Privacy by Design:

Achieving the Gold Standard in Data Protection for the Smart Grid

June 2010

www.privacybydesign.ca

hydro one

Information & Privacy Commissioner of Ontario

toronto hydro corporation

Acknowledgements

The contributors gratefully acknowledge and thank the following staff for their work in preparing this document:

- Catherine Thompson, Regulatory and Policy Advisor, Ontario Information and Privacy Commissioner's Office
- Jim Hall, Manager, Business Development and Support, Hydro One Networks Inc.
- Kshamit Dixit, Manager IT & Security Office, Toronto Hydro Electric System

The contributors would also like to thank the following for their participation and work in facilitating this project:

- Michelle Chibba, Director, Policy Department, Ontario Information and Privacy Commissioner's Office
- Michael Winters, Chief Information Officer, Hydro One Networks Inc., Rick Stevens, Director, Distribution Development, Hydro One Networks Inc., and Adele Pantusa, Senior Legal Counsel, Hydro One Networks Inc.
- Blair Peberdy, Vice-President, Marketing, Communications and Public Affairs, Toronto Hydro Electric System, and Vanessa Nero, Web and E Communications Consultant, Toronto Hydro Electric System

Information and Privacy Commissioner, Ontario, Canada

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

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Foreword

There are two schools of thought among electrical utilities regarding the Smart Grid. The first is that the Smart Grid is simply an extension of current functions and that taking a business-as-usual approach is sufficient. The second is that the Smart Grid presents new opportunities for growth and change, as well as new challenges for collecting more granular data than ever before on customers' energy consumption. Utilities that ascribe to the second group recognize that the Smart Grid will be transformative in nature and can take steps to address any new issues that may arise. I call this taking a "positive-sum" approach wherein the interests of both electrical reform *and* privacy may be achieved.

As Information and Privacy Commissioner of Ontario, I am joined by Ontario's largest electricity companies — Hydro One Inc. ("Hydro One") and Toronto Hydro — to showcase the strong privacy protections embedded in the province of Ontario's emerging Smart Grid system. Hydro One and Toronto Hydro provide electricity to over two million households in a province with comprehensive privacy laws, and are therefore uniquely positioned to understand how to implement large scale systems while respecting privacy. I would like to thank Laura Formusa, Hydro One Networks Inc., and Anthony Haines, Toronto Hydro Electric System, for their leadership.

With virtually every home and business in Canada's most populous province now having a smart meter, we can say that Ontario is a strong leader in laying the Smart Grid infrastructure that is essential to the future of electricity provision and the conservation of electricity. We are also a leader in the area of privacy and Smart Grid policy. The Office of the Information and Privacy Commissioner of Ontario is foremost in promoting the concepts of *Privacy by Design* and Positive-Sum applications of privacy around the world.

We hope this best practice document will assist utilities, including those in the United States and around the world, to understand how Fair Information Practices (FIPs) and *Privacy by Design* can be incorporated into the design and architecture of Smart Grid systems. Utilities will benefit enormously from striving to achieve the Gold Standard in Data Protection for the Smart Grid — *Privacy by Design*.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

Table of Contents

Executive Summary

Privacy by Design (the Gold Standard for data protection), is *the* standard to be adopted for Smart Grid implementation for data protection. Embracing a positive-sum model whereby privacy and energy conservation may be achieved in unison is key to ensuring consumer confidence in electricity providers, as Smart Grid projects are initiated. Customer adoption and trust of Smart Grid energy savings programs is an integral factor in the success of energy conservation.

The Smart Grid in Ontario

The Smart Grid in Ontario is developing through the widespread installation of smart meters, time-of-use, demand management initiatives, and the creation of a Smart Metering Entity resulting from legislative action by the Government of Ontario in the *Green Energy Act, 2009* and the *Electricity Act, 1998*. The province's goal is to meet electricity demand over the next 20 years, while also achieving energy conservation and use of renewable energy resources (for example, to discontinue the use of coal plants by 2014). Functional specifications were issued by the Government that all electricity providers must meet in achieving smart meter policy goals to support the Smart Grid, and the Smart Metering Entity is responsible for the consolidation, management and storage of consumer electricity consumption information.

Hydro One and Toronto Hydro are involved with several Smart Grid activities. Hydro One's focus is on integrating renewable energy generation, customer demand management, and system automation. As well, Hydro One will conduct pilots to investigate, understand and prepare for new innovative technologies to enable the Smart Grid. For example, a Smart Grid zone ("Smart Zone") will be created in a geographic subset of its system. Toronto Hydro's Smart Grid roadmap includes several initiatives focused on climate protection, energy security and customer satisfaction. Toronto Hydro's activities will be in the area of conservation and demand management, distribution grid automation and home energy management systems.

Personal information and the Smart Grid

What constitutes "personal information" on the Smart Grid is the subject of much discussion. Personal information is defined by the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), as "recorded information about an identifiable individual." Once it becomes apparent that a Smart Grid technology, system or project will involve the collection of personal information, privacy considerations begin to apply, such as limiting the amount of personal information collected, used or disclosed, and the safeguarding of that information. The digitization of smart meter information has an impact on privacy experienced in other areas where traditional paper records are being transferred into digital

form. Digital smart meter data, like all digital data, is vulnerable to accessing, copying, matching, merging and massive dissemination.

The changing nature and vast increase of information gathered on the Smart Grid is also resulting in changes in the nature of utilities as power providers. Lack of integration between various systems in the area of communications, operations and information systems, is a significant gap within which challenges may arise for utilities. Utilities should be aware of the gaps and opportunities to work *Privacy by Design* into these systems, such as the introduction of smart transformers and power line monitors, and the centralization and integration of data and processes.

Best practices for Smart Grid Privacy by Design

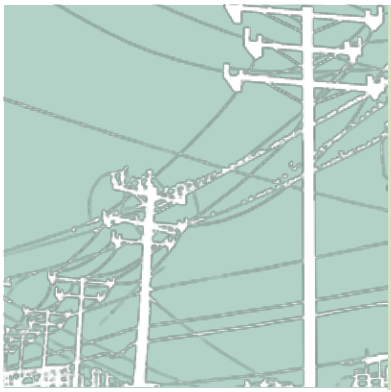
Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure. *Privacy by Design* may be accomplished by practicing the originating 7 Foundational Principles,[1] which have been specifically adapted to the Smart Grid context, to create Best Practices for Smart Grid *Privacy by Design*:

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring;
2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured;
3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature;
4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects;
5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected;
6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives;
7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement.

Smart Grid Privacy by Design Use Case Scenarios

Each Best Practice can be applied by utilities in the planning of their Smart Grid activities. This is illustrated through two use case scenarios describing the implementation of *Privacy by Design* into Smart Grid projects in the areas of 1) customer information access and 2) customer enablement. The customer information access use case scenario shows how all customers must be authenticated, and how multiple consecutive access failure attempts will disable the account. In the first scenario, protecting access to customer information will foster trusting relationships — allowing the customer to trust the utility, and therefore increasing the likelihood of his/her participation to realize the benefits of the Smart Grid. The customer enablement use case scenario examines how privacy concepts may be built into the core design, directly involving customers in the dynamic management of the electrical grid.

1 *The 7 Foundational Principles of Privacy by Design* may be found in Appendix A.



Introduction

At the end of the day, it's all about standards. If we get that right at the onset, we create an ecosystem for the development of technologies that will thrive in the present and future.

Chuck Adams, President of IEEE[2]

While the Smart Grid has the potential to deliver substantial value, it represents a significant endeavour that will require privacy risk mitigation measures to be taken. Many technologies and standards are still in their early stages of development, and not all will move into commercialization or reach a suitable practice point for mass deployment. The costs and time required, as well as the benefits attained, will depend on the scope and pace of implementation, technology trends, and consumer acceptance and adoption. Utilities have an interest in ensuring that consumer adoption of Smart Grid energy saving programs is not impeded by fears relating to privacy. Electricity providers must embrace a new positive-sum business model — one that is protective of privacy — or risk losing consumer confidence and the public's trust.[3]

In November 2009 the Information and Privacy Commissioner of Ontario (IPC) released a white paper with the Future of Privacy Forum entitled, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation,* to call attention to the privacy concerns related to the Smart Grid, and argue that energy conservation can be achieved without sacrificing the privacy of energy consumers. We call this a "positive-sum" doubly-enabling model, not the dated win-lose model involved in traditional zero-sum paradigms.[4] The paper explored how the nature of utilities as power providers will shift due to the large amounts of personal information they will be collecting from consumers as a result of advancements in the Smart Grid, such as the installation of smart meters and the use of smart appliances by households. The concepts discussed in that paper, featuring *Privacy by Design*, are gaining widespread momentum. Ontario's use of *Privacy by Design* has been adopted in various arenas including submissions to the U.S. National Institute of Standards and Technology and the U.S. Federal Communications Commission.[5] *Privacy by Design*

2 Chuck Adams, "Smart grid standards: Why are they needed and how will they work?" *Connected Planet*, 7 April 2010

3 A survey conducted in 22 countries revealed that 32 per cent of consumers do not trust energy companies, and 46 per cent trust energy companies, however only if they have direction from government. *Accenture New Energy World Survey*, 9 March 2010: http://newsroom.accenture.com

4 See A. Cavoukian, *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum*, online at: www.ipc.on.ca

5 E.g. Comments Of The Center For Democracy & Technology Before the Department of Commerce, National Institute of Standards and Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy And Requirements, December 1, 2009, available online: http://www.cdt.org/files/pdfs/CDT%20Comment%20NISTIR%207628%20Draft%2012-02-09%20FINAL%20-%20updated.pdf; Comments Of The Center For Democracy & Technology Before the Federal Communications Commission In the Matter of Smart Grid Technology, October 2, 2009, available online: http://www.cdt.org/privacy/20091002_fcc_smart_grid.pdf .

encompasses and compliments parallel concepts in the area of safety,[6] with which utility personnel may be more familiar.

Privacy standards are needed against which utility stakeholders can map their Smart Grid developments and implementation.[7] For example, observers have commented that "making sense of all the data is a big challenge for utilities" in the United States.[8] Even in jurisdictions, such as the United States, that do not have overarching privacy laws as in Ontario, the need to protect the privacy of energy consumption data is being increasingly recognized, especially as it relates to the Smart Grid.[9]

The purpose of this paper is to put forward *Privacy by Design* (the Gold Standard for data protection) as *the* standard to be adopted for Smart Grid implementation, in order to protect data privacy. We will also showcase how Smart Grid programs in Ontario are being built with *Privacy by Design* as a central guiding design feature.[10] To discover how Ontario achieves the Gold Standard for the Smart Grid, *please read on…*

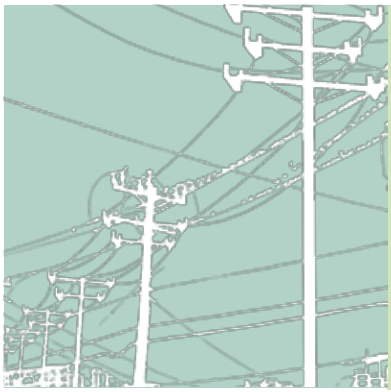
6 E.g. "Safety by Design" which requires considering health and safety issues at early design stages.

7 The U.S. GridWise Alliance, of which the Commissioner is a member, also recognizes this important need. "The Alliance believes that standards will be of critical importance as smart grid technologies are deployed at scale." Reported in: "GridWise Alliance Members Elected to US Smart Grid Panel" *SustainableBusiness.com News*, 23 November 2009, available online: http://www.sustainablebusiness.com/index.cfm/go/news.printerfriendly/id/19288.

