An Examination of Smart Grid Privacy in Ontario

Engineering and Public Policy

Prepared for
Dr. Gail Krantzberg

Roy Raghavan

September 23, 2010

Abstract

The development of the Smart grid in Ontario represents a modernization of the electrical grid that fundamentally changes the relationship between a local utility and its customer. Through smart meters and devices that communicate directly to local utilities, the smart grid promises to empower customers by allowing he or she to have a much more active role in monitoring and managing their energy usage. However, it is feared that these smart devices could reveal personal information to a local utility, thus invading a customer's privacy by potentially exposing his or her habits and/or behavior inside their own home.

To ensure that privacy is part of the core functionality of the Smart grid, the Information and Privacy Commissioner of Ontario has advocated that local utilities adhere to Privacy by Design principles. These principles provide a proactive approach to privacy, where threats are anticipated before they occur. Since the exact design and scope of the Smart grid is not entirely known, many challenges still exist. These include addressing any misconceptions the public may have of smart grid initiatives, sorting out conflicting visions of the Smart grid, and determining the extent of third party access to Smart grid data.

To address these challenges, it is recommended that local utilities and the Ministry of Energy take a much more active approach in educating the public on privacy issues. In addition, clear boundaries need to be established to determine the extent and type of smart grid data that should be available to third parties, as well as procedures to ensure that personal information is never revealed without the consent of the customer.

Introduction

The development of smart grid technologies is a major transformation of Ontario's power infrastructure that will change the way electricity is generated, transmitted, and consumed. It will replace a grid system that is largely viewed as outdated, inefficient and inadequate to deal with future challenges such as climate change. It is believed that transitioning to a Smart grid will deliver several benefits including (1) the ability to deliver energy more efficiently, (2) enabling customers to have greater control over their power consumption, (3) the ability to accommodate an increasing number of electric vehicles and, (4) the ability to significantly reduce carbon emissions (World Economic Forum, 2009, p. 3).

However, the introduction of smart grid technologies also exposes significant social implications that may not yet be fully understood, most notably the issue of consumer privacy. It is feared that the data obtained from smart grid technologies has the potential to reveal intimate details about a particular consumer's habits and/or behavior in their everyday life (McDaniel & McLaughlin, 2009).

The Smart Grid in Ontario

In Ontario, there are several bodies responsible for different aspects of the Smart grid. The *Ontario Ministry of Energy* (M.E.) is the provincial ministry responsible for formulating energy policy in the province, and has legislative authorities for several agencies including:

- *The Independent Electricity System Operator* (IESO) – The agency responsible for directing the flow of electricity to the grid. The IESO forecasts electricity demand and accepts bids from generators to provide the required amount of power needed to meet demand.
- *The Ontario Energy Board* (OEB) – The provincial regulatory body responsible for the electricity and natural gas sectors.

- *The Ontario Power Authority* (OPA) – The agency responsible for developing the province's energy plan. Its goals include for ensuring an adequate, long term supply of power for the province while undertaking initiatives that will meet conservation targets.

In addition to these agencies, local utilities play a big role in smart grid initiatives. Local utilities, of which there are currently 80 in Ontario, are responsible for distributing power from transmission lines and distributing it to mainly residences and small businesses.

Privacy in Ontario

Privacy issues in Ontario are reviewed by the Office of the Information and Privacy Commissioner of Ontario (IPC), an independent body whose role is to "uphold and promote open government and the protection of personal privacy in Ontario" (Information and Privacy Commissioner, 2010). The current commissioner is Dr. Ann Cavoukian. The mandate of the IPC is derived from three pieces of legislation: *the Freedom of Information and Protection of Privacy Act (FIPPA)*, *the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, and *the Personal Health Information Protection Act (PHIPA)*. Part of the mandate of the IPC includes (Information and Privacy Commissioner, 2010):

- Independently reviewing the decisions and practices of government organizations with respect to privacy and access
- Providing input on proposed government legislation
- Conducting research on issues related to privacy and access
- Educating the public on Ontario's access and privacy laws

With respect to privacy protection, the role of the IPC is to safeguard personal information held by the government. The term "personal information" is defined in FIPPA as:

> *recorded information about an identifiable individual, including,*

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name 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; ("renseignements personnels")

The challenge policy makers now confront will be to ensure that individuals are satisfied that their personal information is protected and handled appropriately, all while maintaining full functionality of the smart grid system (World Economic Forum, 2009, p. 30). This paper focuses on the issue of smart grid privacy, and examines Ontario's current measures and practices with respect to this issue while identifying some key challenges. Policy recommendations are also offered as a means of enhancing Ontario's current smart grid privacy practices.

