother process than it has been in California. This is likely due in part to the release of a greater amount of information to the citizens of Ontario about how the electricity companies were incorporating privacy and security into the smart grid and how these companies are protecting customer personal information.

[45] In California, on the other hand, the public has expressed concerns that electricity companies will share customer consumption data too broadly with third parties or even sell this information. The public is also concerned that companies are not properly securing customer personal information. In response to these and other concerns, on July 28, 2011, the California Public Utilities Commission ("CPUC") adopted rules intended to protect the privacy and security of customer consumption data generated by smart meters.[14] By doing so, California became the first state to adopt specific rules regarding the privacy and

---

[11] See http://www.ieso.ca/imoweb/pubs/smart_grid/Smart_Grid_Forum-Report-May_2011.pdf for much of the information in this paragraph.
[12] See OEB Monthly Monitoring Reports at http://www.ontarioenergyboard.ca/OEB/Industry/Regulatory+Proceedings/Policy+Initiatives+and+Consultations/Smart+Metering+Initiative+(SMI)/Smart+Meter+Deployment+Reporting.
[13] Supra, Note 11.
[14] See http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf.

security of consumption information generated by smart meters. In British Columbia, BC Hydro must follow practices that are compliant with FIPPA.

PART III COMPLIANCE WITH FIPPA

COLLECTION OF PERSONAL INFORMATION

Personal Information Collected

[46] In the operation of the SMI project, BC Hydro states that it plans to collect hourly electricity consumption information. BC Hydro currently collects electricity consumption data monthly or bi-monthly.

[47] BC Hydro also collects other customer profile information from its customers (*e.g.,* name, address, phone number) in order to establish and maintain an account for provision of services. However, this is not a new collection related to the SMI project. Further, there will be no changes to the collection of this information due to the SMI project.

[48] "Personal information" is defined in Schedule 1 of FIPPA as "recorded information about an identifiable individual other than contact information".[15] As part of the SMI project, BC Hydro will be recording hourly electricity consumption information about each of its customers. BC Hydro's customers are "identifiable individuals". As such, I find that hourly electricity consumption information is personal information of BC Hydro's customers as defined in Schedule 1 of FIPPA.[16]

[49] Given the current state of the smart grid in British Columbia, it is not reasonable to expect that an analysis of hourly consumption information would reveal exactly what appliances are being used and when. However, it could reveal whether people are home or away. Beyond that, any other conclusions would be merely speculative.

[15] See definitions in Schedule 1 of FIPPA.

[16] See also *R. v. Gomboc*, 2010 SCC 55. The main issue before the Court in *Gomboc* was whether information gathered using a digital recording ammeter to monitor power usage in a home could survive *Charter* scrutiny. The Court also looked at whether consumption information was personal information in the context of the *Charter*. Five of the nine judges found that consumption information constituted personal information. The Court discussed the capabilities of smart meters at para. 40.

Issue 1 – Does BC Hydro have authority to collect personal information for the SMI project and has BC Hydro properly notified its customers about this collection? [ss. 26 and 27(2) of FIPPA]

[50] Section 26 of FIPPA sets out the purposes for which a public body may collect personal information. Section 26(a) – (c) states:

> 26 A public body may collect personal information only if
>
> (a) the collection of the information is expressly authorized under an Act,
>
> (b) the information is collected for the purposes of law enforcement,
>
> (c) the information relates directly to and is necessary for a program or activity of the public body.

[51] Some members of the public have shared with our office their concern over the increased frequency of collection of electricity consumption information that will take place with the implementation of smart meters. However, s. 2(d) of the Smart Meters and Smart Grid Regulation of the *Clean Energy Act* provides that smart meters must be capable of recording measurements of electricity "at least as frequently as in 60-minute intervals". As such, there is express statutory authority under s. 26(a) of FIPPA for the collection of hourly electricity consumption data.

[52] I find that BC Hydro's collection of personal information for the SMI project complies with s. 26 of FIPPA.

Notification

[53] Section 27(2) of FIPPA requires that when BC Hydro collects personal information for the SMI project directly from an individual, it must ensure that it states:

- the purposes for collecting their personal information,
- the legal authority for the collection, and
- the contact information for the person within BC Hydro who can answer questions regarding the collection.

[54] BC Hydro states that it provides notification to its customers through three methods: its Call Centre messaging system; on its website; and on paper bills sent to customers. In addition, before installing smart meters in a particular neighbourhood, BC Hydro provides each customer with a brochure about the SMI project and its most salient feature, the new smart meter.

[55] We have reviewed these methods of notification and I find that while they do provide some general information on the SMI project, they are inadequate with respect to the specific notification requirements of s. 27(2) of FIPPA. They do not state the purposes for BC Hydro's collection of personal information, the legal authority for collection or the contact information for the person within BC Hydro who can answer questions regarding collection.