8 M. LaMonica, "Peering beyond the meter in the smart grid," *CNET*, 11 February 2010, available online: http://news.cnet.com/8301-11128_3-10451082-54.html.

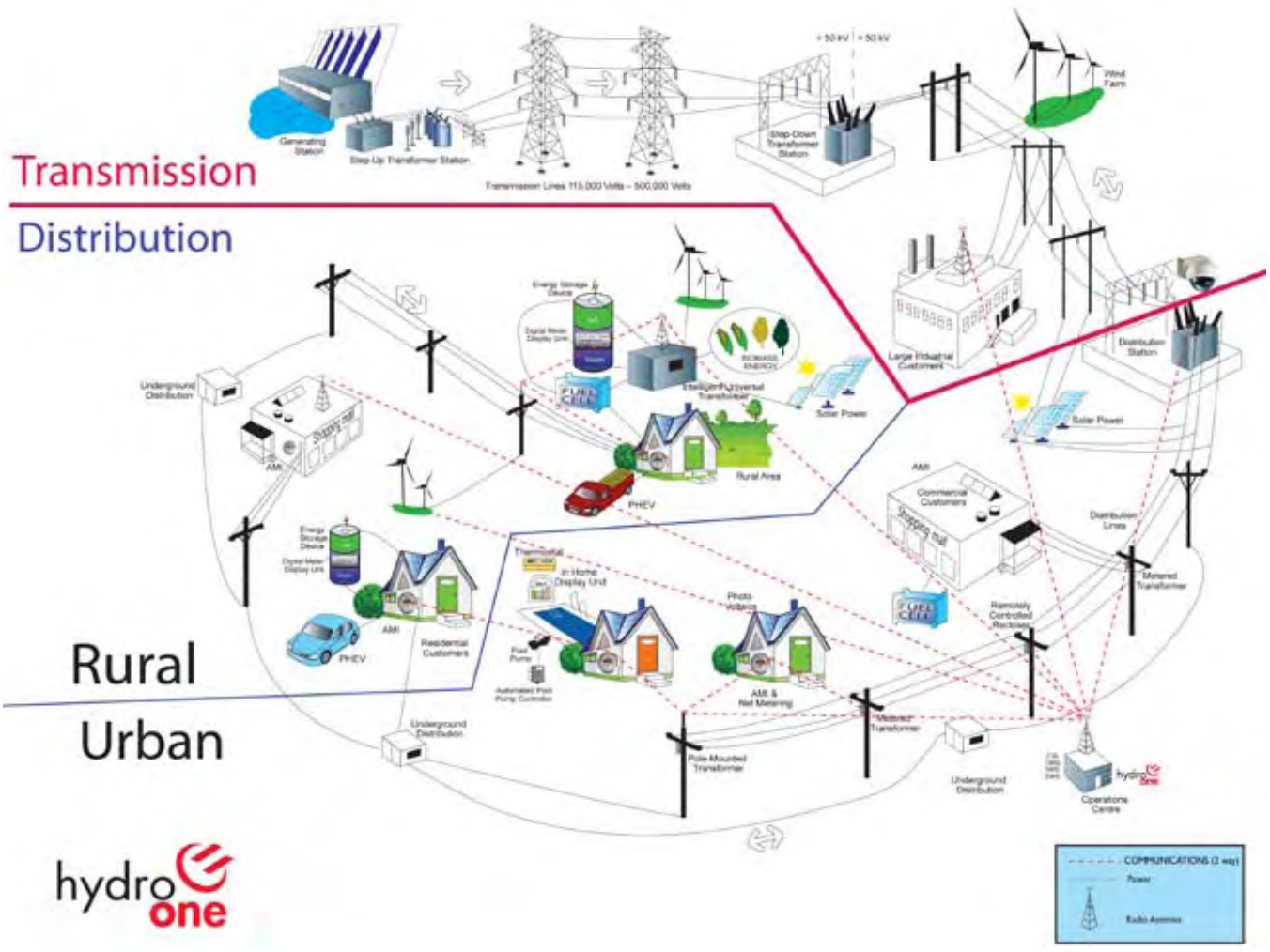
9 California SB 837.

10 For example, electricity distributors in Ontario are permitted to recover the cost of smart meter functionality from consumers so long as it does not exceed the *minimum* functionality required, unless those costs are approved by the Ontario Energy Board (OEB). However, we note that in making their decision, the OEB must take into account the benefits of additional functionality to the distributor's consumers (e.g. increased privacy). See *Ontario Energy Board Act, 1998*, Ontario Regulation 426/06 Smart Meters: Cost Recovery, s. 1 (2)-(3).



The Smart Grid in Ontario

Smart metering provides the anchor tenant for improved communications across the distribution system; communications provides for the convergence of information technologies with the delivery of power. It is the many opportunities this convergence provides that is labelled the “Smart Grid”:

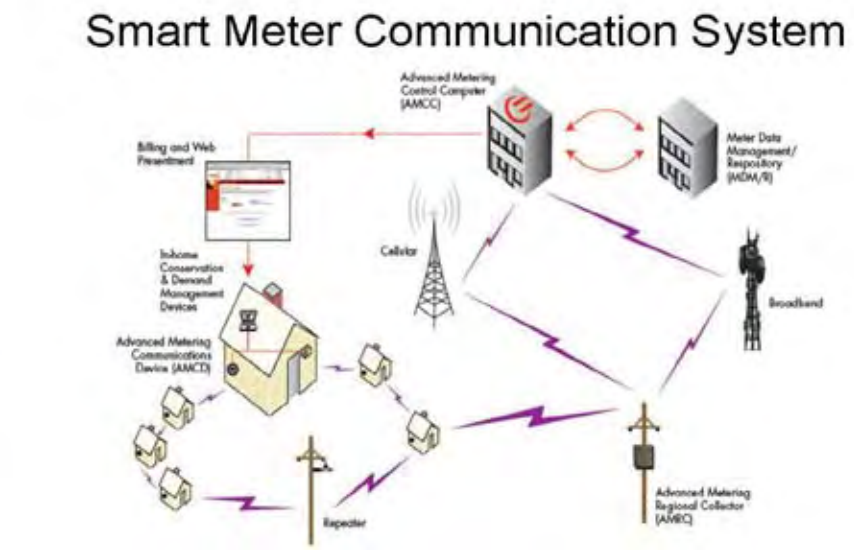


Source: Hydro One Networks Inc.

Ontario law defines the Smart Grid as:[11]

> …the advanced information exchange systems and equipment that when utilized together improve the flexibility, security, reliability, efficiency and safety of the integrated power system and distribution systems, particularly for the purposes of,
>
> (a) enabling the increased use of renewable energy sources and technology, including generation facilities connected to the distribution system;
>
> (b) expanding opportunities to provide demand response, price information and load control to electricity customers;
>
> (c) accommodating the use of emerging, innovative and energy-saving technologies and system control applications; or
>
> (d) supporting other objectives that may be prescribed by regulation.

While exactly what will comprise the Smart Grid in the future is unknown, major components of the future grid in Ontario will include advanced metering infrastructure, time-of-use pricing, demand management, and the creation of a Smart Metering Entity. Ontario's time-of-use pricing goal is to have 1 million customers on time-of-use by the summer of 2010, and by June 2011, to have 3.6 million customers on time-of-use. In order to implement time-of-use prices, electricity distribution companies must achieve four things: install smart meters, enrol those smart meters with the Meter Data Management Repository ("repository") maintained by the Independent Electricity System Operator (IESO), incorporate time-of-use prices within their services, and file their program with the Ontario Energy Board (OEB). At the end of 2009, the number of meters enrolled was 26 per cent of the government's 2010 target.[12] The Ontario government has established a plan that draws on customer demand management and renewable generation to help meet projected electricity demand over the next 20 years. This is projected to enable the shut down of coal plants in Ontario by 2014.[13]



Example of an Advanced Metering Infrastructure (AMI)
Source: Hydro One's Smart Meter (AMI) Solution: Over 1 Million Meters Deployed

11 *Electricity Act, 1998*, S.O. 1998, c. 15, Sched. A, s. 1.3

12 OEB Monitoring Report: Smart Meter Deployment and TOU Pricing – 2009 Fourth Quarter, February 25, 2010, available online: http://www.oeb.gov.on.ca/OEB/_Documents/SMdeployment/SM_Monitoring_Report_20100225.pdf.

13 C Puxley, "Ontario Promises to Close Coal Plants By 2014, Reduce Greenhouse Gas Emissions," redOrbit, 18 June 2007, available online: http://www.redorbit.com/news/business/972199/ontario_promises_to_close_coal_plants_by_2014_reduce_greenhouse/index.html.

Electricity distributors in Ontario are required to adhere to functional specification criteria when installing smart meters, metering equipment, systems and technology.[14] The specifications require a minimum functionality of hourly meter reads, and the ability to transmit this information without field visits. Smart meters contain an advanced metering communication device, and each has a visible display that includes its identification number and meter serial number. Transmission of meter reads may be as frequent as necessary to meet requirements, and must be done using an approved protocol and file structure. Distributors with advanced metering control computers may store up to 60 days worth of meter reads, and must not aggregate meter reads into rate periods or calculate consumption data prior to sending the information to the IESO's repository. The smart meter system must also report on confirming data linkages between the advanced meter communication device, the meter serial number and the customer's account. The smart meter system, including some parts the repository must also log successful transfer of meter reads as well as log unsuccessful attempts, including the cause and status of such attempts. In addition, the system must confirm the accuracy of meter readings and report suspected cases of meter theft, tampering or interference.

An Advanced Metering Infrastructure (AMI) is required to have "security features to prevent unauthorized access to the AMI and meter data and to ensure authentication to all AMI elements."[15] The IESO uses a unique ID for each electricity point of delivery (physical or virtual), including individual residences or multiple meters. The repository maintains internal links that relate each point to metered quantities. The master directory links all points, meters, and utilities. Meter reads are stored in the repository including interval consumption data and billing quantity data. It can support meter reads from 5 to 60 minute intervals. Meter data is aggregated for reporting and analysis. The repository can flag data as outdated and schedule it for re-aggregation when it is required. The repository supports overrides to allow for the utility to update inaccurate information.

The province's specifications also require that an AMI meet all applicable federal, provincial and municipal laws, codes, rules, directions, guidelines, regulations and statutes, including requirements of regulatory authorities and agencies such as the Canadian Standards Association and Measurement Canada.

The Smart Metering Entity was created by legislation to accomplish the government's smart metering initiative.[16] The entity has responsibility for the collection, management and storage of information related to the metering of consumers' consumption or use of electricity in Ontario, including data collected from distributors. In order to do this, the entity can operate one or more databases to facilitate collecting, managing, storing and retrieving smart metering data. The entity is required to provide and promote non-discriminatory access, on appropriate terms and subject to any conditions in its licence relating to the protection of privacy, by distributors, retailers, the Ontario Power Authority (OPA) and other persons. The Smart Metering Entity may also manage and aggregate the data related to consumers' electricity consumption or use. Distributors, retailers and other persons must provide the entity with the information it requires in fulfilling its objects or conducting its business activities. The IESO is designated as the Smart Metering Entity under Ontario Regulation 393/07 of the *Electricity Act, 1998*.

For an overview of electricity in Ontario, see Appendix B.

