TED ROGERS SCHOOL OF MANAGEMENT RYERSON UNIVERSITY

PRIVACY AND CYBER CRIME INSTITUTE

Applying PIPEDA to the Smart Grid

Avner Levin

Research Associate: Colin Rogers

Ryerson University
Ted Rogers School of Management
Privacy and Cyber Crime Institute
March 2011

PRIVACY AND CYBER CRIME INSTITUTE

Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada's Contributions Program and through in-kind contributions from the Ted Rogers School of Management at Ryerson University. We are grateful to the Privacy Commissioner and to the School for their support of this research project. We also wish to thank the project participants who were willing to give up their valuable time in order to advance our meagre understanding of the developing electricity grid, let alone its privacy issues. This project would not have been completed in such a timely fashion were it not for the Privacy Institute's excellent research associate, Colin Rogers who worked tirelessly on this project in addition to all his other many responsibilities.

PRIVACY AND CYBER CRIME INSTITUTE

Table of Contents

Executive Summary 5

Introduction 6

Goals and Objectives 9

Methodology 9

The Findings 10

- The Legal Grid 11
- Personal Information on the Grid 11
- What is New & Needed 13
- Privacy Policies 14
- The Risks 15
- Third Parties 17
- Consent 19
- PIPEDA as Consumer Tool 20
- Smart Appliances 22

Discussion 25

- The Legal Grid 25

Smart Meters 30
Billing Information 31
Operational Information 33
Smart Appliances 35
The Practice of Personal Information Protection 37
Privacy Policies 37
Disclosure 37
Consent 38
Where is the Focus? 40
Do We have to Save Energy at the Expense of Privacy? 41
Recommendations for OPC 45

Executive Summary

Applying PIPEDA to the Smart Grid is a research project into the collection, use and disclosure of personal information obtained by utilities through Smart Grids. The project used interviews with key executives to determine whether such handling of personal information is in compliance with PIPEDA and the extent to which utilities are protecting and securing personal information.

Key findings:

- The Smart Grid's regulatory framework focuses on energy at the expense of privacy.
- The work of Ontario's IPC has promoted the technological incorporation of privacy into the Smart Grid but has caused inadvertent regulatory confusion.
- Utilities, bound by regulation, have little ability to become PIPEDA-compliant corporations.
- OPC is not active enough in ensuring compliance with PIPEDA's core notions.

Recommendations are included that will enable the OPC to develop guidelines for utilities about the Smart Grid and personal information protection, and inform Canadians of the privacy implications of the Smart Grid, enabling them as consumers to choose whether they wish to consent in a meaningful manner to such practices.

The key recommendations are:

- OPC should clearly communicate to utilities and the public that personal information generated by the Smart Grid is subject to PIPEDA.
- OPC should reach agreements with its provincial counterparts that will clarify respective jurisdiction on Smart Grid issues.
- OPC should serve as a resource on Smart Grid privacy issues for utilities and customers.
- OPC should engage Ontario and other provinces to ensure Smart Grid initiatives are in compliance with PIPEDA so that individuals are offered choice and control over the collection of their personal information.

Introduction

Twenty Seven years ago the Supreme Court of Canada heard an appeal whether law enforcement agencies should be allowed to access electricity consumption records without a warrant. Justice McLachlin (our current Chief Justice) stated then:

> The records are capable of telling much about one's personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there. The records tell a story about what is happening inside a private dwelling, the most private of places. I think that a reasonable person looking at these facts would conclude that the records should be used only for the purpose for which they were made -- the delivery and billing of electricity -- and not divulged to strangers without proper legal authorization.[1]

Canadians are now becoming aware of the latest form of collection of their personal information – the Smart Grid. The Smart Grid is the energy grid's next generation. It is defined in Ontario as a grid that will:

> … 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…[2]

It is a grid that will enable us to generate power locally, by environmentally-friendly means such as wind turbines and solar cells, and upload the power we generate into the grid for the benefit of others. The Smart Grid will be able to transmit locally-generated power, and distribute it to others, in a safe, secure and reliable manner, and at the same standards as the current grid does for centrally generated electricity in natural-gas, coal and nuclear power plants.[3]
Electricity users will be able in such a manner to reduce their consumption of electricity, and reduce the electricity bill even further, by selling their utility the excess power they generate and do not

[1] *R. v. Plant*, [1993] 3 S.C.R. 281
[2] *Ontario Electricity Act*, § 2 (1.3), 1998.
[3] Ontario's Smart Grid Forum, Enabling Tomorrow's Electricity System (2009) http://www.ieso.ca/imoweb/pubs/smart_grid/Smart_Grid_Forum-Report.pdf

require for their household consumption.[4] That, in itself, requires large scale re-engineering of the existing grid and the deployment of new components that will be able to handle two-way power transmission and distribution, as well as meters to measure local generation and net consumption.[5] The Smart Grid will use new meters not only to measure local generation, but to introduce time-of-use (TOU) pricing as well, through measurements taken at different hours. These new meters are referred to as Smart Meters, and TOU pricing is, independently of other Smart Grid components, an incentive for individuals to reduce and shift consumptions to periods that allow the utility overall to control demand and conserve energy.[6]

Energy consumption is managed by the Smart Grid not only by enabling local generation and by TOU pricing, but by the introduction of Smart Appliances into the home as well. Smart Appliances (the next generation of washers, dryers, refrigerators and dishwashers) can be operated remotely by consumers and by the utility, with the resulting ability of shifting the power use of these appliances to off-peak times as well. As a result of its features the Smart Grid allows the utility to collect information on the energy use and habits of its customers that may identify them and therefore meet the definition of personal information under PIPEDA. Smart Meters for example enable a detailed analysis of time-of-use that allows a person equipped with basic information on typical household consumptions to determine with a fair degree of accuracy whether a residence is occupied or vacant at a certain time of day. Smart Appliances offer utilities the opportunity to control areas of life that Canadians and their Courts have considered to be private and intimate, by affecting the availability of such appliances through the day.[7]

Of even greater concern is not only the collection and use of personal information by utilities, but its disclosure to third parties as well. Questions have been raised, for example, in light of decisions such as the one quoted above, whether utilities will disclose unusual consumption patterns and appliances

[4] *Id*

[5] *Id*

[6] TOU pricing typically includes three price levels, high, medium and low, reflecting three levels of energy demand during the day. High-peak electricity demand periods are typically day-time during the business week, and low-peak periods of time are typically the weekends, and night-time. These can change according to the season. See e.g., http://www.torontohydro.com/sites/electricsystem/residential/smartmeters/Pages/TOURates.aspx

[7] The Supreme Court of Canada, while allowing the use of thermal devices for surveillance, stated that the home is "the place where our most intimate and private activities are most likely to take place." See *R v. Tessling* [2004] 3 S.C.R. 432.

usage to law enforcement agencies.[8] Online content providers and information location services, such as Google, have already developed interfaces and applications, such as Google's PowerMeter, that they would like both utilities and customers to use. Utilities are attracted to such solutions since development of such tools is not their core activity, but such partnerships necessitate the disclosure of personal information to third parties.

While these may be legitimate concerns there is in fact a paucity of information on the steps that Canadian utilities have taken to secure and protect the personal information that they will collect and in some cases are already collecting through the Smart Grid. The Smart Grid to-date has been heralded as green, environmentally friendly, and generally a good thing. If any, concerns have focused on the security and stability of the Smart Grid given the ability local users will have to upload power and potentially destabilize the grid, and the fears that malicious hackers will have more entry-points into the grid's communications network and the grid itself, with the introduction of 'smart' components such as meters and appliances.[9] The information presented in this report about the actual practices of utilities and the policies they have developed to guide them as they deploy the Smart Grid will allow Canadians to determine the extent to which such concerns are legitimate, and if so, whether utilities have appropriately addressed them.

Furthermore, PIPEDA is based on the idea that individuals must be given choice and control over the manner in which their personal information is collected, used and disclosed, through the legal notion of consent. As this report discusses, the issue of consent is particularly problematic in jurisdictions such as Ontario where the Smart Grid has been mandated by government and is not open to consumer choice. The consent question represents the greater regulatory tension at play – between the personal information protection regime subject to the PIPEDA, and the electricity and energy market subject to its own regulatory forces. The Smart Grid harbours great opportunity for enhanced environmental protection and is generally welcomed by environmental advocates. This report will assist Canadians concerned both about their privacy *and* their environment in determining whether they can endorse the Smart Grid and perhaps avoid unnecessary conflict with the environmental movement with which they shares many concerns.

[8] Extraordinarily high consumption is already considered an indicator of illegal activity, such as drug growth and manufacturing, regardless of time of use.

[9] *Enabling Tomorrow's Electricity System*, p.36 *supra* note 3.

Goals and Objectives

The goal of this project was to develop an understanding of the privacy implications of the Smart Grid, as an emerging issue to which there is little awareness of its privacy and information security implications and/or threats. Specifically, this project targeted the following objectives:

- Details of the personal information that is collected through the Smart Grid.
- Understanding the legal framework of privacy on the Smart Grid and whether Smart Grid initiatives are in compliance with PIPEDA.
- Understanding how utilities are incorporating privacy and security into the Smart Grid.
- Providing knowledge that will allow Canadians to decide whether they wish to consent to Smart Grid features offered by their local utility.