[56] I find that BC Hydro's notification to individuals does not comply with s. 27(2) of FIPPA.

Recommendation 2

BC Hydro must develop more comprehensive web pages and paper notices for its customers for the SMI project regarding the purposes for collecting hourly electricity consumption data, the legal authority for collection, and the contact information for the person within BC Hydro who can answer questions regarding the collection.

Use of Personal Information

Issue 2 – Does BC Hydro have authority for its intended uses of its customers' personal information in the SMI project? [s. 32 of FIPPA]

[57] Section 32 of FIPPA sets out when a public body may use personal information. It reads as follows:

> 32 A public body may use personal information in its custody or under its control only
>
> (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),
>
> (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or
>
> (c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

[58] BC Hydro has informed us that the only use of customer profile information relative to the SMI project is to enable the smart meter installation process through creating field work orders using customer and premise information. Once BC Hydro installs smart meters, it will use consumption

information captured and stored in the smart meter systems to maintain the service-for-payment relationship with its customers. This is the purpose for which BC Hydro obtained or compiled the information and thus this use complies with s. 32(a) of FIPPA.

[59] We understand from BC Hydro that future secondary uses of smart meter system data may include the use of consumption information for BC Hydro customer conservation initiatives.

[60] No secondary use of personal information collected within the SMI project is occurring today. However, for guidance to BC Hydro and to the public, the requirements under FIPPA[17] for a secondary use to be consistent with the original purpose for collection is that it must have a reasonable and direct connection to the original purpose and it must be necessary for performing the statutory duties of BC Hydro or for operating a legally authorized program of BC Hydro. Alternatively, BC Hydro must obtain written consent from its customers in relation to the information BC Hydro intends to use, including specifying how the personal information may be used.

[61] I find that BC Hydro's use of personal information, as currently contemplated, complies with s. 32 of FIPPA.

Recommendation 3
Before any future secondary uses of electricity consumption information take place, BC Hydro should complete a privacy impact assessment and provide it to the OIPC for review and comment prior to implementation.

Disclosure of Personal Information

Issue 3 – Does BC Hydro have authority for its intended disclosures of personal information in the SMI project? [s. 33 of FIPPA]

[62] Section 33 of FIPPA limits the permitted disclosures of personal information by a public body. It reads as follows:

> 33 A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3.

[17] See ss. 32 and 34 of FIPPA as well as s. 6 of the Protection of Privacy Regulation.

[63] Unauthorized disclosures are prohibited [FIPPA, s. 30.4].

[64] BC Hydro states that by default, it will not disclose or share a customer's profile or consumption information with any third party unless a customer formally requests it to do so or where BC Hydro is compelled to do so by law.

[65] Authorized disclosures include those that are for a use that is consistent with the purpose for which the personal information was initially collected [FIPPA, s. 33.2(a)]. Other relevant authorities for disclosure include to an officer or employee of BC Hydro if the information is necessary for the performance of the duties of the officer or employee [FIPPA, s. 33.2(c)] and where disclosure is made to a law enforcement agency in Canada to assist with a specific investigation [FIPPA, s. 33.2(i)]. BC Hydro also looks to disclose personal information in accordance with other statutes (*i.e., Safety Standards Act*) that authorize or require its disclosure [FIPPA, s. 33.1(1)(c)] as well as to collect amounts owing to BC Hydro [FIPPA, s. 33.1(1)(i)].

Internal Disclosures / Access Control Policy

[66] Disclosure of personal information from BC Hydro to its employees for purposes relating to the SMI project is authorized where it is necessary for the performance of the employees' duties [FIPPA, s. 33.2(c)]. BC Hydro should only disclose the information necessary for these employees to perform their duties.

[67] The personal information at issue in the SMI project is electricity consumption information and customer profile information. The more frequently consumption information is provided to utilities such as BC Hydro, the greater the potential that an analysis of this information may reveal whether people are home or away.

[68] The more employees of BC Hydro who have access to customers' consumption information, the greater the risk that this information will be inappropriately accessed for wrongful purposes or disclosed to individuals who seek some sort of insight into the activities of BC Hydro's customers. It is imperative that BC Hydro put in place measures to mitigate this very real risk.

[69] As such, BC Hydro must institute an access control policy that reflects the "need-to-know" and "least privilege" principles. The Information Management and Information Technology Management section of the Core Policy and Procedures Manual of the BC Government[18] defines these principles as follows:

[18] See http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm.

> *Need-to-Know*
>
> A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office.
>
> The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on all information systems.
>
> The need-to-know principle is especially important in protecting the privacy of individuals as required by the *Freedom of Information and Protection of Privacy Act*.
>
> *Least Privilege*
>
> A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use.

[70] In accordance with these principles, BC Hydro's access control policy must determine, for each user, the transactions that the user can make and the data fields that the user can access or update.