14 Functional specifications released on July 5, 2007 for advanced metering infrastructure in Ontario. See also *Electricity Act, 1998* s. 53.16. These functional specifications for advanced metering infrastructure in Ontario are the prescribed criteria for residential and small general service consumers and apply to meters, metering equipment, systems and technology, and any associated equipment, systems and technologies. They are prescribed in Ontario Regulation 425/06 under the *Electricity Act, 1998*.

15 *Ibid.*

16 Part IV.2 of the *Electricity Act, 1998*.

Hydro One key Smart Grid activities

Hydro One followed a three step process to develop its Smart Grid plan. The first step was to focus on integrating renewable energy generation, customer demand management, and system automation by leveraging the new communication infrastructure put into place for smart meters. Secondly, the Company formulated plans to utilize pilots and targeted development work to investigate, understand and prepare for new innovative technologies to enable the Smart Grid. In accordance with OEB guidelines and direction from Provincial Governments, Hydro One plans to fund targeted studies in the area of green energy technologies such as automated home energy networks and energy storage. The final step is the implementation of pilot projects to confirm viability of new technologies and products before widespread deployment. Hydro One takes an active role in forums to develop concepts and standards relating to the Smart Grid and regularly commissions universities and other consultants to examine, test and report on specific aspects of Smart Grid initiatives and technologies.

In order to undergo pilot testing, Hydro One is creating a geographic subset of its system as a Smart Grid demonstration area. Located in the Owen Sound area, the pilot will incubate Smart Grid applications, flesh out requirements for solution sets, while assessing opportunities for system-wide rollout, and establish design parameters and standards prior to full roll-out. Actual devices will be installed, various solutions built or upgraded as required, and business processes developed and tested. In addition, education and training may be required for local field resources needed to support the demonstration projects.

Hydro One's role in consumer demand management is to provide consumers with information and tools that allow them greater understanding and control over their electricity consumption, and help them reduce and shape that consumption. To this end, Hydro One has undertaken a number of initiatives to enable customers to respond in the manner they choose, including directly managing their own behaviour, offering incentive programs to dispose of energy inefficient appliances, purchase energy efficient equipment/technology, and to allow direct utility intervention and automation of their demand response.[17]

Time of Use Rate Examples - Commodity Cost Per Year

	Estimated Annual Commodity Cost		
	Off-peak (5.3¢/kWh)	Mid peak (8.0¢/kWh)	On-peak (9.9¢/kWh)
Clother dryer (1 load)	$24.96	$37.44	$45.76
Clothes washer (1 load/ hot wash) *	$63.96	$98.28	$120.12
Clother washer (1 load/cold wash)	$9.36	$14.04	$17.16
Vacuum cleaner (1/2 hour)	$11.44	$16.64	$20.80
Dishwasher (1 load) *	$49.40	$72.80	$93.60
AC Central 25 degrees (weekday)	$105.60		
AC Central 25 degrees (weekend)	$76.20		
AC Central 20 degrees (weekday)	$47.52		
AC Central 20 degrees (weekend)	$34.08		

* Cost of electric water heating included.

Source: Hydro One Networks Inc.[18]

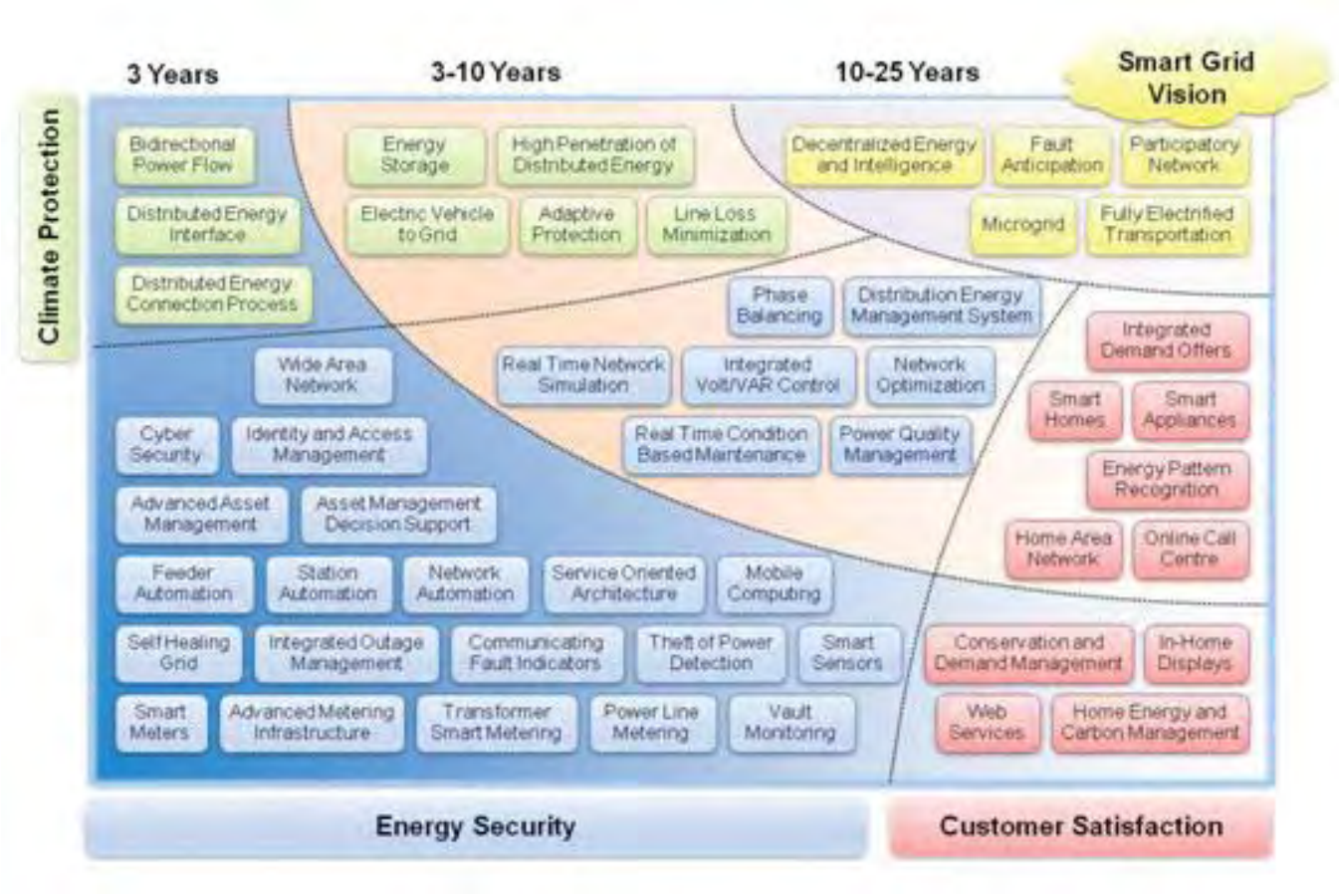
17 Hydro One currently offers four core OPA customer demand management programs to its customers, with contracts in place to continue doing so through 2010. These include: Great Refrigerator Roundup, Electricity Retrofit Incentive Program, PeakSaver®, and Power Saving Blitz. In addition, Hydro One is delivering one rate-funded program, PowerSaver® Plus online audit for its customers. Hydro One has also recently concluded a very successful demand response custom program approved by the OPA, Double Return and has undertaken a number of pilot programs, such as a zero interest loan and rebate pilot program for renewable energy technologies for the Ministry of Energy and Infrastructure.

18 Note, prices reflect commodity portion and not the utility's delivery charge which is the same at all times.

Hydro One will identify elements to be included in Hydro One's implementation of the Smart Grid through: acquisition of "smart devices" to showcase proposed technologies; acquisition of system integration technologies (both real-time and enterprise applications) that monitor, control and remediate faults, outage management/restoration systems, Geographic Information System ("GIS") technology, Energy Storage devices such as battery/compressed air energy storage ("CAES") as well as stationary power systems such as hydrogen fuel cells that can be used to power station services; deployment for proving both technology and inter-operability, as well as business benefits which will drive further adoption in other areas of Hydro One's networks.

Toronto Hydro key Smart Grid activities

Toronto Hydro has been proactively defining and planning for the Smart Grid since 2006 (see Smart Grid Roadmap below).



Source: Toronto Hydro Smart Grid Roadmap[19]

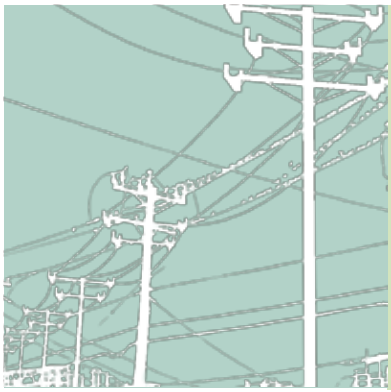
Toronto Hydro participates in the Ontario Smart Grid Forum, and the Advanced Feed-in Tariff which is a comprehensive program expected to substantially increase the deployment of renewable energies in Ontario. As well, it participates in the City of Toronto's "Change is in the Air: Clean Air, Climate Change, and Sustainable Energy Action Plan" — a municipal government policy that

19 See Toronto Hydro 2010 Electricity Distribution Rate Application: Exhibit G1 — Smart Grid, available online: http://www.torontohydro.com/sites/electricsystem/Pages/2010-rate-application.aspx.

includes becoming the renewable energy capital of Canada. The Smart Grid in Ontario will be built on elements that have been, are in the process of being, or will be, established.[20] These building blocks have enabled a wide array of functionalities to provide for the safe, reliable and efficient delivery of power. However, to achieve a Smart Grid, so as to enable advanced conservation schemes, accommodate a large penetration of distributed generation, and further improve on grid safety, reliability, and efficiency, new measures must be in place to expand the functionalities of these building blocks, construct integration paths, and develop new building blocks. Even while leveraging these foundational building blocks, much work will be required to achieve the Smart Grid. Toronto Hydro's Smart Grid Roadmap shows the timeline for implementation of climate protection, energy security and customer satisfaction goals.

Toronto Hydro Smart Grid projects touch on the following areas: customer display integration, web energy portal, OMS integration — customer portal, smart meter connect / disconnect, smart meter — outage identification, network meters integration, network monitoring integration, integration architecture and design, access network, internal network readiness, and smart grid network security.

20 Examples include: Advanced Metering Infrastructure ("AMI"), Distribution Automation, Distributed Generation, Asset Management, Enterprise Applications, Business Intelligence/Service Oriented Architecture, Communications, Conservation and Demand Management, Customer Enablement.



Personal Information on the Smart Grid

In Ontario, "personal information" is defined in the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) as "recorded information about an identifiable individual."[21] *FIPPA* and *MFIPPA* provide a range of non-exhaustive examples of what personal information can include. For example, "personal information" includes the address and telephone number of an identifiable individual and the individual's name where 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.[22] Also, personal information can include any identifying number, symbol or other particular assigned to the individual.[23]

For information to be identifiable, there must be a "reasonable expectation" that an individual can be identified from the information.[24] In determining whether such reasonable expectation is met, the circumstances of a case and the issues arising in it on a balance of probabilities must be examined.[25] The ability to link data with personal information is also a key consideration in determining the scope of personal information and has been the subject of past IPC decisions.[26] In the context of the Smart Grid, the linkage of any personally identifiable information with energy use would render the linked data as personal information. While the precise scope of personal information on the future Smart Grid is not known, utilities should be cautious in employing a definition of personal information that is overly narrow in data linkage scenarios involving information indicating personal behaviour, as well as unique smart meter or appliance data (e.g. serial numbers).