The Smart Grid

The term 'Smart grid' can often have a broad definition, but can generally be defined as an electrical system that enables two-way flows of electricity and information, in an attempt to reduce costs, increase reliability and efficiency, and to save energy (Ontario Smart Grid Forum, 2008). To achieve these goals a wide variety of tools are utilized, including sensors, monitoring, communications and automation equipment (Ontario Smart Grid Forum, 2008). In Ontario, the term is defined in the Electricity Act, which states that a Smart grid is:

> *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.*

The definition in the electricity act is rather broad as there still is some uncertainty as to what exactly the "final" smart grid will consist of or what it will be able to achieve. A report from the Ontario Smart Grid Forum suggests that the concept of the smart grid goes beyond the modernization of transmission and distribution systems, but also includes devices and systems that will: (1) allow consumers to manage their electricity usage, (2) find new ways of creating and storing electricity and, (3) anticipate and accommodate the widespread adoption of electric vehicles (Ontario Smart Grid Forum, 2008).

Figure 1: Smart Grid Network (Source: Electric Power Research Institute)

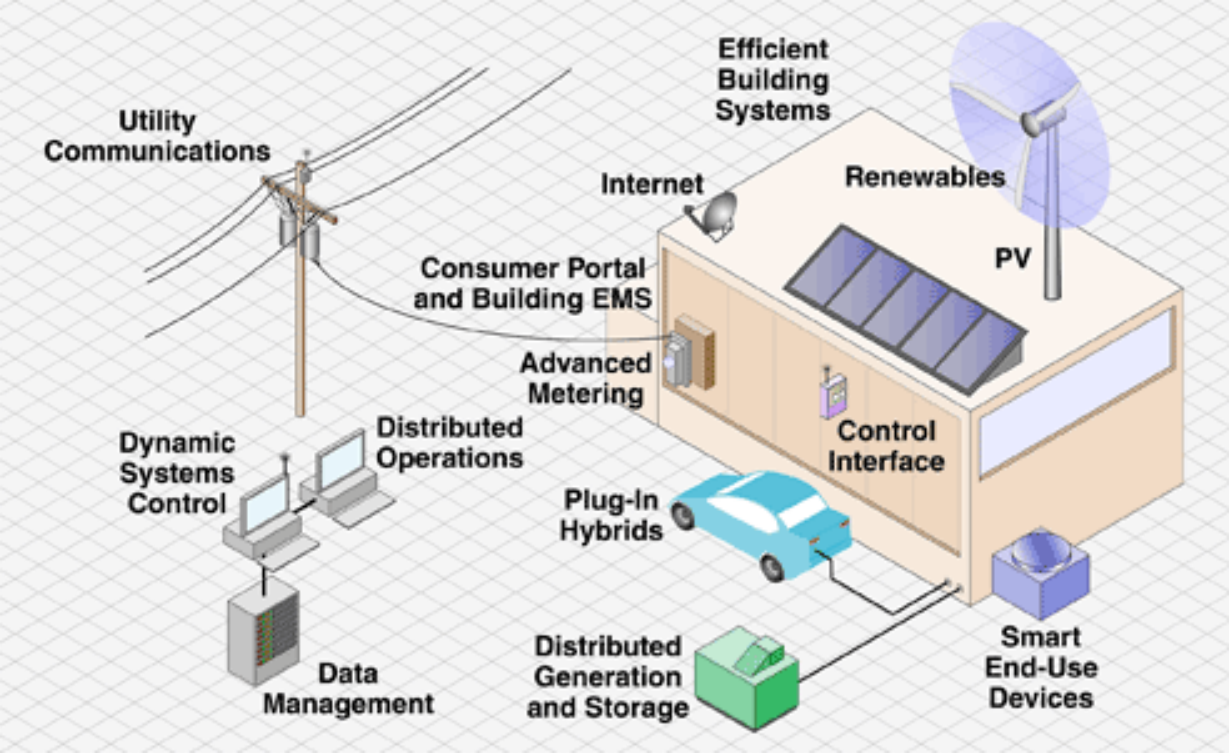


Figure 1 shows one interpretation of what a Smart grid may look like. Smart grid implementations are currently under way in many jurisdictions including the United States. The US Department of Energy's vision of the smart grid is an electrical system that exhibits the following characteristics (U.S. Department of Energy, 2008):

1. *Intelligence* – a system that is capable of sensing system overloads and re-routing power to prevent or minimize a potential outage. A system that works co-operatively in aligning the goals of utilities, consumers, and regulators.

2. *Efficiency* – a system capable of meeting increased consumer demand without adding infrastructure.

3. *Accommodating* – a system that can accept "energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas;" and capable of integrating energy storage technologies.

4. Motivating – a system that enables "real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns"

5. Opportunistic – a system that creates "new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate"

6. Quality-focused – a system "capable of delivering the power quality necessary – free of sags, spikes, disturbances and interruptions"

7. Resilient - increasingly resistant to attack and natural disasters as it becomes more decentralized and reinforced with Smart Grid security protocols

8. Green – a system that will slow "the advance of global climate change and offering a genuine path toward significant environmental improvement"

The Smart grid will represent a fundamental change in how consumers use their electricity. It is hoped that the consumer will be able to take a much more active role in managing their power usage, allowing them to reduce their cost, consumption and carbon footprint. Although a wide variety of smart grid technologies exists, this paper will only briefly describe the concepts of smart metering and smart appliances, two technologies that interact closely with consumers.