[71] BC Hydro must assign roles based on the tasks and services the user provides. The role must reflect the actual services the user is delivering, or supporting the delivery of, to BC Hydro's customers. Roles must also include information technology ("IT") administration.

[72] BC Hydro has informed us that there are four main groups of employees who will have access to electricity consumption information from the smart meter systems:

- Customer Services – for the purpose of billing inquiries and customer support for accessing accounts via the internet;
- Revenue Assurance – for the purpose of theft detection and investigation;
- IT – for the purposes of implementation, maintenance and support; and
- Field Meter Technicians – will have limited access to consumption information for troubleshooting purposes where BC Hydro cannot access the meter remotely.

[73] BC Hydro informed us that currently, in order for a staff member to be granted data access to support his/her respective role, a manager must request and approve the assignment of the role. Apart from the four groups described above, any other BC Hydro employees seeking access to this information for a specific reason must also first receive approval from a manager.

[74] In a role-based access control model, access privileges should be assigned by a central body that includes both program and privacy expertise.[19] The central body should base its decisions on recommendations from senior managers who are familiar with the tasks and services provided by each of their staff. The central body should include senior executives with the organization's primary responsibility for privacy.

[75] From our review, while it appears the role-based access model described by BC Hydro does not allow unlimited access to all employees and appears to put in place reasonable restrictions, BC Hydro has not sufficiently documented this model and improvements can be made to ensure only appropriate access is granted.

Recommendation 4
BC Hydro should follow through with its plans to document in detail its role-based access model for the SMI project. This model should include a comprehensive roles matrix that maps job functions with personal information and privileges required to perform those functions. Roles should be defined as specifically as possible. In accordance with the least privilege principle, BC Hydro should ensure each role only has access to the minimum amount of personal information necessary to perform their functions. ***BC Hydro should fully document the role-based access matrix and regularly check and update it as required. BC Hydro should also implement a monitoring/auditing plan to evaluate whether its staff are properly accessing and using information.***

[19] BC Hydro does have an Access Control Policy, which we look at on p. 25 of this report under "Access Control".

External Disclosures

[76] While BC Hydro is not currently disclosing any personal information from the SMI project to third parties, it did provide us with details on possible disclosures in the future.

[77] BC Hydro will generally have authority to disclose personal information to law enforcement agencies under s. 33.2(i) of FIPPA in instances where law enforcement agencies are investigating suspected criminal activity (such as electricity theft).

[78] BC Hydro has the authority to disclose personal information to the Civil Forfeiture Office of the Ministry of Attorney General in accordance with s. 33.1(1)(i) of FIPPA in order to collect amounts owing to BC Hydro.

[79] Section 19.2 of the *Safety Standards Act* provides authority for BC Hydro to disclose consumption information to municipalities who request residential electricity information within their jurisdictional boundaries. Local governments typically make such requests to determine whether electricity consumption at a particular residence is higher than prescribed thresholds and therefore indicates the residence may be used as a marijuana grow operation. Section 33.1(1)(c) of FIPPA authorizes BC Hydro to make such a disclosure.

[80] BC Hydro informs us that it will not be disclosing individual customer consumption information to companies who are involved in electricity conservation efforts. This is an area that has caused substantial concern in California and elsewhere. The practice BC Hydro is currently implementing is privacy protective and it is important they continue along this path.

[81] I find that BC Hydro's internal and external disclosures of personal information, as described within this investigation, comply with s. 33 of FIPPA.

Recommendation 5
If, in the future, BC Hydro becomes involved in offering its customers the option of disclosing their consumption information to third parties, it should take reasonable steps to ensure that the third parties are transparent about their personal information practices.

Protection of Personal Information

Issue 4 – Has BC Hydro taken reasonable steps to protect personal information within the SMI project? [s. 30 of FIPPA]

[82] Section 30 of FIPPA requires public bodies such as BC Hydro to make reasonable security arrangements to protect personal information in its custody or under its control. It reads as follows:

> 30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

The Standard of Reasonableness for the SMI Project

[83] As previously discussed, BC Hydro is a Crown corporation of the Government of British Columbia and is the main provider of electricity to citizens of this Province. BC Hydro is obligated to take reasonable steps to ensure it protects the personal information of its customers.

[84] Given the ever-increasing sophistication of hackers, all public bodies and organizations need to exercise due diligence in protecting the security of personal information in their custody or under their control. Security of systems requires ongoing vigilance. Public bodies must respond quickly to any identified privacy and security risks. Failure to do so would certainly not meet the requirements in FIPPA. However, reasonableness extends beyond a measure of responsiveness to identified risks. Public bodies must be proactive and implement ongoing monitoring and testing of the security of their systems. Public bodies also must ensure their policies are kept current and that their staff receive regular training.