The collection, use and disclosure of aggregated or de-identified personal information raise little, if any, privacy issues. It is outside the scope of this paper to provide guidance on de-identification practices for Smart Grid energy consumption data, however there is sufficient basis in, for example, the health sector's experience to suggest that utilities should be cautious when anonymizing personal information and in concluding that that information is in fact anonymized.[27] For example, it is possible in some cases that removing identifiers such as name and address do not guarantee that personal information is de-identified.[28]

21 *FIPPA* & *MFIPPA* s. 2(1)

22 *FIPPA* & *MFIPPA* s. 2(1)(d)&(h)

23 *FIPPA* & *MFIPPA* s. 2(1)(c). In the past, the IPC has found that personal information can also include personal behaviour even if it is not linked with the individual's name (MO-2188). See also billing for power consumption as personal information (PO-1723).

24 *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 at 2.

25 *Supra*, at 6.

26 See for example linkage of personal information discussed in P-488, P-1076, MO-2134, and PO-2265.

27 See for example A. Cavoukian and K. E. Emam, *A Positive-Sum Paradigm in Action in the Health Sector*, available online: http://www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf. See also L. Sweeney, "k-Anonymity: A Model for Protecting Privacy", *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems* Vol. 10(5), 2002, pp. 557-570.

28 See for example IPC Orders P-722 and MO-2291.

Efforts to expand the definition of personal information beyond information linked to an identifiable individual are presently underway in California. A law, technology and public policy clinic at the University of California at Berkeley has developed the concept of "household energy data."[29]

While there is much discussion regarding what would constitute personal information on the Smart Grid, a determination that a particular set of data is personal information does not prevent the collection, use and disclosure of information that is necessary for the administration of Smart Grid programs. Rather, it serves to indicate that certain considerations in relation to that data must be taken into account. For example, considering the purpose for which the information was collected (called "primary purpose") is essential in determining appropriate disclosures of personal information. For example, the IESO's repository limits use and disclosure in the following manner:[30]

- Customers may only view data relating to their own consumption;
- Utilities may only see data relating to their own customers;
- Retailers may only see data relating to their own customers;
- Billing Agents may only have access to view billing quantities;
- Utilities may have the ability to edit Meter Reads for only their customers;
- Some users may not have the ability to view data;
- Only appropriately authorized users may have the ability to modify data.

The OEB's *Affiliate Relationships Code for Electricity Distributors and Transmitters* prohibits the release of consumer information (which could include personal information) to a utility's affiliate without the written consent of the consumer. An affiliate can be, for example, a subsidiary corporation under the utility or the utility's parent corporation. If there is more than one subsidiary corporation, than those corporations are also each other's affiliates.[31] The Code states that consent for disclosure must be obtained from the consumer, except to the extent that the disclosure is permitted by the utility's licence. Also, the code states consent is not required where the personal information is required to be disclosed for, e.g., billing purposes, law enforcement purposes, to comply with a legislative or regulatory requirement, or to process past due accounts that have been passed to a debt collection agency. Consumer information (which could include personal information) that has been sufficiently aggregated so that information relating to any individual consumer cannot reasonably be identified may also be disclosed to an affiliate.[32] The distribution licences for utilities contain similar provisions regarding disclosure of consumer information to any other party which would include a utility's affiliate or any other person or entity.

Disclosures of consumer information which comes within the definition of "personal information" as noted above must also meet the requirements of *FIPPA*, *MFIPPA* (where applicable) and any other applicable privacy legislation.

---

29 This concept could include "data collected about an individual household in the Smart Grid that is revealing of home life by itself or when analysed or combined with other information." Examples provided are: "near real-time energy usage data, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering data (e.g. thermostat temperature)." Comments Of The Center For Democracy & Technology Before the Department of Commerce, National Institute of Standards and Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy And Requirements, December 1, 2009, available online: http://www.cdt.org/files/pdfs/CDT%20Comment%20NISTIR%207628%20Draft%2012-02-09%20FINAL%20-%20updated.pdf.

The concept of household data also appeared in California bill SB 837 and stated: "The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, family, household, or residence including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, utility usage, and medical or employment history." [emphasis added]

30 IESO, Meter Data Management and Repository (MDM/R) Functional Specification, Issue 2.0, pp. 27, available online: http://www.smi-ieso.ca/MDMR_Specification/MDMR_Functional_Specification_v2.0.pdf.

31 *Affiliate Relationships Code for Electricity Distributors and Transmitters* at 1.2, definition of affiliate. See also *Business Corporations Act*, R.S.O. 1990, c. B.16, s. 1(4).

32 Note, the Code refers to consumer information which could be information about an identifiable individual *or entity* whereas *FIPPA* and *MFIPPA* refer to personal information about an identifiable individual only. The Information and Privacy Commissioner's Office has also considered the issue of disclosure of personal information in the context of an affiliate-type relationship. See MC-040015-1.

Digitization of smart meter information

The modern concept of privacy emerged in reaction to information and communications technologies in the late 1800s that suddenly made it possible to effectively capture, store and disseminate information on a mass scale never before contemplated, such as the photograph, telegraph and mass printing methods.[33] The appearance of mainframe computers, centralized electronic databases and computerized records in the 1960s and 1970s triggered the next wave of privacy protections. In response to the misuse of large-scale computerized databases by private organizations in the financial, credit and medical sectors, fundamental "privacy" principles came into widespread currency.[34]

The Smart Grid's impact is being compared to the advent of the Internet, which was built without privacy in mind, and which now faces an extreme impediment and very high levels of scrutiny regarding privacy. In fact, the scope of issues in relation to Internet privacy is so huge that they threaten its future viability. Almost all online activities require identity information to be given from one party to another. If one counts cookies and IP addresses as personal information, then Internet users leave behind a trail of personally identifiable information everywhere they've been — and they have little idea how that data may be used or how well it is protected.[35] However, unlike the Internet, consumers cannot opt out of the Smart Grid.

Information systems used by utilities in their 100 year history range predominantly from those that are paper driven to those that are highly automated and interactive. Increasingly, utilities are using information to plan, design, and implement integrated information sharing systems. These systems enhance the ability to collect, access, and use information, including personal information, and introduce the potential for information to be entered once but used multiple times across and between many different systems. When information is digitized (i.e. taken from a paper-based medium to electronic), the implementation of electronic information collection and sharing capabilities increases and results in concerns over the use, or potential misuse, of personal information contained in these systems. Digitized information, unlike paper-based information, can be massively disseminated, matched and merged, and used with ease for purposes far beyond those for which the information was originally collected in the first place.[36] While it is true that someone can sit outside a home and determine when the occupants are home, or read a meter posted outside the home, this only involves one meter and one individual collecting the information. Digital smart meter data, like all digital data, is vulnerable to copying and sending, and therefore lends itself to the possibility for a much larger dissemination of "comings and goings." Much like the creation of electronic health records, several privacy considerations arise as a result of digitization.[37] Privacy considerations in relation to the Smart Grid are canvassed in the IPC's paper *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* co-authored with the Future of Privacy Forum (available online www.ipc.on.ca).

---

33 See A. Cavoukian, Privacy by Design Book, Ch. 16, available online: http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook-ch16.pdf; S. Warren and L. Brandeis, "The Right to Privacy," *Harvard Law Review* Vol. 4(5), 1890, pp. 193, available online: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

34 *Ibid.,* Privacy by Design Book.

35 See A. Cavoukian, *7 Laws Of Identity: The Case For Privacy-Embedded Laws Of Identity In The Digital Age*, available online: http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf. E.g. Unlike the advent of the Internet, today's large-scale plans such as the U.S. broadband plan discusses embedding privacy at the outset. See National Broadband Plan: Connecting America, Ch. 4, available online: http://www.broadband.gov/plan/4-broadband-competition-and-innovation-policy.

36 IPC Order MO-1366: "A number of previous orders have identified that the format of information can affect the determination of whether disclosure would constitute an unjustified invasion of privacy … Order M-981 … Order P-1635 … M-849 … In the circumstances of the present appeal, I am satisfied that the disclosure of the personal information in electronic form, where it can be massively disseminated, matched and merged, and used for purposes far beyond those for which the information was collected in the first place, is a relevant factor to consider, and weighs significantly in favour of non-disclosure of the personal information in that format."

37 For an example of the many considerations involved with electronic health records, see A. Cavoukian and P. G. Rossos, *Personal Health Information: A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records*, available online: http://www.ipc.on.ca/images/Resources/phipa-toolforphysicians.pdf.

Changes experienced by utilities in implementing the Smart Grid

Leading the charge to the changing energy landscape is the shifting nature of information demands for utilities as power providers. The change is in part due to the large amount of information that utilities will be collecting from devices as a result of advancements towards the Smart Grid, such as the installation of smart meters and Intelligent Electronic Devices (IEDs). It is predicted that "[a] Smart Grid is expected to generate up to eight orders of magnitude more data than today's traditional power network."[38] Identified impacts of the Smart Grid on utility functions as it relates to consumers include the primary operation areas of home energy management, metering, and demand-side management.[39] Concern exists that utilities in other jurisdictions may be rushing ahead with Smart Grid implementation without fully considering the impacts on business processes.[40]

One key challenge in achieving the Smart Grid as envisioned relates to the fact that there are many communications, operational and information systems, and as a result there can be challenges with the level of integration between systems to achieve suitable utilization of the available information. The amount of data available from smart metering and Smart Grid devices will grow substantially and may require a significantly more robust means of validating, storing and filtering this data for optimal use. Additionally, two-way, high-data volume and frequency, and low-latency communications, may be required to support many of the Smart Grid operations, protections and control functions.

New technologies may be introduced arising from changes experienced by utilities in implementing the Smart Grid. In some instances this may involve using specific smart devices to monitor and/or adjust voltage levels and similar power conditions across lines and connection points. Smart energy regulators, capacitors, switches and power line monitors are technologies that can be used to support energy conservation by reducing energy losses, distributed generation penetration, plug-in vehicles, and improved reliability and management of utility assets. For Smart field devices challenges may lie in integrating diverse existing systems as well as applying information into new systems and services. [41]

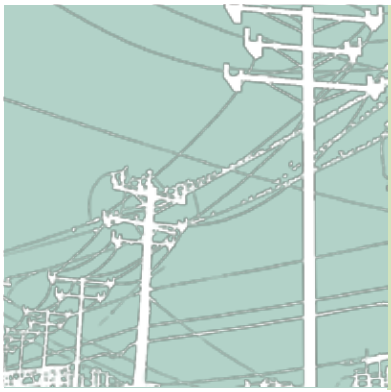
In addressing challenges arising from changes experienced by utilities in implementing the Smart Grid, utilities may find opportunities to adopt *Privacy by Design* when introducing new technologies, integrating communications, operational and information systems, as well as when updating business processes.

38 See http://newsroom.accenture.com/article_display.cfm?article_id=4971.

39 V Pothamsetty and S Malik, *Smart Grid: Leveraging Intelligent Communications to Transform the Power Infrastructure*, February 2009, pp. 9.

40 J Feblowitz and L. Goransson, *From Customer Service to Customer Engagement: Are Utilities Prepared for the Smart Grid Experience?*, February 2010, pp. 1. "Utilities are preoccupied with the implementation of physical infrastructure and have not thought through the implications of new technology and products on customer relationships or the business process."

41 Although technology solutions may be approaching commercialization, it is important to note that the right and best products should always be selected based on specific sets of criteria as part of a utility's Smart Grid strategy which embeds privacy (including security) considerations into the requirements of the program at the outset.