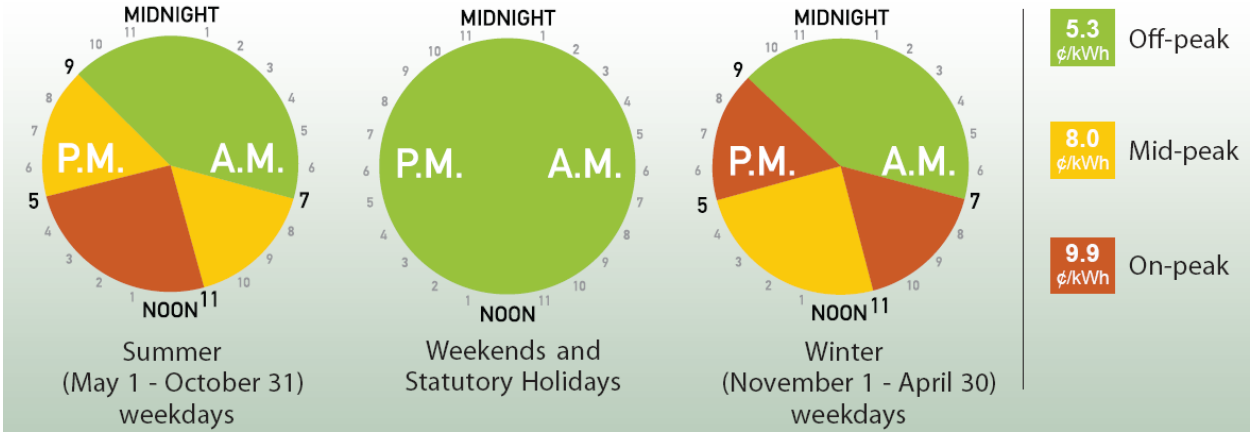
Smart Grid Technologies

Smart Meters

Smart meters are the technology most often associated with smart grid initiatives, with the two terms occasionally (and mistakenly) used interchangeably. Smart meters in particular seem to garner much of the attention from a privacy standpoint, most likely due to the fact that it is a technology that is directly visible to the consumer. The provincial government has mandated that all utilities install the device, which will replace the conventional electromechanical meters, to all small business and residential

customers by December 2010 (Hydro Mississauga, 2008). The meter will enable electricity readings to be electronically sent back to local utilities periodically (at least once an hour), avoiding the need for a technician to visit the premises to record meter data (Ontario Smart Grid Forum, 2008). One of the major touted benefits of smart meters is its potential to empower consumers by allowing them to manage and control their electricity usage much more effectively, by allowing them to financially benefit from shifting power usage to "non-peak" hours. Smart meters will enable local utilities to implement time-of-use (TOU) pricing schemes, where consumers will pay electricity rates based on the time of day power is used. This is in contrast to the conventional meter which only records total power usage without regard to the time of day it was consumed. Figure 2 shows TOU prices in Ontario effective May 1, 2010.

Figure 2: Ontario Electricity TOU Price Periods (Source: Ontario Energy Board)



Through smart metering and the implementation of TOU pricing, consumers can make a conscious choice of shifting their power usage to non-peak hours and realize a substantial financial benefit (a reduction of 4.6 cents/kWh) while simultaneously helping utilities by reducing demand during peak hours. TOU rates will apply to all electrical consumers by the summer of 2011 (Power Stream, 2010).

Smart Appliances

Smart Appliances generally refer to devices which have the ability to operate with a certain degree of autonomy, in ways that are beneficial to the user (Association of Home Appliance Manufacturers, 2009). For example, a smart appliance may consider the TOU electricity rate to determine whether it should it operate, and to what degree. The US Association of Home Appliance Manufacturers (AHAM) - the trade association for the industry whose members include major, portable, and floor care home appliances - defines the term smart appliance as the "modernization of the electricity usage system of a home appliance so that it monitors, protects and automatically adjusts its operation to the needs of its owner" (Association of Home Appliance Manufacturers, 2009, p. 6). The association describes the general requirements and features of a smart appliance, including (Association of Home Appliance Manufacturers, 2009, pp. 6,7):

- *Dynamic electricity pricing information is delivered to the user, providing the ability to adjust demand of electrical energy use.*
- *It can respond to utility signals, contributing to efforts to improve the peak management capability of the Smart Grid and save energy by –*
    - *Providing reminders to the consumer to move usage to a time of the day when electricity prices are lower, or*
    - *Automatically "shed" or reduce usage based on the consumer's previously established guidelines or manual overrides.*
- *Integrity of its operation is maintained while automatically adjusting its operation to respond to emergency power situations and help prevent brown or blackouts.*
- *The consumer can override all previously programmed selections or instructions from the Smart Grid, while insuring the appliance's safety functions remain active.*

- *When connected through a Home Area Network and/or controlled via a Home Energy Management system, Smart Appliances allow for a "total home energy usage" approach. This enables the consumer to develop their own Energy Usage Profile and use the data according to how it best benefits them.*
- *It can leverage features to use renewable energy by shifting power usage to an optimal time for renewable energy generation, i.e., when the wind is blowing or sun is shining.*

It is important to note that the above features and requirements are gathered from a manufacturer's association and that because Smart technologies are still in its early stages, the features and requirements of smart appliances may differ to what local utilities, government and consumers envision.