[85] "Reasonable" does not mean perfect within the context of s. 30 of FIPPA.[20] However, given that BC Hydro is adopting new technology in the form of smart meters, it needs to assure customers that it is properly protecting personal information it will be collecting more frequently with this new technology. As such, we are interpreting "reasonable" to require a high level of rigour in this instance and we have applied this standard in our review and evaluation of BC Hydro's SMI project.

[20] See OIPC Investigation Report F06-01, paras. 49–50, at http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf.

Safeguards

[86] In conducting this review, we interviewed the staff responsible for the security and privacy for the SMI project and reviewed BC Hydro's documentation to assess the safeguards it currently has in place to protect personal information related to the SMI project. We also reviewed the approach taken by BC Hydro to ensure the security of personal information as they add new systems to the SMI project.

[87] BC Hydro currently reads existing smart meters manually. At the time of this investigation, very few of the servers and systems components that will eventually perform the collection and processing of information by smart meters were operational. As a result, much of the review involved assessing documentation such as policies, procedures, standards, planning documents and where available, preliminary testing reports.

[88] To meet the security requirements under s. 30 of FIPPA, a public body must have in place a system of layered defences and it must conduct Security Threat Risk Assessments ("STRA") or an equivalent assessment to evaluate the security threats and risks to personal information. STRAs are a key component of risk management and can help a public body ensure responsible management and security of information and resources. A STRA should review and assess risks related to administrative, technical and physical safeguards. This investigation looked at BC Hydro's risk assessment process in relation to the SMI project.

[89] BC Hydro has implemented an Information Security Design Review Procedure and an associated checklist that it must complete prior to major system upgrades or implementation of new systems. This procedure ensures that BC Hydro staff identify key risk areas and that BC Hydro understands, reviews and adheres to its information security policies and requirements. Sign-off on this documentation is required prior to implementation. Throughout the SMI project, the SMI Security and Privacy team has reviewed and assessed the risks to both the systems and the information housed within the systems to ensure that it has identified and adequately addressed risks. BC Hydro completed both internal and external system testing as a part of this process to validate the effectiveness of the controls.

Administrative Safeguards

i. *Information security policies and procedures*

[90] BC Hydro has implemented policies and procedures that are based on the requirements set out in the international security standard ISO/IEC 27002:2005 Information technology—Security techniques—Code of practice for information

security management. These policies and procedures address areas such as access control, event logging, incident management, software development and system maintenance. BC Hydro has also implemented additional policies and procedures for the SMI project based on NERC CIP[21] and NISTIR[22] 7628 standards, which are aligned to critical infrastructure and the smart grid. BC Hydro's policy and procedure framework is supported by a governance process that requires sign-off at multiple levels prior to the implementation or alteration of systems.

[91] BC Hydro's Information Security Policy states that, "Policies shall be reviewed and approved at least annually to ensure they remain current with technology and business goals, and that they continue to meet the requirements of the standard, which may itself evolve over time". However, BC Hydro last documented the review of this policy in September 2008.

[92] Given that the information security environment changes rapidly, BC Hydro should ensure that it is reviewing and updating all policies in this area on a regular basis. Failure to do so creates a risk that BC Hydro is not keeping pace with changes to its business or technical environments.

Recommendation 6
BC Hydro should ensure that it reviews all policies relating to information security and privacy on a regular basis to ensure that they remain current and relevant. BC Hydro should document this review process; including putting dates on policies to reflect BC Hydro's most recent review.

ii. *Information security education and training*

[93] BC Hydro expects its employees and its contractors to undergo information security training on an annual basis, but this training is not mandatory for all employees. However, training is mandatory for key business groups and

[21] The North American Electric Reliability Corporation ("NERC") is an international, independent, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America. The U.S. Department of Energy designated NERC as the electricity sector coordinator for critical infrastructure protection ("CIP"). NERC works closely with the U.S. Department of Homeland Security and Public Safety and Emergency Preparedness Canada to ensure that the critical infrastructure protection functions are fully integrated and coordinated with the governments of the Unites States and Canada.

[22] The National Institute of Standards and Technology Interagency produces documents known as NIST Internal Reports ("NISTIRs"). NISTIR 7628 is a set of guidelines for smart grid cyber security that presents a framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of smart grid-related characteristics, risks and vulnerabilities.

SMI team members. The Freedom of Information Coordinating Office offers training sessions approximately 10 to 12 times each year, with the last session taking place in May 2011. Employees working on critical parts of the SMI project are required to undergo training on the North American Electrical Reliability Corporation's Critical Infrastructure Protection requirements.

Recommendation 7
BC Hydro should make annual privacy and information security training mandatory for all employees and contractors.

Technical Safeguards

i. *Encryption of personal information*

[94] Organizations that do not properly encrypt personal information place their customers at risk of having others intercept their information and use it for unintended purposes. When dealing with electricity consumption information from smart meters, there is the potential for some criminal interest in studying the patterns of household consumption information to determine when individuals are likely to be away from home. Currently, a person periodically reading the mechanical meter installed at a given residence could accomplish this as well.