Methodology

This project was based on in-depth qualitative interviews with key informants working for Ontario utilities. Six interviews were conducted with utility executives and privacy regulators. The interviews were taped and transcribed. Trends, themes, issues and concerns were sorted, classified and organized, and are reported in the "Findings" section of this report. The following questions formed the basis of the semi-structured interviews that were held:

1) What is the legal and regulatory framework covering Smart Grid data?
2) Does the Smart Grid create personal information, or allow others to collect personal information in ways that were not possible before?
3) What data collection is necessary in order for customers to receive the full benefits of the Smart Grid?
4) Will your privacy policy will have to change (or has it already changed) and if so, in what way?
5) Does the Smart Grid create new security or privacy risks for you or your customers?
6) Will data be transferred to other organizations and if so will it require specific protection?
7) Will customers be able to opt in or opt out of data collection and/or transfer?
8) Are you concerned that customers will attempt to use data protection legislation to challenge various aspects of their Smart Grid data (e.g. accuracy)?
9) Finally, what are manufacturers doing, or should they be doing, in order to make their appliances ready for the Smart Grid?

The Findings

The interviews that have been conducted created the following understanding of the Smart Grid, the different forms in which it processes personal information, and the parties to which utilities are disclosing or intend to disclose such information.

Participants came from Ontario-based utilities. The decision to focus on Ontario was made early on into this project, based on two reasons. First, to minimize costs and ensure completion of this report in a timely manner; more significantly, because Ontario has seen some privacy-related activity around the Smart Grid due to the activities of Ontario's Information and Privacy Commissioner, activities that helped formulate some of the questions of this research.[10] Utilities mainly in the electricity distribution business were contacted and asked to identify the appropriate executive that could represent them on Smart Grid privacy issues.[11] Participating utilities had over 2 million customers between them, and some provided transmission as well as power generation services, in addition to the distribution of electricity. The following table presents some minimal information about the utilities and the executives, for ease of references to quotes in the report, while respecting the confidentiality of participating utilities and individuals.

Utility	Executive
U1	Manager, Metering
U2	Director, Customer Services
U3	Director, Business Development
U4	President
U5	Vice President, Electrical Systems
U6	Senior VP, Metering

[10] The latest of which is titled "Operationalizing Privacy by Design: The Ontario Smart Grid Case Study" http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf

[11] Utilities have traditionally been divided into electricity generators, transmitters and distributors. The generation of electricity in Ontario is mainly performed by Ontario Power Generation (OPG), a crown corporation. Almost all utilities have some transmitting capacity (the transmission of high-voltage electricity), and traditionally, utilities serving businesses and residences have been considered distributors. The advent of the Smart Grid will blur these lines, since it will open up the possibility of local power generation from alternative energy sources, and require utilities to operate a bi-directional grid.

The findings are presented by question, according to the questionnaire provided above. A more detailed discussion of the issues identified by the participants is provided in the following section.

The Legal Grid

Participants did not distinguish between their electricity regulatory framework and their personal information protection framework. Participants named the Ontario Energy Board (U3), the Electricity Act (U5) and the US National Institute of Standards and Technology (NIST) (U4) as regulators that had a say not only in electricity regulation (as could be expected) but also in data protection. When it came to data protection regulators specifically, some participants were not aware of PIPEDA, others were aware more of Ontario's IPC, and some understood that PIPEDA was the legislation that applied to their commercial data transactions:

> It's our understanding that utilities are compliant, must be compliant only with PIPEDA. (U1)

> [W]e're actually saying NIST and we've got the Ontario Privacy Commissioner. These are the things to focus on. (U4)

> We see ourselves as subject to both [provincial and federal privacy legislation]. Along to, obviously, the Electricity Act... we would see ourselves as going the same length as every other distributor to protect customer privacy. (U6)

> I know very little, except I think we're under PIPA [sic] (U5)

The attention paid by utilities to Ontario's IPC is understandable, given her work on the Smart Grid and privacy. Still, it creates an interesting situation where the regulator attempting to set (commendable) standards and norms is not in fact the regulator named in the legislation. For suggestions and recommendations how to resolve this situation see the discussion section below.

Personal Information on the Grid

Somewhat surprisingly, participants were not convinced that the information transmitted by Smart Meters is personal information. Several reasons were provided by participants for this point of view. First, since the meter information has traditionally been accessible participants did not view it as deserving protection simply because the introduction of new metering technology:

> Right now, the way I look at meter readings, always looked at them, is that meter readings are in the public domain. Because anyone can walk up to a house and read a meter. (U4)

Second, billing information, electricity consumption, was simply not viewed as personal or including any identifying features.

> I guess, at this point, I do not view it as personal information. We have consumers' hourly data, it doesn't have any personal identifiers in it, so no I don't view it as personal information at this point in time. (U2)

> You exist as a meter number and a uniquely assigned number that identifies you. But your name, your address, that information doesn't exist anywhere in the [metering infrastructure]. (U6)

A version of this line of thought viewed billing information as personal only when linked in a database with customer information.

> We think that there's the potential for information that would be called 'private'. The issue being that we're creating all these meter readings, but the meter readings on their own aren't private. It's not until you can link them to the customer. So we'd be doing things like making sure that when you're sending those readings back to our system from the meter out in the field, there's nothing in that reading that says what the customer's name is or what the address is. (U3)

> So we read the smart meters through an advanced metering interrogation system, so the data that's sent to us is the unique PIN number to the meter that is read in the software of our metering system, so it isn't captured anywhere that we can identify, so it's just simply that PIN number and the 24 hour interval reads plus the register read. There isn't any identifier. (U2)

> There's an encrypted table that matches it up in billing and that's the only place. And the assignment of numbers, among other things, is all random. Meaning your home, say house number one on your street, the next house is not the next [number]. (U6)

Finally, one participant voiced an opinion that since the information transmitted by the Smart Meter applies to a residence or location, it cannot be considered personal or individual information.

> [S]omeone looking into data wouldn't know specifically how many individual persons might be contributing to the use at that location, but the fact that that location has a usage pattern does indicate something that is personal to that location (U1)

However, participants were aware of the potential of information that they did not consider personal to turn into personal information with the introduction of Smart Meters and more sophisticated analysis, as presented in the following section.

What is New & Needed

One new feature of the Smart Grid identified by participants as having potential privacy implications, is the ability to analyze billing information, which will be available on an hourly basis, to uncover or extrapolate personal information and patterns of behaviour.

> [W]e can determine that energy is being used on an hour-by-hour basis. So someone… could actually see that this person is a night owl or this person has a typical daily profile where they use no energy, or very little energy at night and they use more energy when they wake up in the morning and they seem to go away and there's not much energy during the day and that energy comes back on around 4 in the afternoon and goes off at 10:30. So someone who had access could determine a usage pattern that might infer a personal usage pattern. (U1)

> We can look at a customer's account… and see when [their] family wakes up in the morning. We can tell by looking at their profile. You can see when [they] cook lunch on the weekend, but we're not looking at the data at that type of level. We're purely bundling it off and billing on it. (U2)

Interestingly, participants did not view the operational data (distinct from the billing information) generated by Smart Meters as relevant to the debate over personal information. While there was recognition and appreciation of the role that Smart Meter data would play in that regard, the data were not considered to have any privacy implications.

> [T]here may be information that may help us to better manage our system… the customer may not even understand the data, like it may be very technical information that just helps us… The purpose would be to maintain the safety and integrity of our system; it wouldn't be customer data, per se. (U2)

> A copy goes to our operational data store, because we're pulling that billing data, we're pulling outage reporting, we're pulling minimum / maximum average voltage, we're pulling current information, tampering, theft, a whole host of stuff... [T]he value is in this operational data stream which we never had before... [W]e set things up like outage flagging, theft, tampering, to be instant alarm... we have a dedicated operational channel for critical messaging, so it'll push those messages out immediately. It's not pull, but push in that regard. We have the ability with our system... to reconfigure our data gathering any way we wish. (U6)

Privacy Policies

Most participants, perhaps due to their internal roles, were not familiar with their organization's privacy policy or did not see a need for policy change due to the introduction of the Smart Grid.

> At this point, we haven't seen a need to revise our privacy policy… this is an evolving area, certainly, but at this point we don't see a need to change our policy. (U2)

> I guess I don't understand enough about the legal entity or the legislation to say we should be reacting in a certain way or we shouldn't. (U5)

Some participants did anticipate a future change, once they became more knowledgeable about the privacy implications of the Smart Grid.

> Would it have to change? I don't know. [W]e have deployed... a security audit… that process is really just starting and will probably identify some shortcomings… I suspect it may suggest some changes in policy around privacy. (U4)

> I think that we're going to need to review our privacy policy… there will be some things that will come out in that that may lead us to adjust our privacy policy and that's some thing that we might want to even do differently internally… I think that our privacy policy would have to change. I suspect that it would be… In the future we will need to change the privacy policy to further restrict access internally within the company to that data. (U1)

All in all, the level of awareness to, and consideration of, privacy policies, is similar to the levels found in other industries pre-data-breach. Significant policy change and attitude change typically occurs once an organization has suffered a data breach.[12]

The Risks

Participants were asked about both security and privacy risks and it is clear that security risks were very much top of their mind. Participants worry not only about the security of information as it is transmitted through the grid, but of the physical security of the grid itself, and about attacks on the grid that could destabilize any or all of its components (generation, transmission, distribution) by destabilizing the information technology that will support it. Indeed, much of the regulatory attention in Canada and the US has focused on the cyber-security risks of the Smart Grid and on the provision of cyber-security measures that will protect the grid from malicious attacks.[13]

One participant mentioned the physical instability that the grid could suffer as a result of its new features:

> Let's just speak specifically about the embedded generation within the utility. If it's uncontrolled, there would be some additional risks to security of the grid, and security of the electricity supply. From a distribution system code perspective, there are significant things that a utility must do before it's allowed to connect a generation system to the grid, and there are fairly significant technical requirements that the generator needs to meet for the person who is putting a system on their roof as an example, for solar power. Before we would do that, we have to understand a number of technical things about the generator they're proposing to put on and they actually put on and how it's connected. (U1)