Smart Grid Concerns

While the potential of the smart grid to empower customers is no doubt appealing, there does exist significant concerns around smart grid technologies, most notably those related to privacy. For example, as smart meters will potentially be able to monitor electricity usage in as little as five minute intervals, the technology will offer unprecedented detail with respect to electricity consumption, posing some legitimate concerns around privacy.

One of the most common privacy fears expressed with respect to the smart grid is the potential of local utilities to gather detailed individual electricity consumption usage data (Utility Consumers Action Network, 2010). It is feared that this data could then be potentially used to derive usage patterns of individual consumers, perhaps exposing a particular customer's habits and/or behavior (McDaniel & McLaughlin, 2009). For example, some electrical appliances, such as a television, exhibit a "detectable power consumption signature" which could be tracked, identified and potentially exploited by a local utility (McDaniel & McLaughlin, 2009). By applying modern analytic techniques to an electricity usage profile, Quinn states that "the potential for gleaning potentially private information from this data is

truly staggering, including when a resident showers, watches TV, and how often she prefers microwave dinners to a three-pot meal" (Quinn, 2008). Essentially, electrical utilities could have access to information regarding what an electrical consumer is using, when it is being used, and the type of device(s) that are involved, which could potentially be used for purposes other than that of providing electricity, for example, target marketing (Cavoukian, Polonetsky, & Wolf, 2010).

To illustrate the potential information that can be revealed through smart grid activities, it is believed that the following are examples of information that could potentially be obtained through end-user components such as smart appliances (Cavoukian, Polonetsky, & Wolf, 2010):

- Whether individuals tend to cook microwavable meals or meals on the stove;
- whether a household has breakfast;
- the time at which individuals are at home;
- whether a house has an alarm system and how often it is activated;
- when the TV and/or computer is on;
- whether lights and appliances are used at "odd hours";
- whether and how often exercise equipment such as a treadmill is used;

In addition, Cavoukian et al warns that the information can be even more intrusive and revealing if it is combined with other information obtained from other sources (Cavoukian, Polonetsky, & Wolf, 2010). This could include information such as work hours and the age of residents. Smart grid data combined with this "outside" information may make it relatively easy to draw assumptions regarding consumer personal behavior and/or habits. For example, the following characteristics about an individual may be derived from such information (Cavoukian, Polonetsky, & Wolf, 2010):

- the individual has trouble sleeping and may be sleep deprived;

- an occupant leaves late for work;
- an occupant rarely washes his/her clothes;
- a person leaves his/her children home alone;
- an occupant exercises infrequently;

Quinn raises deep concerns regarding the potential use of such data as he states that "the richness and detail of the insights provided by this newly refined and individualized information is matched only by the number of potentially troublesome uses for such data, which range from the targeted and nefarious to the structural and discriminatory" (Quinn, 2008).

In addition, the scope of the data that will be collected from smart meters and from the smart grid is still unclear. Privacy advocates have expressed concerns about the type of information that will be collected, including the type and amount of billing, usage and appliance information flowing through the smart grid (Utility Consumers Action Network, 2010). If not properly regulated, it is feared that the smart grid could potentially provide a form of real-time surveillance of individuals inside their home.

Access to Information

While protecting consumer privacy is generally regarded as beneficial to the public and society, there are potential consequences to having a smart grid system that is either too restrictive or overly protective of customer data. One of these consequences is that it may exclude researchers from obtaining data that may be of interest to the scientific community. For example, cellular phone records have provided scientists with data on human mobility trends, making it possible to predict movement patterns (Timmer, 2010). These data records are potentially useful in such fields such as urban planning and disease/virus control (Johnston, 2010). With respect to the smart grid, Beyea argues that the full scientific, economic, and historical potential of smart grid data may not be fully understood, and its

usefulness may indeed exceed beyond the original purpose for which it was stored (Beyea, 2010, p. 979).

Social scientists and energy researchers could be interested in smart grid data to study a variety of issues. These may include studying the correlation between energy usage versus current events, appliance standards, or price (Beyea, 2010). Changes in energy usage could be studied between peoples, regions and over various time scales (Beyea, 2010). Another possibility would be for researchers to obtain smart grid information with geographical information tied to it, such as province, municipality and town (Beyea, 2010). Responses to events such as rapid weather changes, changes in public policy or even national tragedies could be tracked and analyzed (Beyea, 2010). Beyea suggests that smart grid data could even be used for health studies. For example, an algorithm could be developed to determine how many times a day a fridge door was opened to aid researchers with dietary and obesity studies (Beyea, 2010). The potential for research highlights the need to find a balance when formulating policies regarding smart grid privacy. It is essential that user privacy is protected; all while implementing procedures that will allow academics to access information for research that could immensely benefit society.