Privacy by Design: The Gold Standard for the Smart Grid

There is no technical reason to attempt to standardize all aspects of the Smart Grid today, if engineered and designed correctly.[42]

Privacy by Design and the 7 Foundational Principles (The Gold Standard) is the next wave of privacy. They incorporate universal principles of fair information practices, but go well beyond them, to seek the highest global standard possible, representing a significant raising of the bar.[43] We believe that *Privacy by Design* should be adopted as the Gold Standard for the Smart Grid.

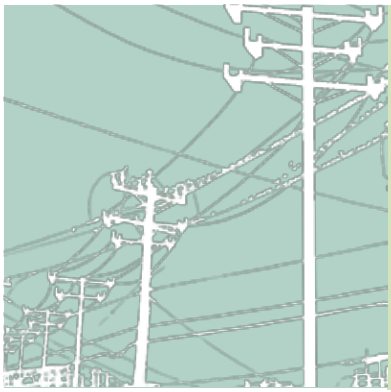
Privacy by Design is a concept developed by Commissioner Cavoukian back in the 90's, to address the ever-growing and systemic effects of information and communication technologies, and of large-scale networked data systems. *Privacy by Design* advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETs *Plus* — taking a positive-sum (full functionality) approach, not the dated zero-sum. That's the "Plus" in PETs Plus: the win/win of positive-sum, not the either/or of zero-sum.

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure. Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data. The strength of the privacy measures taken tends to be commensurate with the sensitivity of the data. The objectives of *Privacy by Design* – ensuring freedom of choice and personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles.

We have developed the following best practices for new Smart Grid projects by adapting the language and concepts contained in the IPC's paper *Privacy by Design: The 7 Foundational Principles* (available online at www.ipc.on.ca). While the vast majority of Smart Grid projects will not involve personal information, or will involve legacy systems that are not easily updated with *Privacy by Design* features, whenever there is an opportunity to incorporate *Privacy by Design* into existing systems that involve personal information, these best practices should be used.

42 Although technology solutions may be approaching commercialization, it is important to note that the right and best products should always be selected based on specific sets of criteria as part of a utility's Smart Grid strategy which embeds privacy (including security) considerations into the requirements of the program at the outset.

43 Smart Grid Standards Adoption: Utility Industry Perspective, Prepared for Smart Grid Utility Executive Working Group and OpenSG Subcommittee, available online: http://osgug.ucaiug.org/Shared%20Documents/Accelerating%20Smart%20Grid%20Standards%20Adoption%20final%20v5%20090302.doc.



Best Practices: Privacy on the Smart Grid

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring

Smart Grid projects involving consumer information require privacy considerations to be integrated into their development, right from the project inception phase. Identifying and incorporating privacy considerations into such requirements provides a solid foundation for *Privacy by Design* principles. Project development methodologies are commonly used for the successful development of any large scale networked data system solution (e.g. ISO12207, Unified Process, etc).

Include the 7 Foundational Principles of *Privacy by Design* in the requirements development and design processes, and subsequently to the building and testing systems for alignment with those requirements. The utility should conduct Smart Grid project privacy impact assessments (PIA) or similar type of assessments as part of the requirements and design stages, to allow incorporation into requirements and plans — right from the outset. For in-flight projects, the PIA or similar type of assessments can be conducted at a later time in the program if necessary, with any corrective actions incorporated at that time.

2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured

Consumer information, specifically personally identifiable information on the Smart Grid, must be strongly protected, whether at rest or in transit. Personally identifiable information that is communicated wirelessly or over wired networks should be encrypted by default — any exceptions should be assessed (risk-based) on the impact to customers of third party access. It is much harder to protect personal information when it is stored in multiple locations — keep personal information in a minimal number of systems from which it may be securely shared. Similarly, allowing need-only access to this information will provide an extra layer of protection. It is important to consider the manner in which third parties will be allowed to gain access, for various legitimate support purposes — there must be appropriate language built into the contractual agreements to safeguard consumers. There should be as little persistency of personal information as possible. At the end of the cycle, personal information must be securely destroyed, in accordance with any legal requirements.

3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature

Privacy must be a core functionality in the design and architecture of new Smart Grid systems and practices. However, these often involve refreshing the existing asset base, which previously had no real need to carry or transmit consumer information. It is understood that many utilities will be building onto existing legacy systems and that few will be able to work with a clean slate, but instead will need to introduce *Privacy by Design* principles into legacy systems as opportunities arise, to ensure the overall architecture is secure. It is important to understand how personal information is being handled within the enterprise and determine whether any adjustments need to be made due to challenges raised by new Smart Grid initiatives.

4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects

Beyond making privacy the default by embedding it directly into systems, achieving *Privacy by Design* entails the ability to embed privacy without any loss of functionality of Smart Grid related goals.

5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected

Ensure that the people, processes and technology involved in Smart Grid projects consider privacy at every stage, including at the final point of the secure destruction of personal information.

6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives

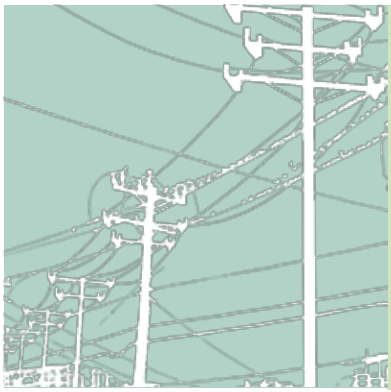
Records must be able to show that the methods used to both incorporate privacy as well as the Smart Grid objectives will meet the privacy requirements of the project. Ensuring such "requirements traceability" between the foundational privacy principles and each stage of Smart Grid project delivery will ensure that one is ready for a third party audit at any time.

Any non-compliant privacy deliverables will require an immediate remediation plan to correct the deficiency and provide an acceptable means of redress.

Informing consumers of the use to which personal information collected from them will be put is a key objective in achieving visibility and transparency.

7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement

From a consumer perspective, it is essential to provide the necessary information, options, and controls so that consumers may manage their energy, costs, carbon footprints, and privacy.



Smart Grid Privacy by Design Use Case Scenarios

Two use case scenarios are provided here to illustrate methods of incorporating *Privacy by Design* following a background description of privacy considerations for the Wireless Mesh Network. The two use cases are: 1) Customer Information Access and 2) Customer Enablement.

Background: The Wireless Mesh Network

Consider the scenario where a utility has a fully functional smart meter deployment across the majority of its client base. These smart meters communicate information back into the utility through a meshed wireless configuration, where designated meters and repeaters act as secure gateways, and data collectors aggregate information for transmission back into the utility's data centre. During this initial phase, utilities will make this information available to their customers to assist them in managing their power consumption. As part of the next phase in grid modernization, the utility would work with its smart meter supplier to pilot derivative meters that can monitor transformer performance. Information from these transformer meters can be used by the utility to back-check the accuracy of smart meters, drawing early warnings of transformer overload or power theft.

Providing customers access to their meter reading information has many challenges, such as the following: registration, authentication and data protection. The information needs to be presented in a simple and easy-to-understand manner that is useful in helping customers manage their energy needs efficiently.

A utility following Smart Grid *Privacy by Design* will consider how to best design information flows to mitigate potential future customer privacy concerns. Since the smart meter information is broadcast wirelessly over the air, the obvious first level of security would be to encrypt the information. The second is to ensure that the smart meter network does not broadcast any sensitive customer information over the airwaves. Designing systems to only pass on the minimum information required protects privacy — in the case of this scenario, a unique numeric ID and consumption data is all that needs to be transmitted. The smart meter-to-customer correlation is only performed securely back in the utility's data centre.

The utility can take the assessment to an even higher level by considering whether transformer meters should communicate over a different wireless network than the smart meters. The rationale for this is that if the smart meter network were ever to be compromised, malicious third parties could not perform the same transformer-to-smart meter correlation, as could the utility. By segregating the information over dual networks, the correlation could only be done by being in possession of both sets of information, which would only be available in the utility's own data centre. While the final solution may well be a single network, it is these added measures of due diligence that will result in a solution truly inspired by *Privacy by Design*.

Use Case Scenario 1) Customer Information Access

When a utility wishes to provide access to information, it must consider how to positively identify the customer during registration and upon each subsequent visit. This step is extremely important because unauthorized access to customers' information will erode trust and result in a loss of consumer confidence.

Such customer access may be required, for example, in order to provide additional information to assist them in making choices around energy, cost, carbon footprint, and privacy.

Ensuring that the registrant to the customer information access service is indeed the owner of the utility account, and that unauthorized access attempts are kept to a minimum, are depicted in the requirements illustrated in Figure 1 below.

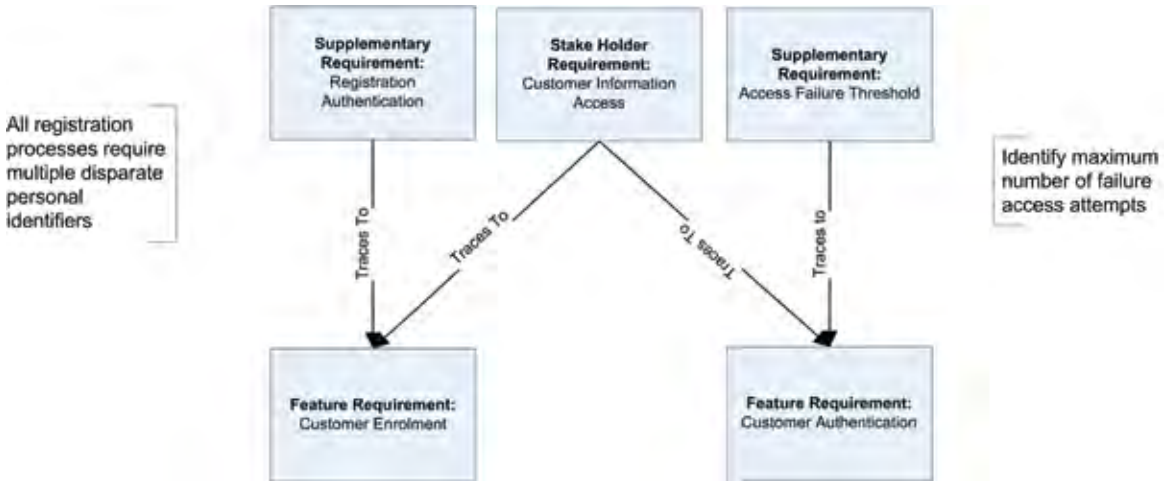


Figure 1 - Customer Information Access Requirements

The two features illustrated above, Customer Enrolment and Customer Authentication, are requirements defined by the utility. These two requirements will have supplemental requirements that may be traced to the features which apply privacy constraints upon them.