[95] Some people have expressed concerns that, once BC Hydro installs a smart meter at their residence, they are at an increased risk of having their household electricity consumption information intercepted and read as it travels wirelessly to and from BC Hydro.

[96] To combat this risk, BC Hydro's internal standards require sensitive data, including personal information, to be protected using 128 bit encryption. 128 bit encryption is the same level of encryption used by many financial institutions and online banking systems. In the case of BC Hydro, the information travelling over the network includes the meter identifier and hourly consumption amounts.

[97] BC Hydro's smart meters communicate via a wireless 'mesh' network. This means that each smart meter will capture and transmit its own data and also transmit data from other smart meters nearby to create a path to a router that will then transmit the information to BC Hydro. BC Hydro will encrypt data travelling on the mesh network in compliance with its internal standards to prevent interception in transit.

[98] BC Hydro assigns each smart meter a unique digital certificate that it uses to verify the authenticity of the information sent from the meter to BC Hydro. BC Hydro also uses this certificate to facilitate secure communications between the meter and the systems located within BC Hydro. This method of information signing and encryption ensures that people from one household cannot decrypt or read data from another household's meter. It also ensures that others cannot intercept and read the data during transmission from the meter to BC Hydro.

ii. *Smart meter devices*

[99] Smart meters store hourly consumption information for the residence at which they are installed. The memory chip within the smart meter does not store any customer account details and does not contain the customer's account number or the service location identifier. The memory chip stores the serial number of the smart meter and the hourly recordings of electricity consumption for the household at which the smart meter is installed. The linkage between the consumption information and the customer account details occurs at BC Hydro rather than at the smart meter itself.

[100] BC Hydro has contracted with a third party testing firm with expertise in smart meter technology to test the smart meters and attempt to access information stored on the memory chip. Even when using complex scientific processes which resulted in irreversible damage to the meter and the chip, the testing firm was not able to read the data stored on the chip.

iii. *Infrastructure security*

[101] The smart metering infrastructure consists of a number of security zones, including a zone with security designed to meet the standards identified in the NERC CIP standards.

[102] Each of the zones that contain, or are planned to contain, personal information collected from smart meters are protected with standard controls such as firewalls, intrusion detection or intrusion prevention systems and event management and monitoring systems.

[103] BC Hydro has a procedure in place to address the threat of malicious code and requires systems to be configured and managed in such a way as to significantly reduce the likelihood of malicious code being successfully introduced.

[104] Key components of the SMI project are subjected to both vulnerability scanning by internal personnel and to penetration testing by an independent third party. Where BC Hydro finds security issues such as insecure configurations or software defects, it has a system in place to track these issues to resolution. The SMI security and privacy team reports to senior management on outstanding issues on a regular basis and, where necessary, is in contact with its vendors to ensure that they address identified vulnerabilities in a timely manner.

iv. *System development*

[105] As new systems are developed and implemented or enhancements for existing systems are introduced, staff are required to adhere to BC Hydro's Information System Design Security Review Procedure. This procedure includes completing documentation and obtaining sign-off to ensure compliance with BC Hydro's security policies and procedures.

v. *Access Control*

[106] BC Hydro's Access Control Policy requires that all business areas adhere to a strict set of requirements to ensure that employees, consultants and vendor personnel have system access privileges that are consistent with the job functions that they are required to perform. To ensure consistency, BC Hydro assigns access privileges based on standard user profiles that it designates for groups within the organization.

[107] Management reviews and approves access privileges such as new accounts and privilege changes prior to implementation. BC Hydro performs reviews of access privileges on a regular basis to ensure that it is adhering to BC Hydro's Access Control Policy.

[108] Employees and contractors who use BC Hydro's systems are required to adhere to BC Hydro's User ID and Password Standard. The standard sets out the processes for requesting user IDs both for employees and for contractors. The standard also addresses the responsibility of the user to maintain the confidentiality of passwords and the requirements for creating a strong password.

vi. *Audit logging (access to electricity consumption data)*

[109] BC Hydro tracks, logs and reviews activities on its servers to ensure compliance with its Security Logging Standard. When BC Hydro introduces the ability for customers to view their hourly electricity consumption information through an SMI portal website, it will also introduce logging that will record when customers and customer-service personnel view a record and the time and date that the record was viewed. BC Hydro's customer-service personnel will see

a notification regarding privacy compliance and the audit logging activities that are in place prior to accessing a customer's electricity consumption information.