Privacy

The challenge of protecting privacy lies in providing secure communication channels to ensure that personal information is never compromised. A brief explanation of how data is collected from the home to where it is eventually stored and the type of data currently being collected by utilities is provided in Appendix 1. The issue of Smart grid privacy was the subject of a joint publication by the IPC, Hydro One, and the Toronto Hydro Corporation. The publication advocates the use of Privacy by Demand (PbD)

principles as a means of guiding local utilities to embed privacy in its AMI. This concept was developed in the 90's by the current Information and Privacy Commissioner, Ann Cavoukian.

Privacy by Design

The goal of PbD is to ensure "the protection of privacy through the use of privacy enhancing technologies—embedding them into the design specifications of information technology, business practices, physical environments and infrastructure—making privacy the default" (Cavoukian, Polonetsky, & Wolf, SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation, 2010, p. 276). The ultimate goal in Ontario is to have PbD incorporated into the design and infrastructure of smart grid systems as a means of protecting Personal Identifiable Information (PII). The seven principles of the PbD concept, as well as how it will relate to the smart grid, are described in Table 1.

Table 1: The Seven Foundational Principles of Privacy by Design, and its Application to the Smart Grid (Cavoukian, Privacy by Design. The 7 Foundational Principles, 2009); (Cavoukian, Polonetsky, & Wolf, SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation, 2010)

Principle	Description	Smart Grid Application
Proactive not Reactive	• Privacy risks must be anticipated and prevented before they occur, as opposed to solving problems as they occur.	• Utilities should conduct Smart Grid project Privacy Impact Assessments (PIA) to ensure privacy is incorporated into requirement and plans.
Privacy as the Default	• Personal data must be "automatically" protected. • No action should be required by users to protect their privacy as it is protected by "default".	• Personal Identifiable Information (PII) travelling through a network should be encrypted by default. • PII should be kept in a minimum number of systems. • Provide need-only access to PII. • Third party access to PII must be carefully considered. • PII must be destroyed at the end of the lifecycle.
Privacy Embedding into Design	• Privacy must become a main component of the core functionality being delivered, as opposed to an add-on feature.	• Much of the smart grid infrastructure will build on existing systems; therefore, PbD will have to be integrated into legacy systems as opportunities arise.

Full Functionality	• No false tradeoffs shall be made during design process. • Counters the notion that increases in privacy must be met with decreases in functionality.	• Must embed privacy without any loss of smart grid functionality
End to End Lifecycle Protection	• Privacy measures extend throughout the entire lifecycle of the data. • At the end of the process, data must be securely destroyed. • Ensures cradle to grave, lifecycle management of information, end-to-end.	• Ensures the people, processes, and technology involved in smart grid initiatives consider privacy at every stage. • Ensures that PII is destroyed at the final stage of lifecycle.
Visibility and Transparency	• System that operates under stated promises and objectives. • Subject to independent verification.	• Must show that privacy method being implemented will meet privacy requirements. • Any non-compliant privacy requirements will require a remediation plan to correct the issue. • Must inform consumers as to how their PII will be used.
Respect for User Privacy	• User privacy must be of utmost priority. • Demonstrated by strong privacy defaults, appropriate notice, and user friendly options.	• Must provide necessary information, options, and controls to consumers. • Will allow customers to manage their costs, consumption, carbon footprint, and privacy.

Policy Challenges

Given that Smart grid technologies are in its relatively early stages, there exist several significant policy challenges. Indeed many of the challenges to implementing smart grid privacy measures stem from the fact that the design and scope of the smart grid itself is yet to be clearly defined.

Public Awareness & Misinformation

One of the reasons why Smart grid privacy is a particularly contentious issue is the fact that it deals with information that originates from within the household, a place where that the Supreme Court of Canada has stated an individual should have the greatest expectation of privacy (R. v. Silveira, 1995). As individuals become more exposed to smart grid programs and policies around privacy, it is reasonable to

assume that many will turn to the Internet for answers. The Internet, while an invaluable tool for information exchange and learning, does not discriminate between information that is factual and non-factual. Indeed, a topic such as Smart grid privacy is one that is ripe for conspiracy theories, many of which revolve around the government using the smart grid as a tool to spy on its citizens. These theories are often put forth by those who already have deep mistrust of government.

While many of these theories will be dismissed by many as paranoia, it does highlight the importance and necessity of communication and public outreach by those overseeing and administering Smart grid initiatives. It is essential that authorities, (most notably the provincial government, the OPA and local utilities) provide electricity customers with information that is both fair and accurate. Consumers must be assured that privacy will be embedded into the design of the smart grid (as privacy by design requires) and that their personal information will never be compromised for the sake of increased functionality. In essence, it is not merely good enough for authorities to undertake privacy measures; they must also communicate it to the public as well. A privacy policy that is constructed to include communication will not only ensure that the public is more informed, but will also provide the public with confidence in authorities.

Conflicting Visions of Smart Grid

One of the major challenges in constructing smart grid privacy policy is the fact there does not exist a single agreed upon vision of what the smart grid will entail. Thus, different stakeholders may have different views on what the smart grid will or should accomplish. For example, demand response programs which allow utilities to remotely cycle appliances on and off during peak times are seen as a vital part of the smart grid from the utility's perspective. However, smart appliance manufacturers may have a different view on the ability of utilities to remotely control appliances it manufactures. In its

"Smart Grid White Paper", the US Association of Home Appliance Manufacturers (AHAM) in fact opposes efforts by utilities to remotely control the devices it manufactures.