Most participants, however, focused on cyber-security issues:

---

[12] See e.g. our study of employer policies regarding online social networks. Levin, A. et al, *The Next Digital Divide: Online Social Network Privacy* http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf

[13] See e.g. the US NIST (a non-regulatory body) *Guidelines for Smart Grid Cyber Security* http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf and the work of the US federal regulator, the Federal Energy Regulatory Commission (FERC) *Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed* http://www.ferc.gov/industries/electric/indus-act/smart-grid.asp

> [S]omebody getting physically getting access to a collector, compromising it, getting a laptop in and trying to get access. Other people have said that it is possible for someone to shoot a wireless antenna and tap into the network and start manipulating the meter information. Compromising the network and start putting false data into the meters, so that's risk and that's occurring as it moves forward… all of a sudden there's [hundreds of thousands of] vulnerability points. Everybody's using connections into the meters… [P]eople are getting a bit excited in wanting to provide all this information, two-way communication with customers and not really understanding, because I'm sure hackers will start to target utilities in a big way... (U2)

> Hacking into the grid… how do we protect data at a level that equates to the actual risk exposure you're looking at? [A]s you look at moving up the grid to a transformer or a transmission or distribution station, obviously the levels of risk and therefore security requirements and all of that escalate, and then when you get into the bulk electric system, you know, now you're Department of Defence type security. (U3)

> Different manufacturers handle communications very differently… every meter has to communicate with the tower… each meter contains an encryption device, and the encryption is a one-to-one encryption. So if you tore the meter off your wall, you smashed it open, pried out the encryption chip and were to de-engineer it so you understood what it was doing, you could only talk to the [tower] from that meter, that's it. You couldn't then break in to all the rest of the meters. [The manufacturers] handle that piece. From the tower on, we have a responsibility to make sure that our data collection network has some physical security, because clearly if it were a set of phone lines and someone were able to walk into one of our substations where these exist and just put a recorder on the lines and then walk out, they could gather as much data as possible, right? (U5)

Participants did mention privacy-related risks as well, but not all saw the Smart Grid as increasing risks in that respect.

> I think that there's a danger that that could happen if the data were to somehow get away from the utility and / or the IESO and become part of either a pirated database or somehow in the public domain, because clearly if you decide that you're going on a trip next week and you head up to the cottage, the electricity usage in your home, when you leave, is significantly different than it was this week when you lived there, and it becomes pretty self-evident when you look at the usage pattern on an hour-by-hour basis. (U5)

> [A]ctually I think it's improved certain risks. Instead of [us] sending someone physically to your home once a month, we're not sending anyone to your home, so we've reduced the number of people that are physically coming to your home and perhaps invading the privacy of your space. (U1)

Finally, participants were strongly committed to minimizing and eliminating as much as possible the security risks (that were for them the most pressing concern). External audits were a common risk management tool, as was working with Ontario's IPC on Privacy by Design.

> [We are] in the process of engaging a firm with expertise in security of these types of systems to perform an audit of the complete system. The results of that audit will be used to develop any kind of potential remedial plan, but the type of system that we're using does use encryption, does use physical access barriers to meters, to the radio towers and to the central computer. The communication protocols between the radio towers and the central communication computer are encrypted data. It is through secure channels. There is user and password access control to any of the software systems that are used to view, review or change data on that system. (U1)

> So we're going to be doing some things. We've engaged some firms to look at physical security, we've engaged them to look at cyber security, because we are bringing it back over various and sundry communication lines, and we're looking for their help to make it as secure as possible. Plus we're working with a group of other utilities to engage cyber security firms to do white hacking for us. Find our weaknesses before somebody else does. (U5)

> Yeah, so again we basically go through a process of identifying the risks, identifying the acceptable mitigation of that risk, which formulates requirements for the solution sets that we're putting in, whether it's communications, IT, or business process and we develop those systems based on those requirements and then you go through your typical design-build-test, you test against those requirements to validate and then you start looking at commissioning. And this is kind of where some of the work the [Ontario] Privacy Commissioner [is doing], talks about Privacy by Design… (U3)

Third Parties

Participants had some experience dealing with third parties and access to customer information, due to the deregulation of Ontario's energy market, and the operation of independent energy retailers that enter into supply contracts with individual customers and are permitted access to customer personal

and billing information for that purpose. For most participants, the introduction of third parties to handle customer billing and consumption information would follow the model of independent energy retailers, in being consumer-driver and reflecting customer choice and control, as well as falling under current OEB regulation.

> [W]e already have framework developed through the Ontario Energy Board to send customers' data to retailers, for example, but that is already working, we're already sending account information, consumption information, customer information to retailers based on three and five year termed contracts, so that framework already exists. (R2)

> One thing, to go back to the protection of information, utilities are regulated but they can have unregulated affiliates. Any data that we have from customers for billing, etcetera, we can't even give it to an affiliate. There's an affiliate relationship code at the OEB that, so even to give it to an affiliate we need customer permission. (R3)

> So you know, once Google is set up as a valid organization to use this data transmission protocol, then assuming they have the correct protocols for an individual customer's data, that was supplied to them by that individual customer, then they would have access to the data. (R1)

> There are two lines of thinking in Ontario, as I understand it. One is… that the utility would manage that security. In other words, we would issue and revoke passwords. So a customer has access, we would give that customer a password, then all of a sudden Microsoft comes and says 'we want the data from that customer' and they've signed off, I would then have to manage security for Microsoft. That's one way to go. My way still is I give you access to your data. You can choose to then share that with Microsoft, Google, or whoever, but you are doing the sharing, not me. All I will do is ensure that your access is secure, so then let your conscience be your guide with who you share that with. (R4)

A second form of third party involvement contemplated by participants was at the utility level, in partnerships that utilities formed or would form with third parties with expertise in data processing and consumer interfaces, to facilitate the transmission of usage information back to the customer, as required by the Smart Grid regulatory framework and to encourage optimal time-of-use. Participants viewed such cooperation as following the contractual model used with any external supplier, similar to their transactions with equipment providers, billing software providers etc.

> We are investigating something that would be more of an in-house solution; an add-on to perhaps our existing billing system. It would be a portal that is completely controlled by [us]. We're also investigating solutions that would use significant third-party technologies, and there's trade-offs in both, in terms of sort of... and the biggest one that we see right now is not necessarily the feature functions, but how do we ensure that the right person is looking at the right data? (R1)

> I know there's a variety of views as to whether this is better outsourced or done in house... we elected to run this project ourselves because we're going to be in the billing business [forever]... as far as knowing if we can install the [smart] meter, if we can back all the data and turn it into an accurate customer bill, we had no knowledge of that... of how you're going to support and enable [and]... protect privacy. But how are you going to do that if we outsourced that? Because the expertise is going to walk away at the end of the project. (U6)

> Well we would have to have customer consent before we pass on any data to any third party, that's very clear in our privacy policy, so we can only use customer's data for our running of our business. We're very specific in that. So without major changes in our policy, which as I said we're not indicating at this time, we would not be passing data on to third parties. (R2)

Participants also noted that it is possible for customers to bypass their utility completely, and process their electricity data directly with third parties.

> [T]here are some devices available, rather than using the data from the utility that actually communicate through the internet. They clamp on to the wires, take their own readings and send the data… It communicates essentially over a router in your house and out over the internet to Google and you go on to the Google website and it's integrated with all your data. So that's a good example of how you can have the same things as being talked about over the Smart Grid but to actually have no interaction with the Smart Grid whatsoever. (R3)

Consent

Participants were unanimous on this important point. Customers in Ontario had no option to opt-out of the use of Smart Meters, and were not asked to consent to their introduction. Participants were unaware of the need for consent from a data protection perspective or for the need to provide individuals with choice and control over their information processing. Participants pointed out that the

Smart Grid was mandated in Ontario by the legal framework created for energy and environmental purposes.

> We're following the Ministry of Energy and Ontario Energy Board guidelines and rules and regulations, so no, if it's been mandated that all residential and small business consumers will have the smart meter and be moved on to the TOU rate structure, unless they're with a retailer, so no it's not customer choice here in Ontario. (U2)

> It's local distribution companies' understanding from the Ontario Energy Board that we have no choice. The customer shall be - if the customer is of a particular class - that customer will have a smart meter and they will be billed on time of use pricing and they will have no choice to opt out. (U1)

> The regulation mandates universal implementation. (U6)

Participants were further probed on this point, asked to respond to the hypothetical scenario of a customer willing to be billed at the highest TOU rate in exchange for avoiding personal information collection through the Smart Meter. Participants were again unanimous that this was not an option available to customers in Ontario.

> It's my understanding that it is not [possible]. (U1)

> But the reality is, you know, even though you [would have] opted out by signing that contract, we will continue to collect hourly data. (U5)

> You can buy a fixed price contract with a retailer, but the reality is we're compelled to install smart meter at your residence and gather time of use data for the purposes of the provincial repository, whether the customer favours it or not. (U6)

PIPEDA as Consumer Tool

Participants were asked to consider whether PIPEDA could play a role in potential disputes between utilities and customers over electricity bills. Ontario's shift to TOU billing was accompanied by a rate increase, which highlighted the fact that TOU is a load management tool rather than an energy

conservation tool as some had thought it to be.[14] The ensuing consumer backlash raised the possibility that privacy legislation would be used by individuals as a legal tool against utilities in challenging billing accuracy, demanding access and correction of personal information, and so on, much along the lines that privacy legislation has been used or attempted to have been used, in general litigation and in employment disputes.

One participant (U1) noted that access/privacy legislation has already been used to obtain information on the Smart Meter program in general. Most participants focused their responses on the governmental accuracy standards that meters have to meet, and thought those standards would prevent the use of PIPEDA in challenging billing accuracy.