Recommendation 8
While it appears to be BC Hydro's intention, it should ensure that it introduces read-access logging prior to commencing the collection of hourly electricity consumption information. BC Hydro should also implement a monitoring/auditing plan to evaluate the effectiveness of its read-access logging.

vii. *Future phases of smart metering*

[110] BC Hydro will carry out security reviews and technical testing on the systems that will collect and manage information from the smart meters as the systems are developed, tested and implemented. This will ensure that BC Hydro configures and maintains the systems in such a way as to minimize their exposure and vulnerability to security threats such as hackers and malicious code. To ensure that the new systems are in compliance with BC Hydro's policies, procedures and security standards, a process is in place that requires approval by the SMI security and privacy team prior to implementation.

Physical Safeguards

i. *Data centre security*

[111] BC Hydro houses the systems that will hold the electricity consumption information collected from the smart meters in two locations. Those systems that are identified as critical assets are housed in a data centre that is designed to be compliant with the NERC CIP standards. Systems that are customer-service oriented or customer-facing are housed within BC Hydro's corporate data centre.

[112] Closed-circuit television cameras and regular building security patrols monitor both data centres. All accesses and activities performed within the data centres are monitored. Alarm and notification systems detect and report unauthorized attempts to enter restricted areas and entry to the NERC CIP data centre requires two-levels of verification, an access card and a corresponding entry code. Visitors are not allowed access to a data centre without written approval from management and are escorted at all times when in the data centre.

Summary of Safeguards

[113] BC Hydro has taken steps to ensure that the systems related to the smart meter project are tested prior to implementation, governed by a strong policy framework and maintained in accordance with industry best practices. The policy framework and on-going risk assessment processes are designed to keep the systems current as both the technology and the risks to personal information continue to evolve.

[114] I find that BC Hydro's security arrangements for the SMI project meets the standard of reasonableness required by s. 30 of FIPPA.

Retention of Personal Information

Issue 5 – Does BC Hydro retain its customers' personal information in accordance with FIPPA? [s. 31]

Stored for at Least One Year

[115] Section 31 of FIPPA sets out a public body's requirements for the retention of personal information as follows:

> 31 If an individual's personal information
>
> (a) is in the custody or under the control of the public body, and
>
> (b) is used by or on behalf of the public body to make a decision that directly affects the individual,
>
> the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.

[116] Public bodies may need to keep records for longer periods in accordance with other legislation such as the *Limitation Act*.

[117] We found that BC Hydro currently retains customer personal information indefinitely. While BC Hydro is in compliance with the one year minimum requirement in s. 31 of FIPPA, this practice raises concerns with respect to retention periods.

Retention Periods and Disposal of Records

[118] In order to minimize unauthorized collection and disclosures, BC Hydro employees should not have ongoing access to personal information no longer required for the delivery of SMI project services. For example, there should be limited access to the records of a customer who has closed his/her account and moved out of the province.

[119] Archiving of records is an effective means to minimize access. When public bodies archive records that they no longer need on a regular basis, these records should be securely stored in a different place from active records.

[120] We found that there is no archiving of records by BC Hydro.

[121] With respect to retention of records, we found that BC Hydro has begun to establish a comprehensive records management program, including information classification and retention schedules. This will apply to the SMI project and other parts of BC Hydro's business.

[122] BC Hydro has not provided us a policy regarding the disposal or destruction of records. Customers have the expectation that an organization will delete their personal information when it is no longer needed. As such, BC Hydro should securely dispose of customers' records in accordance with an internal policy.

[123] In the event that BC Hydro requires historical information regarding electricity consumption, it should ensure that its policy reflects that BC Hydro will anonymize electricity consumption information after a specified time period so that it cannot link the information with any particular customer.

Recommendation 9
BC Hydro should archive SMI project records containing personal information that are no longer required for the delivery of customer services on a regular and ongoing basis. BC Hydro should develop a classification scheme to identify those records.

Recommendation 10
BC Hydro should not retain customer personal information indefinitely. BC Hydro should continue to develop and implement a records retention and disposition policy that sets out when the disposal of personal information of its customers and former customers will occur.

PART IV PRIVACY MANAGEMENT FRAMEWORK

[124] A privacy management framework is the total of all actions taken by a public body to protect the personal information in its custody and control. It includes such things as the staff resources dedicated to privacy and security as well as the policies and procedures that address privacy and security risks through strategies ranging from encryption to privacy training. It is multi-faceted and it instils a culture of privacy within a public body.

[125] We conducted a thorough review of the privacy management framework BC Hydro has in place for the SMI project. Our review consisted of a holistic consideration of BC Hydro's organizational commitment, privacy policies and procedures, and measures to ensure ongoing risk assessment and revision. For the purposes of this report, we chose to include only an outline of the elements we expect to see in an organization's privacy management program as well as our general findings and recommendations we made to BC Hydro to improve its current program.

[126] When evaluating a public body's commitment to privacy, we look for the naming of an individual responsible for privacy and an adequately funded Information and Privacy Office.