With respect to utility interaction, the association has taken a very firm stance in favour of strict consumer control. AHAM fears that providing utilities with the ability to control its devices from a remote location could lead to "unexpected risks and consequences" for consumers (Association of Home Appliance Manufacturers, 2009). Ideologically, it believes that the "utility's reach should end at the smart meter", and that communication or interaction activities inside a building should be under the control of the consumer (Association of Home Appliance Manufacturers, 2009). In short, the association advocates for much more limited smart grid capability, where utilities merely inform consumers whether a device is operating under "ideal" or "non-ideal" conditions, leaving the final decision to the consumer as opposed to allowing utilities to take direct actions such as remotely turning on and off appliances.

Indeed this issue is just one of many issues that must be resolved. To illustrate another ideological difference, AHAM has also taken a very pro-consumer privacy stance. It suggests that the "the management of energy consumption and device profiles remain within the realm of the home and be invisible to the utilities" (Association of Home Appliance Manufacturers, 2009). By keeping information "invisible" to utilities, it believes that third party activities such as data mining and behavioral pattering will be prevented (although they do not mention whether research access de-identified data would be acceptable).

Both of these stances from AHAM are not necessarily widely accepted or agreed upon characteristics of the smart grid. Utilities may argue that effective management of the smart grid will require utilities to certain limited controls over appliances (such as demand-response programs), and researchers may argue that invaluable information may be gained from allowing information to be "visible" to utilities. It

is clear that manufacturing groups have a much different ideological stance than local utilities, and these differences must be resolved.

Third-Party Access to Information

Another major challenge in constructing policies around smart grid privacy will be to determine what potential relationship, if any, will exist between local utilities and third parties interested in obtaining smart grid data. The extent of smart grid data that a third party could potentially obtain not only must be addressed but must be clearly communicated to electricity customers. Third parties can consist of a wide variety of groups including corporations such as appliance manufacturers and non-profit groups such as academics and researchers. Quinn believes that utilities will be very motivated to sell smart meter data to third parties as he states, "e-commerce has proven that collection and sale of personal information can be a lucrative endeavor. This confluence of forces may well push utilities toward more invasive behavior than they have engaged in before now. In short, electric utilities are (or soon will be) collecting more information than they have in the past, and there is more reason to sell it to other parties" (Quinn, 2008). Cavoukian et al points out that the collection of smart grid data from consumers brings about many "temptations" that must be avoided. One of these temptations includes taking identifiable information and bundling it into different data packages such as data usage or appliance data. Another temptation may include utilities and third parties using the information to seek consent for other services (Cavoukian, Polonetsky, & Wolf, 2010). It is therefore essential that policies are put in place to address third party access to smart grid data. Such policies should address who would have access to smart grid data, for what purpose, and what the role of the utility, and most importantly the electricity consumer, in releasing this information. In addition, policy around whether to treat de-identified data differently from identified data from a privacy standpoint must be examined.

Policy Recommendations

Local utilities and M.E. must openly and honestly convey privacy concerns to the public

It is often stated that Smart Grids require smart people, an expression that highlights the importance of educating consumers on Smart grid technologies. While there is much focus of educating the public on the capabilities of the Smart grid, it appears that outside of the IPC there is virtually no mention of issues related to privacy from the various parties participating in Smart grid implementation. Even though part of the IPC's mandate is to engage in public outreach and educate Ontarians on issues of privacy, the issue of smart grid policy should not be left solely in the domain of the IPC. One could make the argument that a local utility that was truly implementing PbD principles would be obligated to communicate privacy issues to its customers, consistent with the "Respect for User Privacy" principle.

In addition to actual privacy measures put in place, a positive public perception of the Smart grid program will be essential to its future success. Even if authorities (such as the OPA, IESO, local utilities and the M.E.) feel that privacy considerations have been adequately integrated in to the design of the smart grid, it is still vital to communicate this to the public. By engaging in public outreach at an early stage of development, public confusion, fear, misconception, and resentment can be avoided. It can also provide an important counter-balance to misinformation that may be circulating in the public domain. In addition, an honest and open engagement of the public will encourage and give confidence to consumers to participate in future enablement programs such as demand response-programs, conservation programs, voluntary curtailment, advanced device management, and in-home displays (Cavoukian, Polonetsky, & Wolf, 2010).

Given the Ministry of Energy's role in developing Smart grid policy, it is particularly obligated to educate the public on such matters. While much of the M.E. focuses on the opportunities that the Smart grid

presents, it is recommended that the Ministry take a much more active approach towards educating the social implications of the smart grid initiative, including issues related to privacy. This should be viewed as an opportunity to communicate any privacy measures already in place, and reassure the public that privacy is a core consideration. Hoping the public will simply trust that adequate privacy measures have been put in place will most likely not be adequate and may lead to distrust of smart grid technologies. By not directly addressing the issue, the government opens itself up to criticism and allows advocacy groups to spread information that may be misleading or overly exaggerated.