> And again, our Measurement Canada requirements haven't changed. If the customer has a concern about high consumption or the accuracy of the meter, we will pull that meter, we will test in on our test boards – we're a regulated meter test shop… – if the meter tests fine and the customer still isn't satisfied, they have the right to go to Measurement Canada and request a second independent test of the meter, so really whether it's interval data, through smart meters or through a conventional meter, our processes around data accuracy and our standards haven't changed. (U2)

> Well at the end of the day, the meter is the meter. One of the things that Industry Canada is very strong on is, you know, the reading... you will be taking the reading from a register and that reading is absolute. (U5)

Some participants thought PIPEDA could be brought in as a consumer tool in interactions involving third parties, but were not certain that the utilities would necessarily be parties to such disputes.

> I think it just comes down to once you start pushing the data out to somebody else and it comes into your home, then that might be a whole different ball game, right? And actually I think [we] wouldn't be liable for that anyways. It would be more the other parties, 'what are you doing with your data'? I would care about that as a homeowner. 'You're profiling me? Who else do you have?' Kind of like PIPEDA, right?... So that's what will happen if somebody signs an agreement with a Google. You allow Google to send this info to every electrical [sic] energy

[14] See e.g. John Spears and Robert Benzie, *What's the return on $1 billion smart meter investment?*, The Toronto Star http://www.thestar.com/business/cleanbreak/article/949116--what-s-the-return-on-1-billion-smart-meter-investment

> saving company manufacturer in the world, and you start to get targeted. That's where I think you want to look at. (U2)

Ultimately, participants did not find the use of PIPEDA in consumer disputes intuitive.

Smart Appliances

Smart Appliances are household appliances that have the ability to communicate wirelessly through a Home Area Network (HAN) and allow customers to manage them remotely. The HAN functionality allows management by utilities as well, which utilities could utilize as part of load management. Utilities already engage in an earlier-generation version of such load management through programs such as Ontario's PeakSaver, which target heavy-load appliances such as air conditioners.[15] Participants were asked, on the assumption that utilities would want to manage Smart Appliances as part of their load management, about how they will incorporate Smart Appliances into the Smart Grid.

Participants pointed out the deficiencies of the existing grid, but some questioned whether Smart Grid technology, and specifically Smart Meters as deployed across Ontario, was in fact compatible with Smart Appliances.

> The program's a good idea; the [existing] technology's a piece of junk. The problem with it is that there's no verification that the load came off the system. The IESO can't use that as in-demand response because they don't know if the load reduction actually ever materialized. Where we want to get to is a two-way system that says 'whatever quantity' load came off the system. (U6)

> [W]hile the systems are potentially capable of doing it, the meters that have been installed across the province are not capable of providing that. So my sense would see that if it were to be legislated or mandated, we're into a situation where we're going to be replacing 100% of the meters again, essentially throwing away a lot of money that we just put into doing all these meter changes up to this point. (U1)

Moreover, and somewhat surprisingly, participants were reluctant to identify Smart Appliances as a load management technique that they would adopt. Participants suggested that Smart Appliances are

[15] For more information on such programs see for example http://www.torontohydro.com/sites/electricsystem/electricityconservation/residentialconservation/Pages/peaksaver.aspx

essentially a consumer feature, as part of a futuristic HAN, and that it would not have great relevance for load management.

> I'm not sure, to be honest, if we decided that we want to go that deep into the homes, and I think the same goes for many of the other utilities in Ontario… [T]he strategy with the air conditioner was that it's related to the peak. We're a summer-peaking province and typically when it peaks it's because of air conditioning. Now would we get into controlling other appliances like stoves? Well if people want to cook, people want to cook. Now if we were a winter-peaking [province], or if we started to develop a serious peak in the winter, then do we want to control heating? Well heating is more essential than air conditioning. There [are] all kinds of appliances that you can start controlling… (U2)

> I think GE has the capability to build them. Currently, it's a rather premium line that they're testing it in. So it's not like tomorrow every fridge that's being sold is going to have them. It's going to be a premium product for some period of time, I don't know how long, it could be a very long time. It may never be in the average fridge. Time will tell. (U3)

Participants also thought these were early days for Smart Appliances, particularly in the absence of a US standard.

> I've seen some things that indicate that there may be some available later this year, but I'm surprised at that because the National Institute of Standards in the States that's working on an interoperability standard for the smart grid, which would include the appliances, and their work isn't expected to be done for a couple of years. I'm not sure how that's going to play out. I think the big thing on any of those smart appliances is that it's all going to be based on the standard. (U5)

> I'm not going to have [hundreds of thousands of] customers in 18 months tell me 'you're the idiot who sells ZigBee. That's yesterday's technology. (U6)

Participants were aware that even use of Smart Appliances by consumers could have security and privacy implications for utilities.

> [W]here I look at the Smart Appliances, that's more on the customer side. What I have to make sure of is that they're going to start buying those things. Those appliances are going to be

looking for information from me. I have to make sure that information's available securely to them. That's my next ten yards is to get through that. (U4)

I've got to guess that… someone's going to figure out how to sit in front of your house and intercept those signals and manipulate them if they want to. Now why anyone would want to turn on my dryer and turn it off is beyond me, but there may be people who get their kicks out of doing stuff like that. (U5)

Discussion

The findings above raise a series of questions discussed in this section, such as whether the current and planned processing of personal information comply with PIPEDA and the proper role of other regulators and regulatory regimes besides the Privacy Commissioner of Canada.

The Legal Grid

It is beyond the scope of this report to delve into the many ways in which energy and privacy are regulated across jurisdictions. The electricity industry has undergone privatization to some extent, with the introduction of independent energy retailers, but just as significantly, with the meaning that utilities themselves may actually be private, for-profit corporations (such as industry giant Fortis) while remaining under public regulation in order to ensure that Canadians are provided with electricity.[16] Since the interviews were conducted with Ontario utilities this report will use Ontario as an example. Electricity is regulated in Ontario through the aforementioned *Electricity Act*. This Act establishes how electricity is generated, transmitted and distributed across Ontario and how prices are determined. The Act also governs the establishment of the Smart Grid, as discussed above. The Act, together with the *Ontario Energy Board Act,* establishes an energy market regulator, the Ontario Energy Board, which oversees the independent retailers, the various utilities and other bodies such as the IESO. In other jurisdictions where the energy market has been somewhat deregulated similar governing bodies have been introduced, such as California's Public Utility Commission.

While the legislation dedicated to the energy sector governs in principle all aspects of this sector, it does not explicitly (neither directly nor through regulations) address the information collected by the operations of utilities and other bodies. Historically, as public bodies, these organizations fell under the jurisdiction of Ontario's access/privacy legislation. Arguably, as they continue to fulfil an essential public good, these bodies should continue to be considered under the jurisdiction of this legislation, particularly with respect to freedom of information. Within the access/privacy regulatory regime exist two statutes. Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) regulates the provincial government and its institutions, while its counterpart, MFIPPA, regulates municipal governments and their institutions. A body such as the IESO would be governed by FIPPA, while Toronto Hydro would be governed by MFIPPA. Since the two acts are essentially identical the distinction is of little consequence.

[16] Electricity in Canada is subject to provincial jurisdiction.

Of greater consequence is the realization that access/privacy legislation is not set up to address commercial flows of information. Its main purpose is to ensure that citizens have timely access to the information used by the government to operate, in the interests of transparency and public accountability. The legislation is also concerned with ensuring that government does not collect unnecessary information on its citizens, and that members of society have some rights in this information to ensure the democratic and free nature of society. Access/privacy legislation upholds liberty – freedom from government – as a core value. It is less concerned with dignity – the social status and societal reputation that are impacted primarily by transactions *between* members of society, such as commercial transactions.

Ontario does not have commercial data protection legislation (only three other Canadian provinces, Alberta, British Columbia and Quebec do). By default, commercial transactions are governed by Canadian federal legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Private sector retailers in Ontario, such as supermarkets and drugstores are governed by PIPEDA, as is the financial services sector. However, public sector entities that engage in commercial activities, such as Ontario's Liquor Control Board of Ontario (the LCBO is one of the largest retailers of alcohol in the world and a de-facto monopoly in Ontario) have traditionally been governed by Ontario's access/privacy legislation and were not made been subject to PIPEDA when that legislation was applied to the provinces in 2004.

With all its flaws (PIPEDA is a traditional piece of data protection legislation, ill-equipped to deal with issues such as online privacy) PIPEDA is more suited to govern the data that will be generated by the Smart Grid than access/privacy legislation. For example, it is clear that the Smart Grid will generate commercial data flows, and that consumers will want to use some private sector products to manage their electricity consumption. These private sector exchanges would fall under PIPEDA. Further, PIPEDA, unlike access/privacy legislation, incorporates within it the next generation of Fair Information Practices (FIPs) – a robust set of principles aimed at ensuring consumer choice, control, agreement, transparency and accountability – to mention a few – over the use of personally identifying data.[17] Public sector bodies, including utilities, have already recognized these principles in their earlier

[17] The full set of principles is given in PIPEDA, Schedule A.

iteration as Canada's model privacy code, and incorporated them into their privacy policies. Indeed, Toronto Hydro, mentioned above, refers to PIPEDA as its governing legislation alongside MFIPPA.

This, in turn, raises a host of jurisdictional and regulatory questions that should be resolved. What is the regulatory boundary between Ontario's Information and Privacy Commissioner (IPC), and the Privacy Commissioner of Canada? MFIPPA is governed by Ontario's IPC, whereas PIPEDA is governed by the Privacy Commissioner. What issues are to be considered MFIPPA issues, and what issues are PIPEDA issues? Where should the utility see Ontario's IPC as its authority and regulator, and where should it turn to the Privacy Commissioner of Canada for guidance and supervision? Where should a customer go to complain about her local utility and its information practices? Should she turn to the provincial or to the federal regulator?