Figure 2 illustrates how a supplementary requirement such as an "Access Failure Threshold" can be incorporated and traced within the design of a Customer Information Access program, which would then be reviewed by the Smart Grid project team to ensure that it also meets their business needs:

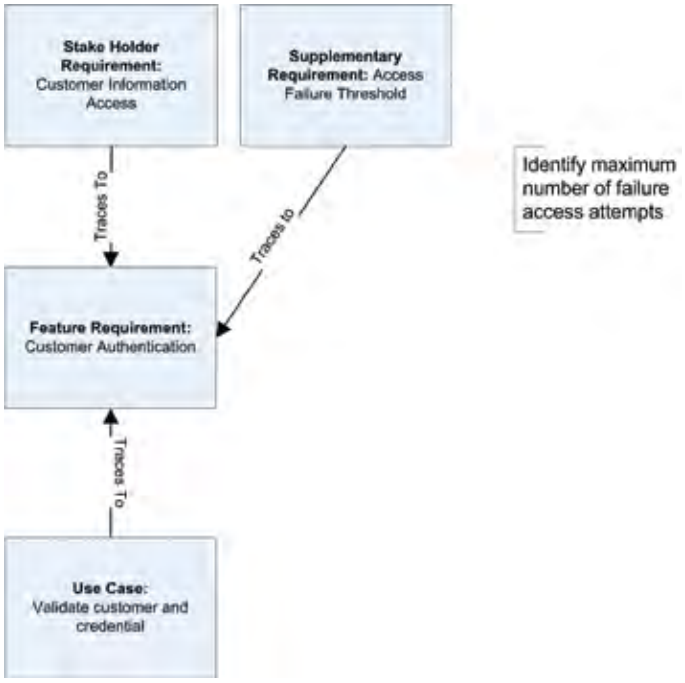


Figure 2 - Use Case Tracing for Customer Information Access

The requirement definition stage of any adopted Smart Grid project methodology involves the creation of one or more use cases to satisfy core foundational privacy requirements, such as "Access Failure Threshold," showing interactions between various actors (people and systems), as well as the functionality that will be delivered by the systems involved. For example, the diagram below illustrates four usage/operations case scenarios incorporating the same supplemental requirement of "Access Failure Threshold." They are: Authenticate Customer, Authentication Failure, Authentication Success and Welcome Page.

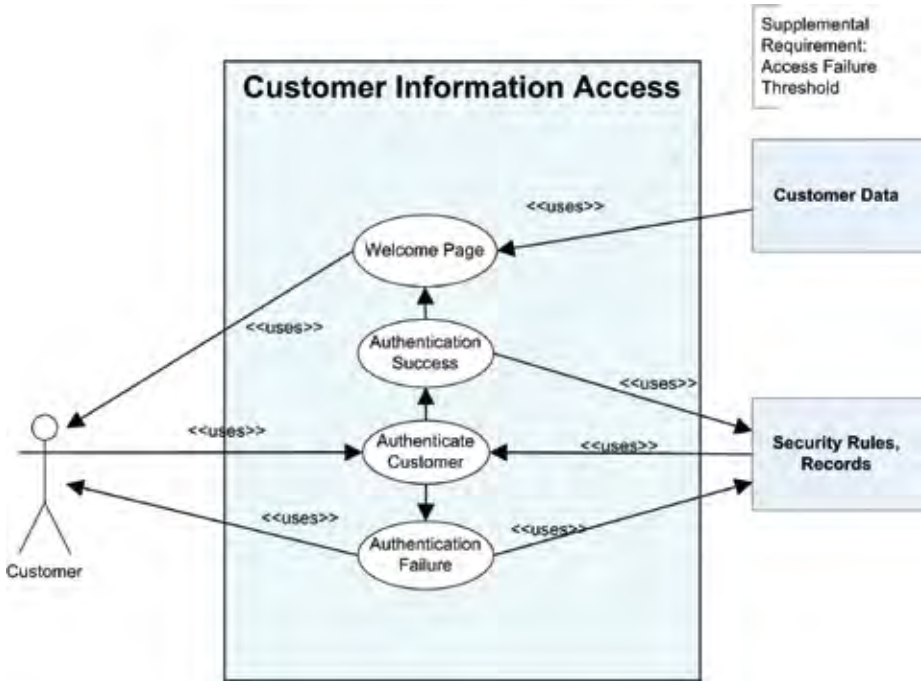


Figure 3 – System and Actor Diagram for Customer Information Access

The utility must then document all flows of information that would occur during customer authentication. The sequence presented is the successful access request. The steps are presented in Figure 4 below.

I. The customer provides his/her unique identifier and their challenge information.

II. The customer information access will require that the identifier and challenge information be verified. If correct and the account has NOT been disabled due to multiple access attempt failures, then the customer is considered to be authenticated.

III. The successful access is recorded.

IV. The basic information regarding the authenticated customer is then retrieved.

V. The customer is now presented with welcome information.

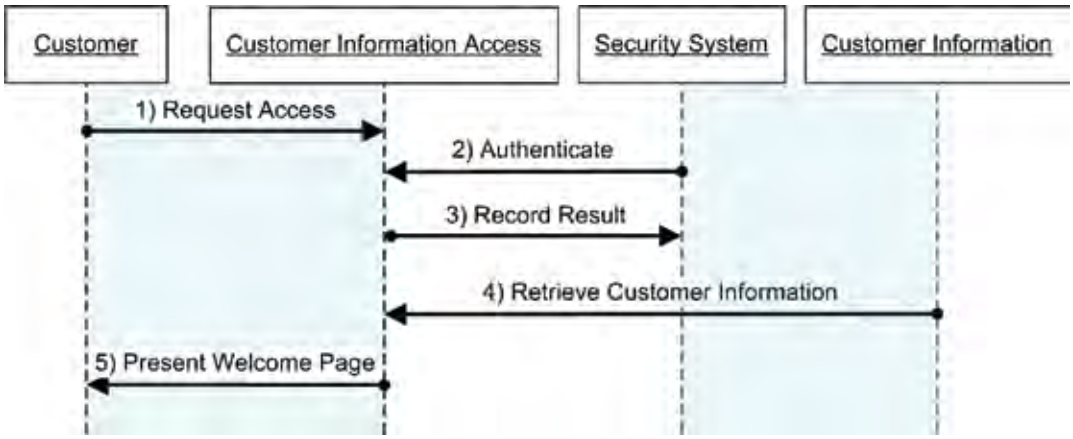


Figure 4 – Sequence Diagram for Customer Information Access

In this example, the requirement that all customers must be authenticated was illustrated. All access attempts are recorded, with multiple consecutive access failure attempts disabling the account. This requirement was developed to prevent unauthorized users from accessing an account by attempting to randomly create passwords.

Protecting access to customer information builds trust in the system, and thus increases the likelihood of customer participation to realize the benefits of the Smart Grid.

Use Case Scenario 2) Customer Enablement

A utility is in the process of rolling out smart meters and billing system changes to support time-of-use billing, and expects that future Smart Grid programs will include further customer enablement. Examples of future customer enablement include demand-response programs, conservation programs, voluntary curtailment, advanced device management, in-home displays, and many others. For the purpose of this use case scenario, consider the case of customers choosing to participate in demand-response programs, such as when there is a peak in power-demand and some customers have opted to make their thermostats available for a 2 degree Celsius reduction.

Within customer enablement, the concept of involving the customers in the dynamic management of the electrical grid provides opportunities for all stakeholders, and ultimately benefits the environment.

However, it also introduces new challenges, particularly in the realm of privacy and security. The success of a customer engagement program hinges on the utility's ability to empower willing customers to become active participants in their energy use and generation. This is broadly defined as "customer enablement" and covers the end-to-end scope of a customer's interaction with the utility's technology systems and processes. These interactions may be characterized as three basic activities:

I. *Enrolment* — The ability for an eligible customer to enrol and define their participation in programs offered by the utility.

II. *Usage* — The active operation and management of participating customers. This refers to the daily functioning of systems and processes for the utility to deliver the service. This area is often referred to as "Operation."

III. *Termination* — The ability for a customer to terminate their active participation.

In establishing customer enablement for this demand response program, the associated initiatives, from a simplified point of view, must consider several stages of deployment including establishing the objectives of the program, program definitions, and determining how customers can engage with the utility. In addition, establishing customer enablement in this project requires setting out how the program itself will run, including customer engagement and enrolment, registration programs, operations such as events requiring demand-response, and program life-cycle management and wrap-up. Below is an example of these requirements and their traceability:

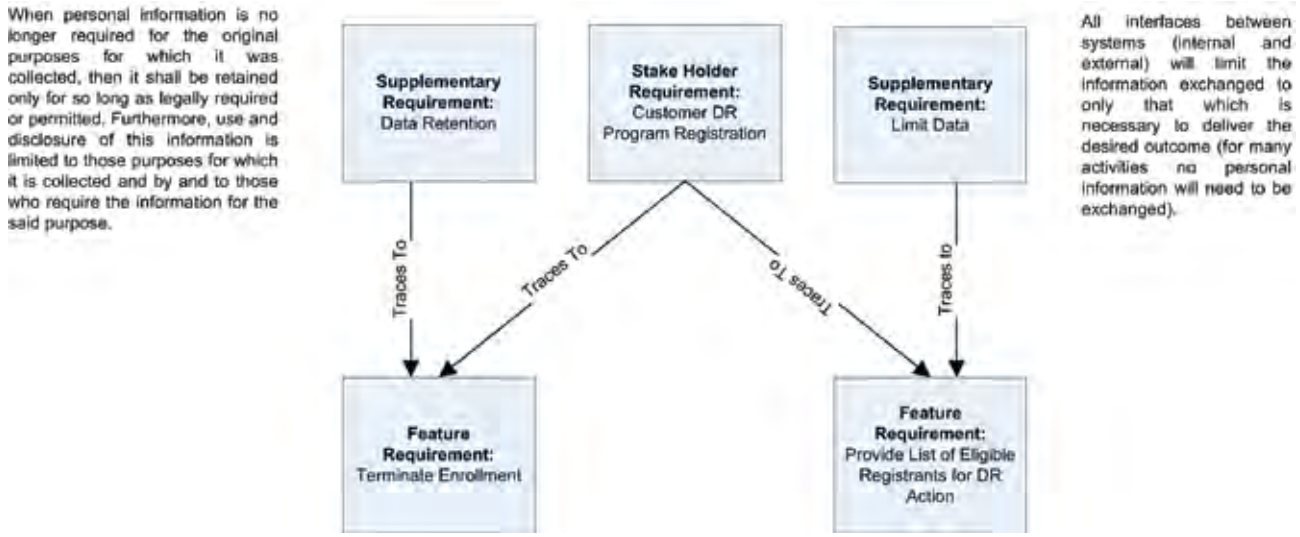


Figure 5 – Customer Demand Response Requirement Example

Note that the features being delivered are based on the business requirements to permit demand response registrants to terminate their enrolment and to provide eligible device information to a demand response program. Both of these have supplementary requirements placed on them to which the design and development teams must adhere. These supplementary requirements establish requirements for data retention, and requirements for what personal information is to be shared, or in this case, the opposite — limited, with downstream systems (i.e. limiting information only to that required for the particular purpose involved, "Limit Data").