Clear boundaries on researcher's access to information must be established

While protecting consumer privacy should always be of utmost concern, data obtained from smart grid technologies could potentially have great benefit to society provided it is not used for malicious intent. Since smart grid technologies are still in their very early stages, it is reasonable to assume that the potential usefulness of this data for academia and research is not fully understood (Beyea, 2010). Imposing privacy standards that does not consider the academic community may prove to be short sighted and a lost opportunity to benefit society. Since it is not entirely clear what types of data will be transmitted through smart grid infrastructure over the next two decades, legislators and regulators may be tempted to impose overly restrictive privacy policies out of an abundance of caution.

Determining the type and extent of information academia will have access to will be essential component of smart grid privacy policy. Whether PII should be available to researchers will undoubtedly be controversial, but as Beyea argues, "many researchers have great experience dealing with the privacy of study subjects through service on, and interactions with, Institutional Review Boards" (Beyea, 2010, p. 979). However, Beyea does concede that there will be some data that will be considered off limits (Beyea, 2010).

Cavoukian et al believes that consumers must always maintain control of their PII, and that any access to PII by third parties should be authorized directly by consumers only, and should not be determined by utilities (Cavoukian, Polonetsky, & Wolf, 2010). This procedure would be beneficial as it would help avoid third parties from using PII for dishonest reasons or personal gain (such as targeted marketing). However, whether this policy should be extended to de-identified data must be examined. Beyea suggests that data that has been removed of personal identifiers (de-identified data) may be considered a useful option that could help researchers study trends over geographic areas (Beyea, 2010).

Ultimately, privacy issues can be rather subjective in nature. What constitutes an invasion of privacy will vary by person, depending on their values and beliefs. Given the social impact of a policy decision such as determining research access to smart grid information, it is essential that views of the public, legislators, regulatory bodies, and academic institutions be considered. Such policies should address who would have access to smart grid data, for what purpose, and what role the utility and the customer have in releasing this information.

Conclusion

Ultimately, the benefits of implementing smart grid technologies greatly outnumber the concerns it raises. However, privacy concerns around these technologies do in fact exist, and therefore must be carefully examined. Perhaps the most significant aspect of smart grid technologies is the utility's ability to automatically collect information from its customers on a much more frequent basis with likely an increasing level of detail. This development has far greater implications beyond the technical challenges in storing and managing ever increasing volumes of data. It is a fundamental change of the relationship between the utility and the consumer. Traditionally, the relationship between a utility and its customer was very linear and one-directional, with the utility providing electricity and the customer consuming it

in a rather “passive” manner. However, the smart grid will empower electricity customers by allowing them to have a more active role in their energy usage and, in some cases, even provide electricity back to the utility through the use of installed renewable energy generation units. These developments are mutually beneficial for consumers and utilities, as well as the province at large as it helps reach its environmental and economic goals.

The result of this change in relationship between the utility and the customer implies that the customer will be much more familiar with the role of their utility in their community. It is therefore essential for utilities, now more than ever, to gain and build the trust and confidence of its customers. Part of gaining the trust of customers is communicating the complete and full implications of the smart grid, including issues related to privacy. This will, in the long term, help utilities implement other initiatives such as demand-response programs with the support and enthusiasm of its customers.

By using Privacy by Design principles, Ontario’s utilities are effectively taking a pro-active approach to smart grid privacy issues. While all parties involved in implementation will face and likely solve the many technical issues that arise from smart grid technologies, it is important to recognize the social implications of such technologies. Ultimately, public education on privacy issues will not only help consumers further understand privacy issues, but help with adoption and acceptance of the smart grid itself.

Appendix 1 – Smart Meter Systems

Electricity data that is collected from households and businesses travels through what is known as the Smart Meter System.

Smart Meter Systems

Smart Meter Systems consists of two main components: The Advanced Metering Infrastructure (AMI) and the Meter Data Management and Repository (MDM/R). The AMI is the smart metering infrastructure that is maintained by the local utility while the MDM/R receives data from the AMI for processing and storage, and is the responsibility of the "Smart Metering Entity" (the IESO in the interim).

Advanced Metering Infrastructure (AMI)

Implementation of the AMI can vary widely as it is the responsibility of the local utilities (there are currently 80 local utilities in Ontario). The purpose of the AMI is to collect meter reads from customers (through a communication device located on the customer's premises), and send it through communication networks to a control computer that temporarily stores this information. The control computer eventually sends this data to the MDM/R, where it is maintained by the IESO on a long term basis. The functional specifications for the AMI states that at a minimum, the following functionality must be provided:

- Meter reads must be collected on an hourly basis the Communication Device and transmitted to the Control Computer, and subsequently sent the MDM/R.
- All meter reads shall be collected, dated and time stamped at the end of each hour recorded as year, month, day, hour, minute (YYYY-MM-DD hh:mm)

Basic security measures include mandating that all meter reads collected in a given day must promptly sent to the MDM/R by early the next morning (presumably to ensure that data does not stay in the remotely located Control Computer too long where it may be at risk to tampering and/or theft). The AMI will also provide several reports to the MDM/R, including those related to identifying instances of tampering, interference and theft.