Ironically, jurisdictional boundaries in Ontario have become blurrier due to the innovative work done on the Smart Grid and privacy by Ontario's IPC. The work, which broke ground in identifying privacy risks associated with the Smart Grid, and culminated recently in a suggestion to build "privacy by design" into the Smart Grid, has created the impression that the Smart Grid – and in particular – the commercial data flows it will generate - is subject to provincial jurisdiction, when in fact commercial processing of personal information is squarely within federal jurisdiction and is governed by the Privacy Commissioner of Canada. Participants, as noted above, felt they were required to comply with the instructions of Ontario's IPC (and in fact they probably do in some respects) and perhaps felt less guided by the OPC.

It should be relatively easy for the two privacy regulatory bodies (and by extension, for privacy regulators across Canada) whom have worked together and continue to cooperate on many initiatives, to reach an agreement on their respective regulatory mandates as far as the Smart Grid is concerned. It seems, based on the nature of the legislation and the findings above, that utilities should continue to be regulated by the provincial commissioner with respect to their public nature, translating mainly into provincial regulation of access to information. At the same time, utilities should clearly turn to the federal commissioner for all personal information protection issues, and customers should clearly understand that their personal information is protected by PIPEDA.

The PIPEDA framework is well-suited to deal with the privacy questions raised above, and provides consumers with the opportunity not only to ask these questions, but demand answers. Under PIPEDA

there are restrictions on the managing of personal information, both through the principle of data minimization (the significance of which is discussed further below), through the principle of reasonable management throughout the information's life cycle, and through the principles requiring the notification and consent of individuals to the handling of their personal information by others. In such a manner for example, utilities will be required *not* to measure consumption at shorter that hourly intervals, even though meters can measure consumption more rapidly. And utilities will be required to ask consumers to consent to the disclosure of their data to private sector parties such as independent market retailers or software giants such as Google. Toronto Hydro, for example, has partnered with Google to produce to helpful visuals above, yet no attempt was made to notify, let alone ask customers to agree, to this partnership. Such conduct could well be a breach of PIPEDA.

Then, of course, there is the matter of disclosure of personal information not only to the private sector, but to law enforcement agencies. Police services have known for quite some time that energy consumption can be an indicator of criminal activity. The in-house cultivation of marijuana (referred to as a grow-op) requires large amounts of energy, above and beyond normal residential consumption. Police services have asked, as a result, for the ability to access and monitor utility consumption data. (Extremely low consumption is also suspicious – criminals may simply be stealing electricity.) In some jurisdictions this is achieved by enabling online access to the utility's database from a police computer, without court supervision or authorization. That, in fact, was the practice in parts of Canada until it was challenged in the *Plant* case cited at the beginning of this report. In *Plant* the Calgary Police used such access to locate an address in which electricity consumption was four times the average residential consumption. The police used this data to ask for a search warrant and when the warrant was granted the police found a grow-op on the premises.

In analyzing the collection and use of information by law enforcement agencies courts question whether Constitutional rights have been duly protected, rather than whether personal information protection legislation has been followed. Such legislation typically contains provisions that allow organizations to disclose information to law enforcement agencies when criminal activity is suspected (there are other such 'disclosure loopholes' as well). Furthermore, such legislation did not exist in Canada and Alberta in 1993. The relevant Canadian Constitutional section is Section 8 – "Everyone has the right to be secure against unreasonable search or seizure." The Court therefore had to determine whether the computerized access granted to the Calgary Police was unreasonable

While the Court did set the standards for warrantless searches the Justices differed on the issue of privacy in electricity records. Justice Sopinka, writing for the majority, determined that there is "no reasonable expectation of privacy with respect to computerized electricity records". However, Justice McLachlin (as she was then) disagreed, voicing the opinion presented above. As a result some jurisdictions have passed legislation explicitly authorizing police such access, some utilities simply allow access, and some require court authorization – production orders.

Recently, in *R v Gomboc,* the Court revisited the constitutionality of requesting electricity records without judicial supervision.[18] Mr. Gomboc was suspected of running a grow-op by Calgary Police. The police contacted the utility directly, without requesting court authorization, and asked them to install a Smart Meter equivalent, known as a digital recording ammeter (DRA), to measure the flow of electricity into Mr. Gomboc's house. The information recorded by the DRA was then used to request a search warrant for the house itself. Unfortunately, the Court split three ways in determining whether Mr. Gomboc's Charter rights were violated. Five Justices found that the DRA did generate personal information and therefore that Mr. Gomboc had a subjective expectation of privacy. Three of the Five Justices, however found that he had no *reasonable* expectation of privacy since Mr. Gomboc could have asked his utility (as could every customer) to keep his electricity consumption private, an option that he failed to exercise. The remaining Four Justices found that the DRA did not create personal information, and therefore did not consider whether any expectations of privacy arose. The result was that Mr. Gomboc's appeal was denied and the Court ruled that the police did not violate his Charter rights. Importantly, however, a majority of the Court did find that personal information is created by the use of devices similar to Smart Meters.

While the Supreme Court was busy sorting out these issues a dispute in British Columbia over electricity consumption occurred. The police applied for a production order requesting names and addresses of all customers of BC Hydro that consumed more than 93 Kilowatt Hours per day. BC Hydro objected that this threshold was too low, and that 1115 customers in North Vancouver and 100,000 across BC would have their name and address disclosed to the police as a result.[19] The police withdrew their request once it was clear BC Hydro would challenge it formally, but the approach of the police is

[18] *R. v. Gomboc*, 2010 SCC 55. Available at http://scc.lexum.org/en/2010/2010scc55/2010scc55.html

[19] See news reports http://www.vancouversun.com/Hydro+fights+RCMP+power+records/3090498/story.html

telling – law enforcement agencies will request information once it is possible to obtain it, and the introduction of Smart Meters will provide many more possibilities for such requests.

Smart Meters

The installation of Smart Meters has far-reaching privacy implications, due to the amount and nature of information Smart Meters collect and the data analysis that they enable. While TOU pricing is typically being deployed on the basis of hourly consumption measurements, Smart Meters are actually capable of measuring consumption at much shorter intervals, of a few seconds.[20] Ontario's *minimal* standards, for example, require that meter readings be identified by a per-minute time-stamp, and that the information be transmitted by the meter to the utility for billing purposes on an hourly basis.[21]

Smart Meters are measured wirelessly on a dedicated communications network. Meters actively transmit their readings via antennas to a central database, which is typically managed on behalf of utilities by an independent organization. In Ontario, this organization is known as the Smart Metering Entity (SME), and the already existing independent price regulator, the Independent Electricity System Operator (IESO) was designated as this entity, and assumed databases responsibilities as well.[22] Smart Meters generate a wealth of information that arguably is personal and has the capacity to identify individuals and households. It is important to understand that these new meters *create* this personal information through their measurement technology, as well as collect it. The personal data are then used by the SME and by utilities for a variety of purposes such as (of course) billing, electricity demand management and grid stability management.

A distinction must be made between the data created and collected for billing purposes, which are transmitted on an hourly basis, and between the data created for those other, operational purposes. Based on the findings (see e.g. U2 quote above) it appears not only that utilities will use Smart Meter data for operational purposes, but that such data, in order to effectively assist operations, will be created, collected and transmitted on an almost real-time basis, as is indeed technically possible. There are privacy implications to both forms of transmission that must be considered and addressed by utilities and regulators.

---

[20] See e.g., California Energy Commission, Proposed Load Management Standard, p.25, http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF

[21] http://www.mei.gov.on.ca/en/pdf/electricity/smartmeters/AMI%20Specifications%20July%202007.pdf

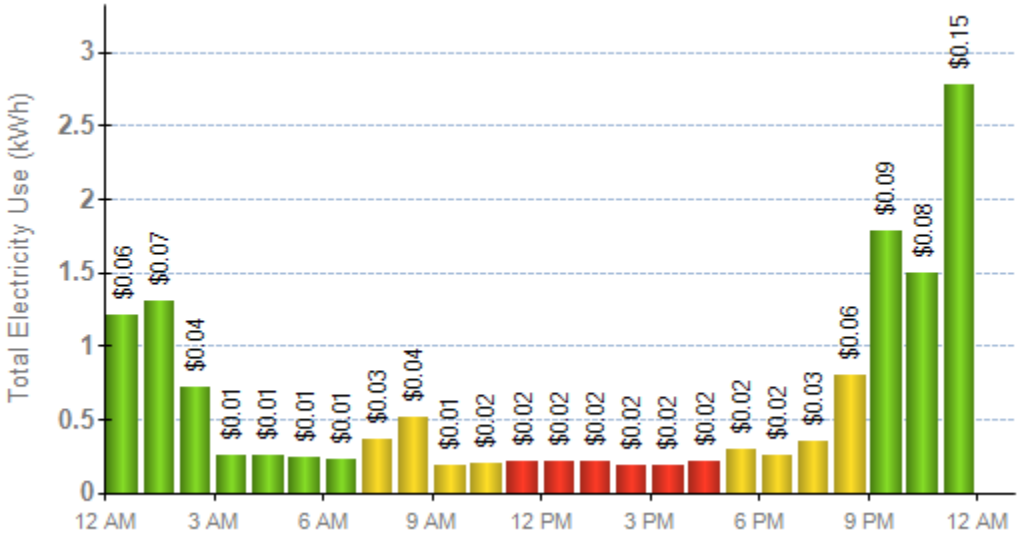
[22] Ontario Regulation 393/07 of the *Electricity Act*, 1998.