The figure below illustrates how a supplementary requirement such as "Limit Data" can be incorporated and traced within the design of a demand management program, which would then be reviewed by the Smart Grid project team to ensure that it also meets their business needs:

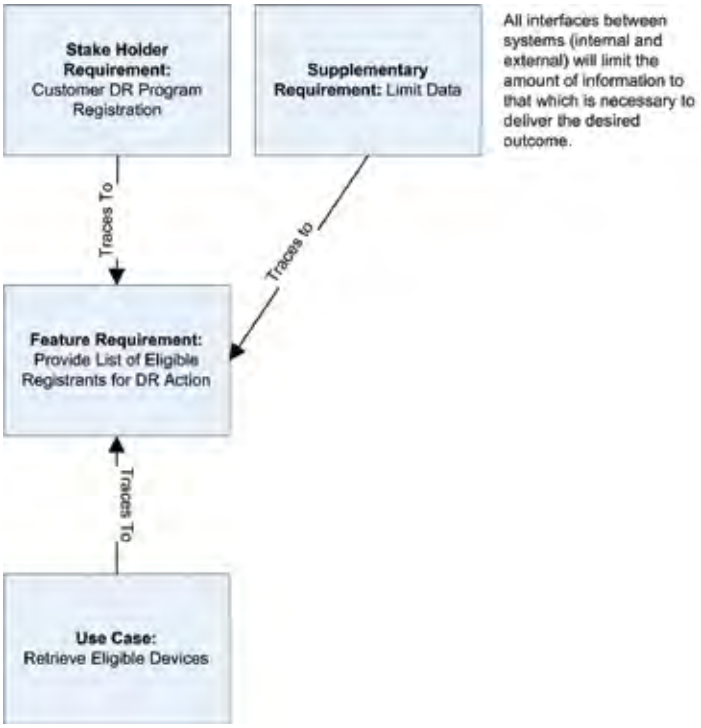


Figure 6 – Requirement Types for Demand Response Registrants

The requirement definition stage of any adopted Smart Grid project methodology involves the creation of one or more use cases to satisfy core foundational privacy requirements, such as "limit data," showing interactions between actors (people and systems), as well as the functionality that will be delivered by the systems involved. For example, the diagram below illustrates four usage/operations case scenarios incorporating the supplemental requirement of "limit data": Configure Program, Determine Program Action, Execute, and Retrieve Eligible Devices.

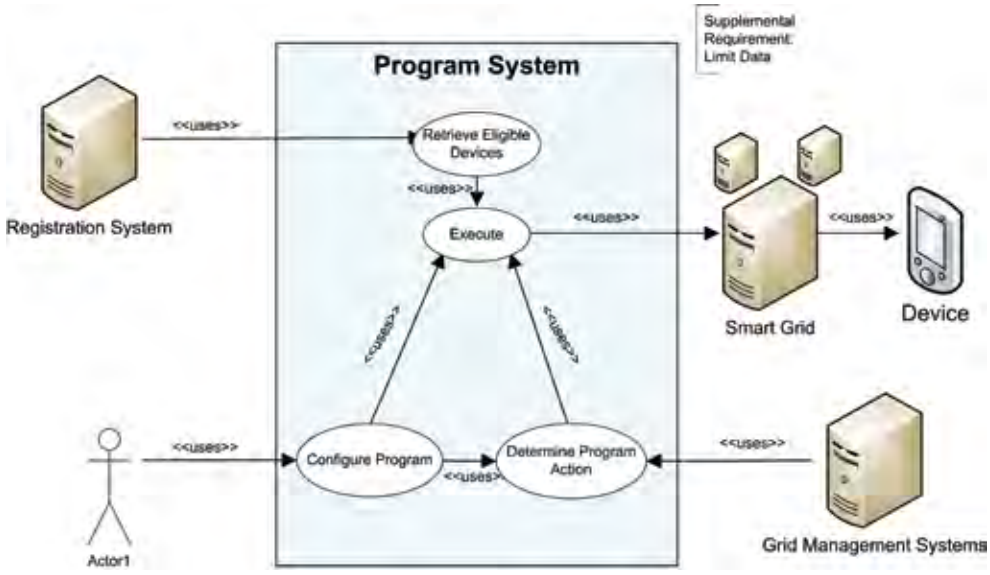


Figure 7 – System and Actor Diagram for Usage (part of Customer Enablement in the Smart Grid)

The utility must then document all flows of information that would occur in a demand response program (Figure 8 below), as follows:

I. ***Configure*** **—** Operators need to configure a program. This allows Hydro One to configure the behaviour of the demand response program when an event is received from the Smart Grid Management system.

II. ***Alert*** **—** The Smart Grid continually monitors the stability of the network and events are generated whenever problems occur (i.e. if demand exceeds supply).

III. ***Retrieve Devices*** **—** Based on configured rules in the demand response program, the system will determine how many consumer thermostats are needed to be adjusted to meet the DR need. At this point, the system is completely agnostic to specific customer data. It will retrieve device information from the registration system and will be limited to the device identifier and user constraints (e.g. minimum/maximum temperatures). Note: This is the essential step for the supplemental requirement to "Limit Data."

IV. ***Notify Device*** **—**The demand response system will request all the devices where the tolerances are allowable to change their temperature settings.

V. ***Deliver to Device*** **—** The Smart Grid ensures that the device is authenticated and the message is delivered securely to the device.

VI. ***Respond*** **—** Depending on the technology, a response will be provided to the request.

VII. ***Deliver Response*** **—** The Smart Grid ensures that the response is delivered to the demand response program system. The information is limited to an acknowledgement and state of action requested.

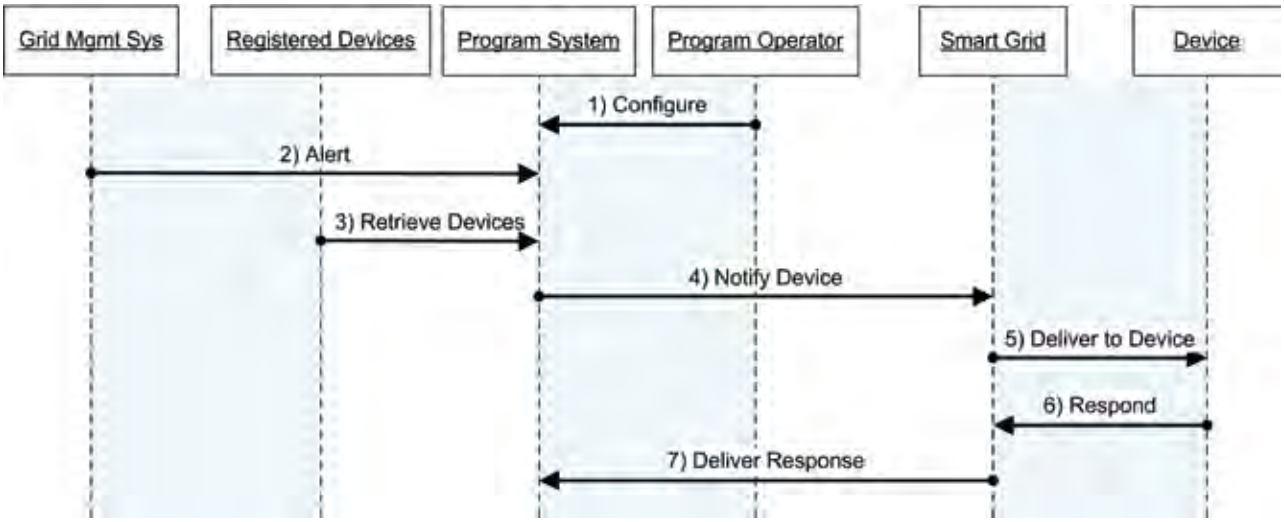


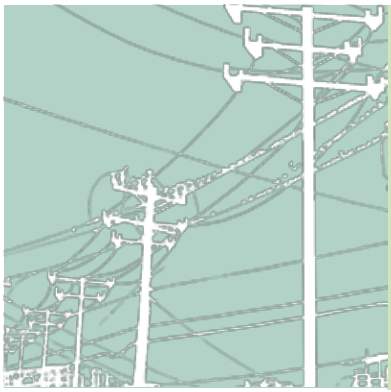
Figure 8 – Sequence Diagram for Usage (part of Customer Enablement in the Smart Grid)

In this example, the fundamental concept that underlies the entire flow is that the operating system executing demand response operations is completely blind to any of the specific, identifiable details of a given individual. Personally identifiable information is a function of program enrolment, but

this association operates separately from device management. In other words, the system running the Smart Grid only knows the rules for the management of devices based on the program it is associated with, and is completely agnostic to the particular details of a given customer.

This distinction demonstrates several tenets of the Smart Grid *Privacy by Design*. The segregation of data is proactively embedded directly into the system design — it is not a reactionary after-thought or mechanism that is tacked on to the initial solution. Similarly, privacy is the default — not something that must be asked for by the customer or initiated separately by the utility. Not only is this an elegant solution, but the most efficient option from an operations perspective; it also achieves the utility's goal of demonstrating a strong respect for user privacy.

Finally, all use case designs and implementation artefacts must be reviewed to ensure compliance with this requirement and any supplementary requirements. When the system is delivered, test cases specifically aligned with the use cases will be developed and exercised. If the implementation deviates from the design artefacts, then it will be identified as a defect, requiring remediation. Thus, privacy is not only embedded into the design of the system, it is verified after it is built (trust but verify), and then tested along with other requirements.

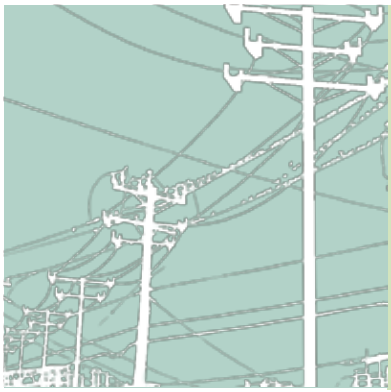


Conclusion

Utilities will face many challenges in their transformative role of revamping our current electricity system into a truly "Smart" Grid. We acknowledge that while a significant portion of the Smart Grid implementation will not involve consumer information, the amount of personal information being collected and the digital nature of that information will precipitate internal changes within utilities that go well beyond individual IT departments. The Best Practices for Smart Grid *Privacy by Design* were developed by the Information and Privacy Commission of Ontario (IPC) in collaboration with Ontario's largest electricity providers, Hydro One and Toronto Hydro, to be used by utilities in Ontario and elsewhere, that will be facing these challenges. We hope that our Best Practices will help utilities view the challenges posed by the Smart Grid as opportunities to enhance consumer trust by building *Privacy by Design* directly into their Smart Grid systems.

In Ontario, we have been working on the question of privacy and the Smart Grid for several years. Hydro One Networks and Toronto Hydro — both subject to the privacy laws that the IPC oversees compliance with — began their Smart Grid projects knowing at the outset that privacy became an essential component any time that personal information was involved. The Information and Privacy Commissioner's office embarked on work when first approached by the government several years ago on Bill 21, *Energy Conservation Responsibility Act, 2006*, which added amendments to the *Electricity Act, 1998* relating to smart meters, and the Smart Metering Entity.

Jurisdictions outside of Ontario may only be starting to enter into Smart Grid initiatives, such as the wide deployment of an advanced metering infrastructure. These utilities, now embarking upon Smart Grid initiatives involving the collection of personal information, may also benefit from these practices. In the U.S., for example, billions of dollars are being invested into new initiatives, fuelling the pace of Smart Grid implementation beyond the point where standards and practices around personal information are being fully developed. A point which bears repeating is that we must take great care not to sacrifice consumer privacy amidst a sea of enthusiasm for electricity reform. In this regard, other jurisdictions may benefit from our experience with building *Privacy by Design* into the foundational elements of all Smart Grid developments in Ontario.



Overview of Organizations

Information and Privacy Commissioner, Ontario, Canada

The role of the Information and Privacy Commissioner of Ontario, Canada is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under the three *Acts*, the Information and Privacy Commissioner: resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction; investigates complaints with respect to personal information held by government or health care practitioners and organizations; conducts research into access and privacy issues; comments on proposed government legislation and programs; and educates the public about Ontario's access and privacy laws.

Hydro One Inc.