Meter Data Management and Repository (MDM/R)

In 2007, regulation designated the IESO as the Smart Metering Entity, and as part of its mandate, it is responsible for maintaining the province wide data repository (MDM/R) that collects and manages smart meter consumption data (IESO, 2010) (Ontario Regulation 393/07, 2007). The purpose of the MDM/R is to provide a centralized infrastructure that will receive meter reads from all AMI in the province. It serves several purposes including the processing of meter reads to produce billing quantity data, storing and managing data, and providing access to data to all "interested parties". Some of basic privacy measures the IESO implements on the MDM/R include ensuring that:

- Customers may only view data relating to their own consumption;
- Local Distribution Companies (LDCs) may only see data relating to their own customers
- Billing Agents may only have access to view billing quantities

The MDM/R will be capable of archiving and restoring data "to provide long-term storage, preservation, disposition, and distribution of meter reads, algorithms and associated data" (IESO, 2006). This data will be kept for a minimum of 26 months to "Interested Parties", who must be registered with the IESO (IESO, 2006). The challenge of protecting privacy lies in providing secure communication channels to ensure that personal information is never compromised. This includes information in storage systems such as the Control Computer and the MDM/R, as well as information that travel through WAN communication channels.

Bibliography

Association of Home Appliance Manufacturers. (2009, December). Smart Grid White Paper: The Home Appliance Industry's Principles & Requirements for Achieving a Widely Accepted Smart Grid. Washington, DC.

Beyea, J. (2010). The Smart Electricity Grid and Scientific Research. *Science , 328*, 979-980.

Cavoukian, A. (2009, August). Privacy by Design. The 7 Foundational Principles. Information and Privacy Commisioner of Ontario.

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). *SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation.* springerlink.com.

Electric Power Research Institute. (2010). *EPRI | SmartGrid Research Center*. Retrieved August 12, 2010, from Electric Power Research Institute: http://www.smartgrid.epri.com/

Gallant, P. (2010, February 19). *Smart grid could turn appliances into spies, experts warn*. Retrieved August 26, 2010, from CBC News - Technology & Science: http://www.cbc.ca/technology/story/2010/02/09/smart-grid-electricity.html

Herold, R. (2009, September). SmartGrid Privacy Concerns.

Hydro Mississauga. (2008). *Hydro Mississauga | Smart Metering*. Retrieved August 3, 2010, from Hydro Mississauga: http://www.enersource.com/smartmeter.aspx?ekmensel=c580fa7b_90_134_btnlink#q6

IESO. (2010). *How Your Smart Meter Works*. Retrieved August 9, 2010, from ieso: http://www.ieso.ca/imoweb/siteshared/smart_meter_information.asp?sid=ic

IESO. (2006, November 29). Meter Data Management and Repository (MDM/R). Functional Specification. Issue 2.0. Ontario.

Information & Privacy Commisioner of Ontario. (2010). *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid.* Toronto.

Information and Privacy Commissioner. (2010). *IPC - Office of the Information and Privacy Commissioner/Ontario | About us*. Retrieved July 23, 2010, from Role and Mandate of the IPC Office: http://www.ipc.on.ca/english/About-Us/Role-and-Mandate-of-the-IPC-Office/

Johnston, C. (2010, February 23). *Cell phones show human movement predictable 93% of the time*. Retrieved August 6, 2010, from ars technica: http://arstechnica.com/science/news/2010/02/cell-phones-show-human-movement-predictable-93-of-the-time.ars

McDaniel, P., & McLaughlin, S. (2009, May/June). Security and Privacy. Challenges in the Smart Grid. *IEEE Security and Privacy* . IEEE.

Ministry of Energy and Infrastructure. (2007, July 5). Functional Specification for an Advanced Metering Infrastructure. Version 2. Ontario.

Ontario Smart Grid Forum. (2008). *Enabling Tommorow's Electricity System. Report of the Ontario Smart Grid Forum.* Toronto.

Power Stream. (2010). *Power Stream : Smart Meter General Information*. Retrieved August 23, 2010, from http://www.powerstream.ca/app/pages/SmartMeters.jsp

Quinn, E. L. (2008). *Privacy and the New Energy Infrastructure.* University of Colorado Law School, Center for Energy and Environmental Security. University of Colorado Law School.

R. v. Silveira, [1995] 2 S.C.R. 297 (Supreme Court of Canada May 18, 1995).

Smart Metering Entity, O. Reg. 393/07 (2007).

Timmer, J. (2010). *Smart grid privacy rules may be blown opportunity for science*. Retrieved August 6, 2010, from ars technica: http://arstechnica.com/science/news/2010/05/smart-grid-privacy-rules-may-be-blown-opportunity-for-science.ars

U.S. Department of Energy. (2008). *The Smart Grid: An Introduction.* Prepared by Litos Strategic Communication.

Utility Consumers Action Network. (2010, March 5). The Privacy Problems Inherent in the Smart Grid.

World Economic Forum. (2009). *Accelerating Smart Grid Investments.* Geneva.