In addition, the personal information collected can also be disclosed, both by the SME and by the utilities, to commercial, private-sector third parties with expertise in data analysis and online services, and of course to other branches of government such as law enforcement agencies. In the US, for example, online giants such as Microsoft and Google are already in the Smart Grid market, with consumer focused products such as Microsoft Hohm and Google PowerMeter, that offer users the ability to manage and control their energy consumption by using the data generated by Smart Meters. A myriad of smaller corporations that offer a variety of consumer devices operate in the market as well, and have called for unfettered access to meter data in the name of competition and innovation.[23] For the Smart Grid to succeed in its demand management goals, energy consumers must have easily understood and readily available data at their disposal in order to make informed consumption decisions, and some utilities (such as Toronto Hydro) recognize that the repackaging of information is not their forte and have teamed with online companies to create an appealing consumer interface.

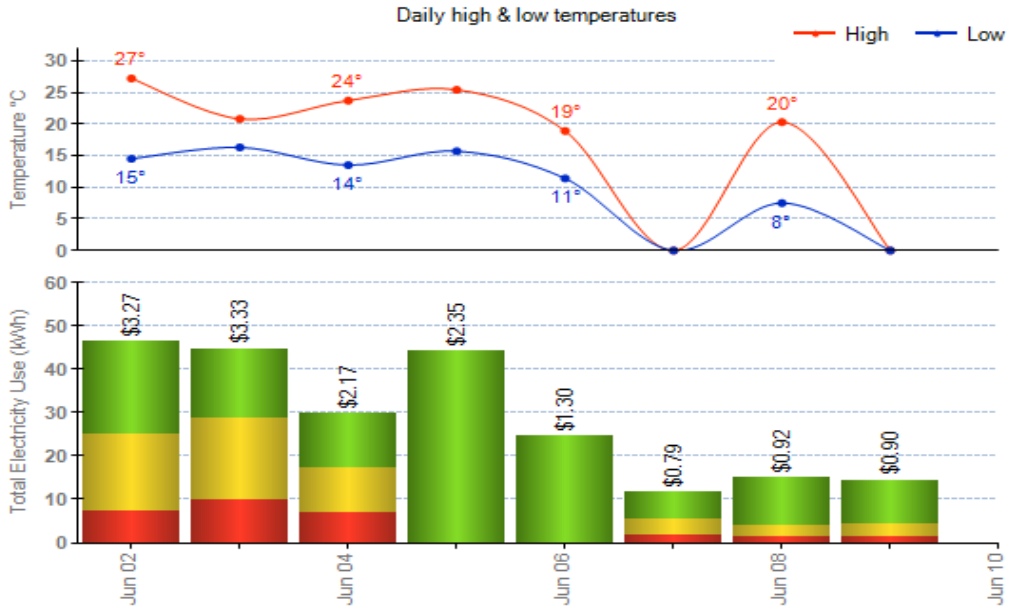
Billing Information

The following page provides an example of the billing information generated by Smart Meters already deployed by Toronto Hydro and made available to its customers:

[23] According to a survey conducted by the US NIST about 70% of respondents stated that (consumer) authorized third-party service providers should have a clear right to unmediated access of the near-real-time smart meter usage data. See http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/OSTPConsumerInterfaceSmartGrid#DataOwnershipandAccess



Customers are able to understand their hourly consumption over a 24 hour period, as well as the price the will pay for that specific hour (based on the color coding). Toronto Hydro also provides customers with the opportunity to understand their usage against other relevant information, such as the temperature:



In this "mash-up" (combination of information from several different sources) a customer is able to view her weekly consumption and compare it with the daily temperature (note that although consumption on Saturday was high the customer only paid the lowest rate, based on the weekend pricing used by Toronto Hydro).

This information is undoubtedly extremely helpful to consumers that truly wish to conserve energy and lower their bill. However, it does come at a privacy cost and raises questions of personal information. Should these data be treated as personal, identifying, information? Are there property rights in this information, and, if so, who owns it? Should there be restrictions on the creation, collection, use and disclosure of this information? If so, what should be these restrictions?

Based on the findings, it is clear that some preliminary confusion exists about the role of the location of the meter, which traditionally has been located externally on residences, to allow readers easy access, and the nature of the information the meter generates. Put differently, information may be publicly available and still personal and identifying, and its availability, or potential to become publicly available does not render it as unworthy of legislative and regulatory protection. This confusion is significant, and discussed further below, in the context of the role of consent and PIPEDA's framework as applicable to the Smart Grid.

On the other hand, it appeared clear to most participants that billing information, especially when linked with customer identifying information, becomes personal and has the potential of identifying not only customers but also patterns of behaviour when analyzed. The efforts of Ontario's IPC have been to ensure that the transmission of billing information, and its linkage with customer information, are done in a secure manner and that data analysis is limited or done on an aggregate basis.[24]

Operational Information

Data created for operational purposes is not available to customers. However, it can identify ongoing activities within a metered location and is therefore arguably personal. In order to understand why the operational information generated by Smart Meters is personal, it is necessary to look at technology that has existed since the 1980s and is in many aspects the precursor to today's Smart Meters. This

[24] *Supra* note 10.

technology is known as Non-Intrusive Appliance Load Monitoring (NILM) and it allows utilities to measure the consumption of electricity on a per-second basis, just as Smart Meters do today.[25] As discussed by Quinn in a series of papers, NILM creates very detailed information about ongoing activities inside a house, through external monitoring, and so branding it as "non-intrusive" is somewhat of a misnomer.[26] It is worth copying Quinn's example in some length, to drive home this point. This is a graph of electricity consumption over 24 hours, created by NILM:

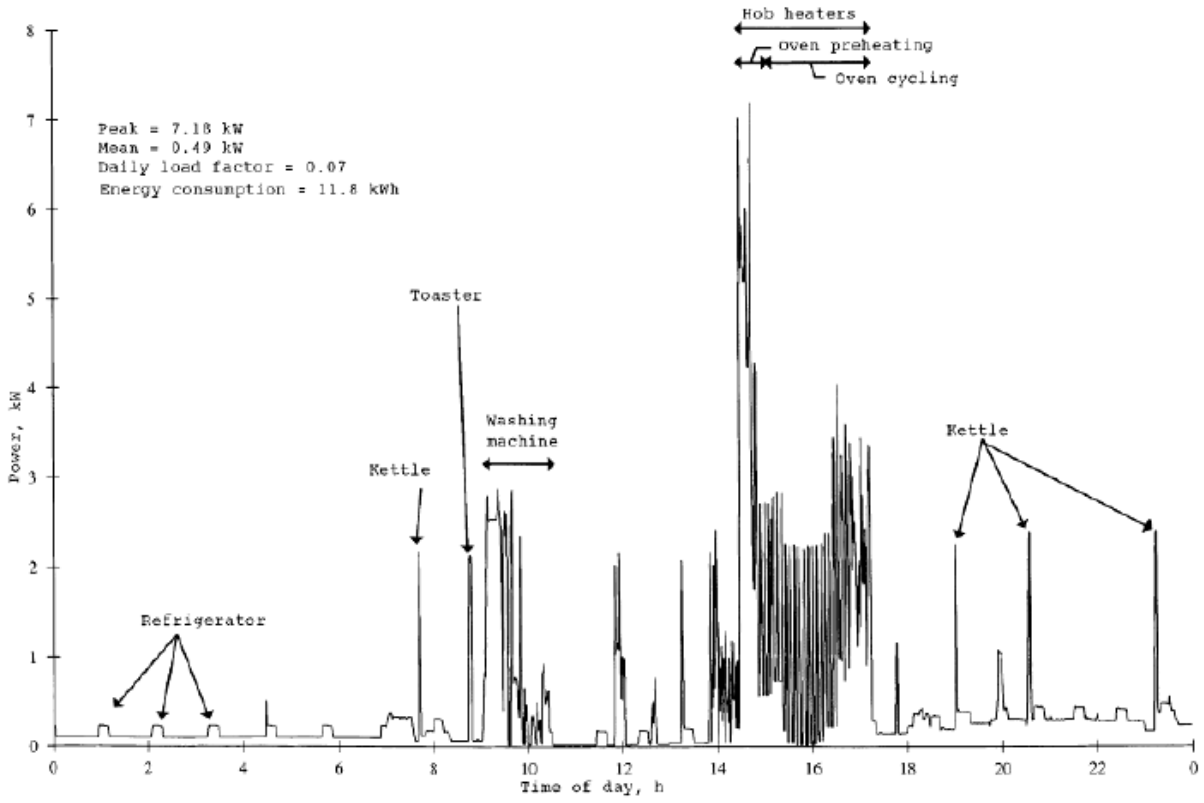


Figure 3: Household Electricity Demand Profile Recorded on a One-minute Time Base[139]

The graph provides a narrative of an individual, let us call her Ann, which woke up around 6:30am, put the kettle on just before 8am, had toast for breakfast around 9am, and then put on the wash. Later that day, around 3pm, Ann started on dinner, which was ready around 5:30pm. Suffering from

[25] Elias Quinn *Privacy and the New Energy Infrastructure*. http://ssrn.com/abstract=1370731

[26] Quinn, *id*; Mikhail Lisovich, Deirdre Mulligan & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems* IEEE Security & Privacy 2010.

indigestion, or perhaps being queasy at the thought of being monitored in this way, or perhaps, as Quinn suggests, being British, Ann had several cups of tea later that night.

Whereas NILM has had, up to now, to have been deployed especially and specifically (in response to some commercial or legal concern), Smart Meters will generate similar data flows and similar narratives effortlessly and routinely, unless restrictions are placed on their deployment and the measurements they actually make. There is no doubt such information is highly personal and intimate, and has traditionally required actual surveillance of the inner parts of a residence and court authorization.