[127] In examining privacy deliverables, we expect to see that a public body has undertaken an inventory of the personal information it is collecting, using and disclosing. We also look for essential privacy policies and procedures.[23] Public bodies should be preparing privacy impact assessments ("PIAs") to assess and mitigate privacy implications of any new project. Public bodies should treat PIAs as evergreen documents that they review and update on a regular basis as required.

[23] Examples include: privacy breach management policy; security policies (*i.e.* systems security policy, travelling with personal information policy, physical security policy); role-based access policy; guidelines on the collection, use and disclosure of personal information; and retention and disposal policy.

[128] Our office expects a public body to undertake STRAs to test that reasonable security is in place for all new systems. We also expect that all contracts with service providers involving personal information will include privacy protection schedules and that there is mandatory training and education for all staff with access to personal information.

[129] Employees should be aware of whom to report complaints and breaches and public bodies should have policies to reflect these practices.

[130] The management of personal information requires ongoing monitoring, assessment and updating of privacy policies, procedures and practices. Public bodies must effectively communicate updates to staff. It is critical to regularly test and audit the security of systems and for public bodies to ensure they evaluate their breach management system after any incidents to ensure they are implementing best practices.

[131] Annual performance plans of a privacy office should include such items as a privacy audit schedule, training schedule, policy review schedule and performance measures. Among the other items we would expect to see is evidence of a public body's commitment to contractor compliance. A public body can demonstrate this commitment through the use of audits, ensuring contractors receive regular privacy training and ensuring contractors regularly update their confidentiality agreements.

BC Hydro's Privacy Management Framework

[132] As the SMI project is in its early stages, we wanted to ensure that BC Hydro has in place the appropriate framework to properly address privacy both now and in the future. I am reasonably assured that BC Hydro can properly manage privacy and security for future phases of the SMI project.

[133] As a result of our review, it is clear that BC Hydro has invested considerable resources in ensuring it builds privacy into its organizational culture. BC Hydro has numerous policies, procedures and standards that govern its handling of personal information. It has completed and provided us with a comprehensive range of PIAs for the SMI project and has shown that it has in place measures to monitor ongoing privacy issues.

[134] We have made recommendations in areas where BC Hydro should make improvements to its privacy management framework and we will monitor BC Hydro's implementation of our recommendations.[24]

[24] These are Recommendations 11 – 14 in Appendix B.

PART V CONCLUSION

[135] As a result of my office's investigation into the SMI project, I find the following:

1. (a) BC Hydro's collection of personal information for the SMI project complies with s. 26 of FIPPA.

   (b) BC Hydro is not compliant with the notification requirement in s. 27(2) of FIPPA. In order to comply with this requirement, BC Hydro should develop more comprehensive web pages and paper notices for its customers regarding the purposes for collecting hourly consumption data, the legal authority for collection, and the contact information for the person within BC Hydro who can answer questions regarding collection.

2. BC Hydro's use of personal information in the SMI project complies with s. 32 of FIPPA.

3. BC Hydro discloses personal information in the SMI project in compliance with s. 33 of FIPPA.

4. BC Hydro protects personal information within the SMI project in compliance with s. 30 of FIPPA.

5. BC Hydro's retention of personal information related to the SMI project complies with s. 31 of FIPPA.

[136] BC Hydro has demonstrated to me that it has the capacity to properly manage privacy and security risks. However, I have made various recommendations[25] that would improve BC Hydro's privacy and security governance. BC Hydro has committed to put in place action plans to address these recommendations. I will continue to monitor the SMI project to ensure I am satisfied with how BC Hydro carries out its plans.

[137] The SMI project is in its early stages and BC Hydro is still developing solutions and ideas on how it will implement various aspects of the project. BC Hydro has significant work ahead of it on such things as the security architecture of the SMI project and the BCHydro.com customer portal in advance of the spring of 2012, when it expects smart meters will be fully functional. As the SMI project progresses, it is imperative that BC Hydro continue to avoid using its customer's consumption information for additional purposes and that it

[25] See Appendix B for complete list of recommendations.

discloses its customer's information with third parties only in a manner that complies with FIPPA.

[138] BC Hydro is committed to consulting with our office as it moves forward with the SMI project and further develops the privacy and security framework.

[139] There are clear and specific legislative requirements for BC Hydro in relation to smart meters. BC Hydro must install smart meters for each residence and collect hourly consumption data from these residences. By law, there is no choice for the citizens of our province.

[140] However, the citizens of British Columbia will have substantial choice as to the degree of their future involvement in the smart grid. Investment by customers in "smart home" functionality will be encouraged and guided by BC Hydro. BC Hydro will do this through initiatives such as financial incentives to buy in-home feedback devices. BC Hydro's customers should carefully consider the privacy implications of their choices, including what products they will purchase to try to reduce their electricity consumption.