Hydro One is the largest electricity transmission and distribution company in Ontario. Substantially all of Ontario's electricity transmission system is owned and operated by Hydro One. Its transmission system is one of the largest in North America based on assets, with almost 30,000 km of high-voltage transmission lines. Its distribution system is the largest in Ontario based on assets and spans roughly 75 per cent of the province, with over 123,000 km of wires serving approximately 1.3 million rural and urban customers, local distribution companies connected to the distribution system, and large industrial customers. Hydro One also operates, through its subsidiary, Hydro One Remote Communities Inc., small, regulated generation and distribution systems in a number of remote communities across Northern Ontario that are not connected to Ontario's electricity grid.

Toronto Hydro Electric System

Toronto Hydro Corporation is a holding company, which wholly-owns two principal subsidiaries: Toronto Hydro-Electric System Limited, distributes electricity and engages in Conservation and Demand Management ("CDM") activities. Toronto Hydro Energy Services Inc. provides street lighting services. The principal business of the Corporation and its subsidiaries is the distribution of electricity by Toronto Hydro-Electric System Limited. Toronto Hydro-Electric System owns and operates an electricity distribution system, which delivers electricity to approximately 690,000 customers located in the City of Toronto. It is the largest municipal electricity distribution company in Canada and distributes approximately 18% of the electricity consumed in Ontario.

Appendix A

The 7 Foundational Principles of Privacy by Design

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Lifecycle Protection

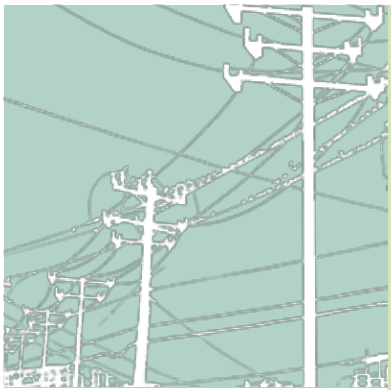
Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.



Appendix B

Electricity in Ontario

Electricity in Ontario is shaped by a framework that involves a mix of law, regulation, standards and mandatory codes. The *Green Energy Act, 2009* and legislation including the *Electricity Act, 1998* established a smart metering entity, smart meter procurement requirements and functional specifications. Objectives of the province of Ontario in implementing the Smart Grid include increasing the availability of renewable energy in Ontario and increasing the use of renewable energy sources in Ontario. In addition, it is the province's goal to stimulate the search for and development of sources of energy, to stimulate energy conservation through the establishment of programs and policies, and to encourage prudence in the use of energy in Ontario.[44] Through the *Green Energy Act, 2009*, the government of Ontario updated a suite of laws to achieve these objectives.[45]

The wires that make up the Ontario electrical grid are interconnected with the U.S. electrical grid, including full circuits. As a result, U.S. standards in the area of the Smart Grid are also applicable. The U.S.-based North American Electric Reliability Corporation (NERC) develops standards that Ontario utilities must comply with, as specified under international agreements. NERC is a "standards authority" within the meaning of Ontario's *Electricity Act, 1998* and Ontario is a member of NERC coordinating councils.[46] The U.S. National Institute of Standards and Technology (NIST) are also developing standards in the area of cyber security and interoperability for the Smart Grid which will impact Ontario utilities.[47]

Previously, the energy sector in Ontario was dominated by one government-owned company, Ontario Hydro. This sector was restructured in the 90s to allow for greater competition and supply of electricity. Today, there are several energy sector players in Ontario in the area of transmission, distribution, management of electricity, policy setting, and enforcement.[48]

Transmission of electricity is primarily the responsibility of Hydro One, which operates most of the transmission lines in Ontario. Hydro One distributes electricity to large industrial and local distribution companies, such as Toronto Hydro, that distribute power to homes, schools and small

44 See Appendix C for an overview of fair information practices. See also *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices* available online: http://www.ipc.on.ca/images/Resources/pbd-implementation-7found-prin.pdf.

45 *Ministry of Energy Act* , s. 8 (1)

46 *The Green Energy Act, 2009* also allows for the creation of regulations that would require public agencies and certain consumers to establish energy conservation and demand management plans. When government makes a capital investment or acquires goods and services, it will have to consider energy conservation and efficiency. The *Act* provides guiding principles for government facilities along these lines, and restricts sale or lease of appliances and products that do not meet efficiency standards, or labelling requirements. The *Act* also facilitates participation of aboriginal people and community groups in developing renewable energy generation facilities, and transmission and distribution systems.

47 Memorandum Of Understanding Between The Ontario Energy Board And The North American Electric Reliability Corporation: http://www.nerc.com/files/OEB-NERC-MOU-Final.pdf.

48 NIST 800-53/82, NISTIR 7628. In addition, utilities must comply with ISO standards such as 17799/27001.

businesses. Hydro One also distributes electricity directly to certain areas of the province, including rural areas.

The Independent Electricity System Operator (IESO) forecasts the short term demand for electricity; electricity generators in turn bid to sell energy at the specified price. This process is done every five minutes and thus operates as a real-time spot market. To ensure reliability of the electricity supply, the IESO also ensures that extra energy is available, should it be needed, by paying certain power generators to be on stand-by. The IESO is one of eight Independent System Operators in North America. One of the IESO's legislative mandates is to plan, manage, and implement the smart metering initiative in Ontario.[49] The Ontario Power Authority (OPA) is responsible for longer term planning of the supply of electricity in Ontario.

The Ontario Energy Board (OEB) is a regulatory body which, among other responsibilities, issues electricity licenses to participants in the electricity industry. The Board protects the interests of individual consumers regarding the price of electricity, as well as the reliability and quality of electricity. The OEB also conducted a Smart Price Pilot in June 2006 which was the first pilot in North America to both examine changes in energy consumption behaviour in response to three different types of time-of-use pricing (off-, mid- and on-peak; critical peak pricing; critical peak rebates).[50] The OEB's objectives include facilitating the implementation of a Smart Grid in Ontario; promoting electricity conservation and demand management, including having regard to the consumer's economic circumstances; and to promote the use and generation of electricity from renewable energy sources.[51] The Government of Ontario can issue directives to the OEB requiring that it take steps relating to the establishment, implementation or promotion of the Smart Grid in Ontario.[52]

Toronto Hydro and Hydro One are part of the Ontario Smart Grid Forum, spearheaded by the IESO and involving others in the field, including representatives from the Ontario government and the OEB. The Forum released its report *Enabling Tomorrow's Electricity System* in February 2009, calling for a co-ordinated effort to increase reliability, develop economic opportunities, and promote environmental sustainability through Smart Grid technologies. One of the report's key recommendations stated that consumers should have access to timely information on their consumption and price information from a smart meter with two-way communication capability or via the Internet.[53]

Policy for the delivery of electricity is set out by the Ontario Ministry of Energy and Infrastructure, including the introduction of smart meters and the *Green Energy Act, 2009*. Similar to other players in the sector, the Ministry's goal is to ensure that electricity is increasingly reliable in the future. The Ministry is also involved with bringing innovation to the electrical grid, and focusing on cleaner and renewable forms of energy.

When it comes to privacy, data protection and transparency, the Ministry, OEB, IESO, OPA, Hydro One and Toronto Hydro all come within the oversight jurisdiction of the Information and Privacy Commissioner of Ontario.

---

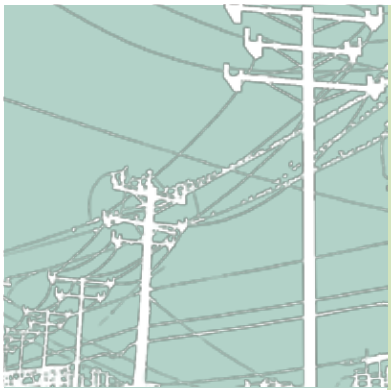
49 As Ontario Power Generation (OPG) does not handle personal information, they are not discussed in this section. OPG is the largest power generator in Ontario and produces 70 to 80 per cent of Ontario's energy. Its sources of electricity generation are hydroelectric, nuclear and fossil fuel.

50 *Electricity Act, 1998*, Ontario Regulation 452/06 Additional Objects of the IESO.

51 Consumption of electricity lowered by 5.7, 25.4 and 17.5 respectively. See Backgrounder: Ontario Energy Board Smart Price Pilot, July 26, 2007, available online: http://www.oeb.gov.on.ca/documents/communications/pressreleases/2007/press_release_smartpricepilot_backgrounder_20070726.pdf.

52 *Ontario Energy Board Act, 1998*, S.O. 1998, c. 15, Sched. B, s. 1(1)

53 *Ibid.*, s. 28.5 (1)



Appendix C

Fair Information Practices

By the late 1970s, information and communication technologies were facilitating a growing global trade in, and processing of, personal data. As various countries passed laws restricting the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data, worries arose that global trade would be constrained by the growing patchwork of national laws. In a far-sighted initiative, members of the Organisation for Economic Co-operation and Development (OECD) came together and agreed to codify a set of principles that might serve as a framework for countries to use when drafting and implementing their own laws. The result was the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Since 1980, these voluntary "fair information practices" (FIPs) have been widely adopted around the world in statutes, standards, codes of practice, information technologies, and in norms and common practices. In Canada, for example, businesses, consumers and the government agreed to adopt a comprehensive set of privacy practices, known as the Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) or CSA Privacy Code (see below), which was subsequently incorporated in its entirety into Canada's private sector privacy law.[54] The Ontario *Freedom of Information and Protection of Personal Information Act* and municipal counterpart base their privacy protection rules on fair information practices, which are the basis for privacy legislation in most jurisdictions around the world.[55]

The National Institute of Standards and Technology (NIST) in the United States has primary responsibility to coordinate development of a framework for the Smart Grid that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems. Since advancing the Smart Grid is a priority for the Obama administration, NIST has expedited its standards development process. In its Second Draft Smart Grid Cyber Security Strategy and Requirements (NIST IR 7628) document, NIST uses fair information practice principles in discussing privacy considerations for the Smart Grid.[56]

In Ontario, utilities have been adhering to privacy law and fair information practices for years.

- Hydro One's Privacy Code reflecting these practices is available publically at: http://www.hydroone.com/OurCompany/Documents/privacy_code.pdf.

54 *Enabling Tomorrow's Electricity System: Report of the Ontario Smart Grid Forum*, available online: http://www.ieso.ca/smartgridreport.

55 See Schedule 1, *Personal Information Protection and Electronic Documents Act*, (2000, c. 5). See also A. Cavoukian, Privacy by Design, Ch. 16, available online: http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook-ch16.pdf. While there is a range of privacy principles (or 'fair information practices principles'), with OECD privacy principles at the beginning of the privacy spectrum, Privacy by Design the next wave of privacy protection principles. See next section.

56 See http://www.nist.gov/smartgrid/.

- Toronto Hydro's Privacy Policy Statement reflecting these practices is available publically at: http://www.torontohydro.com/sites/electricsystem/pages/privacypolicy.aspx

See below for the CSA Privacy Code principles:[57]

1. Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

57 Privacy principles are found in the principles from the OECD Privacy Principles, the Generally Accepted Privacy Principles (GAPP), principles from ISO/IEC 27001, and concepts from ISTPA. The Global Privacy Standard modernizes the FIPs in the digital world, see: http:// http://www.ipc.on.ca/images/Resources/gps.pdf.

Information and Privacy Commissioner
Ontario, Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

Hydro One Inc.
483 Bay Street
North Tower, 15th Floor Reception
Toronto, Ontario
Canada M5G 2P5
Web site: www.hydroone.com
Telephone: 416-345-5000

Toronto Hydro Electric System Ltd.
14 Carlton Street
Toronto, Ontario
Canada M5B 1K5
Web site: www.torontohydro.com
Telephone: 416-542-3100

June 2010

Information & Privacy Commissioner of Ontario