Left unregulated therefore, the detailed information provided by the Smart Grid will come at the expense of privacy, since it will be possible to determine, without conducting surveillance that would normally require court approval, patterns of behaviour within a household, such as when clothes are washed or hot showers are taken, that many would consider intimate.[27] That would allow law enforcement agencies, for example, to determine whether certain houses are used for the growth of marijuana or for other illegal purposes, by simply accessing the information generated by the Smart Grid.

The perceptions of participants of operational data as "operational" and therefore lacking privacy or personal implications is problematic in this regard. Similarly, it may be that customers are even more unaware of the generation of operational information by Smart Meters and of its privacy implications. Public discussion of this aspect of the Smart Grid hardly exists and should be addressed through further public awareness initiatives by OPC.

Smart Appliances

The ability of the Smart Grid to create personal information will be enhanced even further when Smart Appliances are introduced. These household appliances, such as a washer, dryer, dishwasher and refrigerator, will also be able to communicate wirelessly with the Smart Grid, and receive instructions to turn on or off, or work as reduced capacity, as necessary. While these are all laudable goals that will help utilities manage ever-increasing demand, and improve the stability and reliability of our energy

[27] In *Kyllo v. United States* 533 US 27 (2001) the US Supreme Court stated that the time in which "the lady of the house takes her daily bath [is] a detail that many would consider 'intimate'".

supply, it is clear that Smart Appliances will be another source of personal information, and a more direct and reliable source than Smart Meters and their information. Whereas an energy consumption graph such as the one generated by NILM and Smart Meters has to be analyzed and compared with experimental data to deduce what appliances operate within a residence, Smart Appliances simply provide such information directly and without complication to the utility, and from it to its private-sector partners and potentially to law enforcement agencies.

The findings indicate that Smart Appliances are not on the immediate horizon for utilities in Ontario, in the absence of US and Canadian inter-operability standards. However, manufacturers are moving ahead with the introductions of products, and the HAN (Home Area Network) is of particular interest to software and technology companies such as Microsoft and Google in addition to household appliances manufacturers such as GE and LG (whose vision for the HAN is presented below).[28]

[28] See http://www.lgnewsroom.com/ces2011/view.php?product_code=3&product_type=3&post_index=102

Given the enormous potential of HANs to generate personal information in conjunction with the Smart Grid, utilities must clearly define their future role, and give particular thought to scenarios in which government may mandate the collection of HAN information by utilities for the purpose of energy conservation, for law enforcement, or for any other purpose.

The Practice of Personal Information Protection

How are utilities managing personal information when viewed from a data-protection perspective? The findings indicate a number of personal information protection issues in which utilities could develop better practices. Utilities have not had a great need for such practices until the development of the Smart Grid, since they concentrated more on their public mandate of energy provision, and the old grid did not generate significant quantities of personal information. Monthly billings are not that revealing, and customer information for billing purposes has not been a sensitive category of information that required special attention beyond the usual safeguards. It is no surprise, in that respect, that privacy issues in electricity records emerge in litigation when consumption is monitored continuously, as will be the case with the Smart Grid.

Privacy Policies

It is incomprehensible, from a personal information protection perspective, that a major transformation in the processing of personal information will occur and that it will not be reflected in an organization's policies, yet that precisely is the situations with many Ontario utilities. While some policies refer to PIPEDA, as they should, most contain boilerplate provisions and can be thought of as "first-generation" policies that repeat PIPEDA's principles while avoiding meaningful talk of the actual processing of data that occurs due to the Smart Grid.[29] The privacy policies of utilities must be modified, to account for the ways in which the Smart Grid and Smart Meters have changed and will change the processing of personal information.

Disclosure

Utilities do not treat disclosure of personal information to third parties consistently. On the one hand, participants were clearly supportive of consumer choice, and it is probably a good practice to allow consumers control, and the responsibility that comes with it, over disclosure of individual consumption data to third parties that offer HANs and consumption management. Utilities are somewhat familiar in

[29] Toronto Hydro's privacy policy (effective date: 2010-04-07) does not include or refer to the terms "Smart", "Meter" or "Grid". http://www.torontohydro.com/sites/electricsystem/Pages/PrivacyPolicy.aspx

dealing with third parties thanks to the privatization of the energy market in Ontario and the introduction of independent retailers. It is probably inevitable that as the Smart Grid starts generating more granular, personal information on consumption that independent retailers will want, and claim, access to such information in the name of free and open competition.

On the other hand, utilities appear to not have given much thought to their cooperation with third parties in a systemic manner, and specifically to the question whether individuals should have a say in such cooperation. Disclosing personal information to third parties at the utility level, even if it is a service that some individuals would desire, may introduce an unnecessary complexity into an already complex personal information system. Further, disclosure to independent energy retailers may raise different issues, both commercially and from a personal information protection perspective, than disclosure to HAN managers, making it difficult for utilities to draw upon their experience with independent retailers when dealing with new requests. Several utilities have partnered for example, with information technology and data management businesses to handle the processing of billing information and the manner in which it is made available to customers. Viewed from an information protection perspective such disclosure, particularly since it is done for a new purpose and does not constitute a previous or existing business practice, requires the notification and consent of individuals.[30]

Utilities should evaluate and decide upon their preferred approach to information disclosure, and careful consideration should be given to the inadvertent impact that regulation or deregulation of the energy market may have for the protection of personal information and the disclosure demands that third parties may make. A prudent approach would direct third parties to customers, leaving individuals the ultimate control over sharing their personal information rather than acquiescing to utility-driven disclosures.

Consent

Probably the most glaring problem that attempting to apply personal information protection to the Smart Grid framework creates is the problem of the absence of consent as it is required by law. PIPEDA, similar to all data protection legislation (but significantly, unlike access/privacy legislation) is based on the principle of individual control. According to this European principle individuals should

[30] For a current list of Google's partners see http://www.google.com/powermeter/about/partners.html

control their personal information since individuals are autonomous and should be empowered to interact with other members of society as they see fit. Control manifests itself through the ideas of choice and agreement. Individuals must be able to choose what to do with their personal information, and must be able to agree to the actions of others that bear upon their data. Translated into legal tools, these ideas become the principle of consent, and the mechanisms of opting in and out of information processing initiatives. There are of course other important data protection principles, all enumerated in PIPEDA, but they could be all said to support in some way the basic idea of individual control.

As found above, the Smart Grid does not offer individuals any choice or control over their personal information. Smart Meters will create personal information that did not previously exist, without allowing individuals an option to opt out. This information will then be collected by utilities and then used for billing and operational purposes, again without requiring consent or providing individuals with alternative options. The information could very well be disclosed to third parties for secondary purposes, again without asking customers to agree and as perhaps is already occurring, without customer notification.

All of this processing of personal information appears to be in clear violation of the Consent Principle as it is outlined in PIPEDA's Schedule 1. The existence of a regulatory and legal framework mandating (in Ontario) the installation of Smart Meters as a by-product of the development of a Smart Grid does not serve as an exemption or a reason for utilities – as commercial entities – not to be in compliance with PIPEDA. In fact, the legal framework in Ontario obligates *utilities* to use Smart Meters and does not apply to individuals directly.[31] Meters, old and new, are utility property, and utilities have relied on the traditional legal elements allowing them access to property for a variety of electricity-provision purposes (including billing) and the sanctions these elements carry (including disconnection from service) as the framework that facilitates the installation of Smart Meters. This reliance, of course misses the point about the privacy-based objection to Smart Meters. It is not the device that is problematic from a personal information protection perspective, but the information that it generates. In such a manner the debate resembles other property/privacy debates, such as workplace privacy expectations debates, in which employers argue that their property rights in technology such as computers trump the expectations of privacy that employees may have in the information stored.

[31] See Ontario's *Electricity Act* §§ 53.7-53.21 and the related regulations.

Furthermore, the lack of change and revision found in privacy policies prevents utilities from claiming that they have already obtained consent for Smart Meter information processing. PIPEDA specifically requires organizations to obtain consent when a new purpose is identified for personal information (under Principle 4.2.4. of Schedule 1) yet the major transformation of the electricity grid has failed so far to meet this standard. Similarly, Principle 4.3.3. of Schedule 1 prevents organizations from collecting information unnecessary for its stated purposes, yet utilities are unable to offer customers a choice of a different, less-intrusive billing system due to their Smart Grid obligations.

Indeed, it should be clear that utilities have not initiated this dismal state of affairs, but have simply followed the dictates of Ontario's Smart Grid framework. The result is a personal information collection regime that, even with the best efforts of Ontario's IPC to build into it Privacy by Design technologically, will remain in violation of PIPEDA unless individual choice and control are built into it by regulatory action. OPC, as PIPEDA's guardian, should engage Ontario and other Canadian provinces looking into Smart Grid initiatives, to ensure that individuals retain meaningful choice and control.[32]

Where is the Focus?

It seems that utilities are occupied – as perhaps they should be – overwhelmingly with the engineering and infrastructure demands of the Smart Grid, and in Ontario, of the provincial government's mandated deployment. Faced with the monumental tasks of revamping their systems, and introducing components and structures that will facilitate the environmental and security goals of the Smart Grid that are key to its definition, such as generation facilities embedded within the distribution system, two-way transmission, load management and prediction etc., utilities have little attention to spare to the privacy implications of the Smart Grid, and executives are by nature individuals with engineering backgrounds and focus. Even when attention is paid to privacy and personal information protection, the approach, perhaps due to Ontario's IPC Privacy by Design ideology, remains focused on the design of systems and components that will achieve some technological, privacy-supporting purpose.[33] Similarly, the identification of risk, the meaning of risk, is for participants the risk that the supply of

[32] It should be noted that lack of choice has emerged as a political issue in Ontario during the 2011 provincial election campaign.