[141] Citizens of British Columbia have expressed considerable concern regarding BC Hydro's implementation of smart meters. They are right to question how BC Hydro is mitigating the privacy risks for this project. Hopefully, they will take some comfort in knowing that our investigation found that BC Hydro is taking reasonable steps to protect its customers' personal information.

ACKNOWLEDGEMENTS

[142] BC Hydro has cooperated fully with our investigation.

[143] Troy Taillefer, Policy Analyst, and Angela Swan, Technical Investigator, co-ordinated this investigation and were assisted by Helen Morrison, Senior Policy Analyst, in the preparation of this report.

December 19, 2011

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

OIPC File No.: F11-46341

APPENDIX A
Relevant Sections of the *Freedom of Information and Protection of Privacy Act*

Purpose for which personal information may be collected

26 A public body may collect personal information only if

(a) the collection of the information is expressly authorized under an Act,
(b) the information is collected for the purposes of law enforcement,
(c) the information relates directly to and is necessary for an operating program or activity of the public body

...

How personal information is to be collected

27(2) A public body must ensure that an individual from whom it collects personal information is told

(a) the purpose for collecting it,
(b) the legal authority for collecting it, and
(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Protection of personal information

30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Retention of personal information

31 If an individual's personal information

(a) is in the custody or under the control of a public body, and
(b) is used by or on behalf of the public body to make a decision that directly affects the individual,

the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.

Use of personal information

32 A public body may use personal information in its custody or under its control is used only

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),
(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or
(c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

Disclosure of personal information

33 A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3.

Disclosure inside Canada only

33.2 A public body may disclose personal information referred to in section 33 inside Canada as follows:

(a) for the purpose for which it was obtained or compiled or for a use consistent with that purpose (see section 34);

...

(c) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister;

...

(i) to a public body or a law enforcement agency in Canada to assist in a specific investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result;

APPENDIX B – Recommendations

Recommendation 1

As BC Hydro introduces new elements to the smart grid, or increases the functionality of existing elements of the grid, it should continue to complete privacy impact assessments in each instance and provide it to the OIPC for review and comment before implementation.

Recommendation 2

BC Hydro must develop more comprehensive web pages and paper notices for its customers for the SMI project regarding the purposes for collecting hourly electricity consumption data, the legal authority for collection, and the contact information for the person within BC Hydro who can answer questions regarding the collection.

Recommendation 3

Before any future secondary uses of electricity consumption information take place, BC Hydro should complete a privacy impact assessment and provide it to the OIPC for review and comment prior to implementation.

Recommendation 4

BC Hydro should follow through with its plans to document in detail its role-based access model for the SMI project. This model should include a comprehensive roles matrix that maps job functions with personal information and privileges required to perform those functions. Roles should be defined as specifically as possible. In accordance with the least privilege principle, BC Hydro should ensure each role only has access to the minimum amount of personal information necessary to perform their functions.

BC Hydro should fully document the role-based access matrix and regularly check and update it as required. BC Hydro should also implement a monitoring/auditing plan to evaluate whether its staff is properly accessing and using information.

Recommendation 5

If, in the future, BC Hydro becomes involved in offering its customers the option of disclosing their consumption information to third parties, it should take reasonable steps to ensure that the third parties are transparent about their personal information practices.

Recommendation 6

BC Hydro should ensure that it reviews all policies relating to information security and privacy on a regular basis to ensure that they remain current and relevant. BC Hydro should document this review process; including putting dates on policies to reflect BC Hydro's most recent review.

Recommendation 7

BC Hydro should make annual privacy and information security training mandatory for all employees and contractors.

Recommendation 8

While it appears to be BC Hydro's intention, it should ensure that it introduces read-access logging prior to commencing the collection of hourly electricity consumption information. BC Hydro should also implement a monitoring/auditing plan to evaluate the effectiveness of its read-access logging.

Recommendation 9

BC Hydro should archive SMI project records containing personal information that are no longer required for the delivery of customer services on a regular and ongoing basis. BC Hydro should develop a classification scheme to identify those records.

Recommendation 10

BC Hydro should not retain customer personal information indefinitely. BC Hydro should continue to develop and implement a records retention and disposition policy that sets out when the disposal of personal information of its customers and former customers will occur.

Recommendation 11

BC Hydro should ensure that it has designated an individual to be responsible for privacy within the organization. This individual should have primary responsibility for privacy within BC Hydro and within the SMI project. This individual should be a member of BC Hydro's executive team and/or should be fundamental to BC Hydro's business decision-making process.

Recommendation 12

BC Hydro should develop annual and/or multi-year privacy performance plans for the SMI project.

Recommendation 13

BC Hydro should ensure it has reporting mechanisms regarding its privacy management framework and it should state these mechanisms in its privacy policies and procedures.

Recommendation 14

BC Hydro should develop policies relating to training of employees and service providers, audit and breach management.