[33] For example, Ontario's IPC Smart Grid Case Study focuses on the division of the grid into domains, and designing the appropriate data flows between domains. It notes that "Smart Meters, while a very important element of the Smart Grid, actually represent a small fraction of the overall grid." *supra* note 10, p.10.

electricity would be disrupted by either physical attacks, cyber attacks, or some combination of both. Again, that is as could – and should – be expected, but utilities cannot focus as a result on personal information and the potential risks to privacy

As a result, insufficient attention is paid to the features of the Smart Grid that have caused the greatest concern for consumers and privacy advocates from a policy perspective. Smart Meters, Smart Appliances, HANs, third-party access to personal information, privacy implications of operational data, the governing regulatory framework, the applicability of privacy policies, are all issues to which utilities have devoted until now – understandably – only a fraction of their time in comparison with the time and resources spent on the actual work of deploying the Smart Grid according to government mandate and plan. The balance of time and resources has to change if customers are to be provided with meaningful personal information protection and with answers to the Smart Grid privacy issues that they perceive as relevant.

Do We have to Save Energy at the Expense of Privacy?

When Smart Appliances and Smart Meters are fully deployed the Smart Grid may very well end up creating personal information on an unprecedented scale. It is now clear that the protection of personal information must be at the heart of the deployment of this technology. Ontario's Privacy by Design principles are instrumental and helpful here, yet they cannot stand alone. Personal information protection legislation is required, and PIPEDA, with all its flaws, is the legislation to which utilities and consumers should turn.

Space precludes here a complete analysis of the respective strengths of the environmental and privacy advocacy movements, but suffice it to say that privacy advocates have always looked to the environmental movement as a model for a successful grassroots initiative that has captured the public and political agenda.[34] It is doubtful that in a direct confrontation privacy would be chosen over the environment, and indeed, the deployment of the Smart Grid and the regulatory framework set for the Smart Grid by energy regulators in Ontario has all but ignored PIPEDA and would have ignored privacy completely were it not for the efforts and activism of Ontario's IPC. Probably the best course of advocacy for those concerned over privacy would be to argue along the lines of Ontario's Commissioner – that it is possible to have privacy and save energy at the same time.

[34] Colin Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT: 2008), p.200

This argument must be bolstered not only by practical Privacy by Design solutions, but by answers to the many data protection compliance questions that remain unanswered. The very conceptual problem posed for privacy by the Smart Grid is significant, and Canada's top court has chosen not to grapple with it in the *Gomboc* case. The Canadian court had traditionally demarcated distinct privacy interests – personal (physical – bodily integrity), territorial, and informational.[35] The court determined that personal interests deserve the highest protection from law enforcement, followed by territorial interests, and leaving informational interests for last. It was on this conceptual basis that the Canadian court ruled in *Tessling*, in contradiction to the US Supreme Court, that use of an infra-red device to look upon – and into – a residence, did not require a warrant since there was no reasonable expectation of privacy in the information (the heat signature) that was captured by the device. The court viewed the interests in the information as informational interests, and not as territorial interests.

The introduction of Smart Grid information turns these notions upside down, and shows how interconnected in fact they are. For while it is clear that the Smart Grid collects information, the privacy interest that is harmed in this collection is the territorial interest, since the collected information reveals information about the activities inside the residence, as Quinn's NILM example above demonstrates. That usage and consumption profile is much more than mere information. Simply put, it is as if the Smart Grid has the ability to render walls transparent and allow the utility and the law to gaze into a dwelling. In this sense, then-Justice McLachlin's observation in *Plant*, cited above was, while a bit ambitious on the facts in *Plant*, prescient and accurate now that the Smart Grid has arrived. At the same time, it is also important to remember that the Court addressed only the constitutional aspects of law enforcement access to electricity consumption information. The court's decisions did not touch on privacy issues that arguably play larger roles in the lives of most members of society, common commercial issues, such as the partnerships forged between utilities and online corporations such as Google and Microsoft. The design of the Smart Grid must ensure that privacy from other members of society, not only the state, is protected as well.

As discussed above, access/privacy legislation does not actually ensure that personal information is protected from other members of society (e.g., from corporations). For example, Ontario's legislation does not require that an individual consent to the collection of personal information, merely that an

[35] *R v. Tessling* 3 S.C.R. 432 (2004)

individual be notified.[36] While utilities profess to adhere to PIPEDA's higher principles their compliance is iffy. Toronto Hydro did not notify, for example, its customers on its partnership with Google. On the other hand, consent is a cornerstone of private sector data protection legislation. Other building blocks of such legislation, the principles of minimal collection, use, disclosure and retention, are also nowhere to be found in access/privacy legislation, and are found only in the privacy policies of utilities that have realized that they must comply with PIPEDA. These, as well as the introduction of the notion of *creation* of personal information into the data life-cycle, are of crucial importance to privacy in the Smart Grid era.

There is no question that electricity utilities will remain private corporations and/or continue to be privatized in those jurisdictions where they are still a government body. Independent retailers are purely commercial entities. It is also clear that the industry while privatized, will continue to be regulated by respective governments through legislation that sets industry standards and creates regulatory bodies such as Ontario's Energy Board. None of this, however, necessitates subjecting electricity companies to access/privacy legislation that is relevant to these corporations in their role as suppliers of a public good, but not relevant to their increasingly commercial operation. Access/privacy legislation is designed to provide the citizen with an answer why personal information is required in order to supply her with a health card or a driver's license, and to ensure that the information that is collected for the provision of these government services is dealt with the respect that it deserves as information that identifies an individual. It is not intended to govern commercial transactions.

In their operation and development utilities (let alone energy retailers) resemble less a government department, and more a regulated industry. An analogy, albeit imperfect, is the finance industry. It is a highly regulated industry, providing essential services to the economy of the provinces and Canada, yet its highly regulated nature does not turn it into a government body. Banks and Insurers, accordingly, are not subject to access/privacy legislation, but to provincial and federal private sector data protection legislation *in addition to* the other laws and regulations with which they must comply due to the nature of their business. If we are to hope that the Smart Grid will not bring about the largest erosion and elimination of privacy since the internet, then a small step would be to ensure that as this grid is deployed and privacy is built in, the relevant legal framework is that of PIPEDA.

[36] FIPPA § 39 (2)

The Privacy Commissioner of Canada and her office have a large role to play here. OPC is clearly aware of the important implications of the Smart Grid for personal information protection, as it has supported this research project and continues to call for further research. Yet OPC has, as of yet, not issued guidelines for utilities or engaged utilities and energy regulators in discussion over the applicability and application of PIPEDA to their work, and the Commissioner, Assistant Commissioner and other senior staff have not addressed the privacy implications of the Smart Grid in public in any detail.[37] Whether out of deference to Ontario's IPC important Smart Grid work, or by tacit agreement, the result of the absence of OPC from public Smart Grid discussion has been, as supported by the findings above, a blurring of the regulatory lines for utilities and their customers.

Applying PIPEDA to the Smart Grid is no less, and perhaps more, important than the incorporation of protective measures into its design. Much work lies ahead, in the form of meaningful privacy policies, substantive disclosure of third party data processing, and, most importantly, the provision of real choice to individuals that do not wish to have their personal information collected and used on a massive scale in the name of environmental protection. As suggested here, and as done in other jurisdictions, it is possible to offer consumers the choice of opting into the Smart Grid, "enjoying" TOU rates, and assisting utilities in their load management.[38] Consumers must also be allowed to opt out of the Smart Grid, perhaps in exchange for higher electricity rates, perhaps for a set fee. Only then would PIPEDA truly apply to the Smart Grid, as it should.

This report opened with a quotation from *Plant* a twenty-seven year old Supreme Court case. In 2010 the Court had the opportunity to revisit the privacy implications of electricity readings, and specifically, of smart meters, in the *Gomboc* case mentioned above. Justice Deschamps, writing for the majority,[39] wrote:

> … [S]ubmissions about smart meters raise concerns about theoretical capabilities and potential future uses of technology rather than realistic privacy concerns applicable in the present case…

[37] The Smart Grid received some mention in Assistant Commissioner Bernier's speeches as listed on the OPC website. http://www.priv.gc.ca

[38] See for example the utility PG & E operating in Northern California. Somewhat ironically, health and environmental concerns drove the option more than privacy concerns. http://www.pge.com/about/newsroom/newsreleases/20110324/pgampe_proposes_smartmeter_option.shtml

[39] The majority dismissed the appeal but was divided into two factions as to the basis of dismissal, for reasons that do not touch upon the argument here.

> I would… leave the privacy implications of the more evolved technology to be decided when a comprehensive evidentiary record has been developed.[40]

It is hoped that this report has made a modest contribution to the development of said evidentiary record, and that the report and its recommendations will contribute to the protection of privacy as well.

Recommendations for OPC

OPC should clearly communicate to utilities and the public that personal information issues related to the Smart Grid are subject to PIPEDA.

OPC should reach agreements with its provincial counterparts that will clarify respective jurisdiction on Smart Grid issues.

OPC should serve as a resource on Smart Grid issues for utilities and customers.

OPC should clarify the privacy implications of operational data generated by the Smart Grid.

OPC should ensure that the privacy policies of utilities are updated and refer to the Smart Grid and its implications.

OPC should ensure that utilities interact with Smart Appliances according to PIPEDA.

OPC should engage Ontario and other provinces to ensure Smart Grid initiatives are in compliance with PIPEDA in offering individuals choice and control over the collection of their personal information.

[40] *Gomboc* at ¶ 40.