Consumer Adoption Challenges To The Smart Grid

Anu Gupta, University of New Brunswick, Canada

ABSTRACT

The smart grid represents the next significant evolution of the power infrastructure with many enhancements and challenges. This paper provides a qualitative review of the key consumer adoption challenges of the smart grid. This literature review takes disparate pieces of work and identifies strategic research focal areas. Through existing research and media documents, it identifies the primary consumer adoption challenges as privacy, Radio Frequency (RF) safety, and power rate increases. It also provides a review of each adoption challenge. The review is applied to the Canadian perspective drawing from smart grid experiences across North America. The review demonstrates that each of the challenge areas has a negative impact on the adoption and support of the smart grid.

This paper recommends further in-depth research be conducted in the following areas: testing each of the consumer adoption challenges—privacy, RF Safety, and rate increases—separately with quantitative measures; testing the willingness to accept a power infrastructure with the security and stability level of a bank; and testing the impact that proactively educating the public would have on the smart grid adoption.

Keywords: Smart Grid; Power Infrastructure; Consumer Challenges; Privacy; Radio Frequency (RF) Safety; Power Rates; Dynamic Pricing; Time-Of-Use; Renewable Energy

INTRODUCTION

This paper will focus on the adoption challenges faced by the smart grid, specifically consumer challenges. It will ask the question, 'How significant are the consumer adoption challenges to the smart grid?' This question was addressed through a review of the existing research and media materials. This literature review takes disparate pieces of work and identifies strategic research focal areas. The review will provide a foundational understanding of each identified challenge area and is applied to the Canadian perspective drawing from smart grid experiences across North America. The paper will also give a brief overview of the smart grid in order to place the consumer challenges in context. Finally, the paper will close with a discussion of the findings, results, and recommendations.

OVERVIEW

The smart grid represents the next significant evolution of the North American power infrastructure. It has the potential to bring great benefits, but also presents many challenges. The concept of the smart grid is to make the power infrastructure more intelligent by providing new capabilities such as real-time usage and rate information to utilities and consumers (Larsen, 2009). This will require enhancements throughout the system, including the home, the power lines, generation points, and utility control centres (Larsen, 2009). The potential benefits are vast: from automatic fault detection and resolution to integration of distributed generation such as renewables, consumer energy usage knowledge, cost savings and energy conservation (Canadian Electricity Association [CEA], 2010). Currently, trials and limited deployment are occurring across North America (CEA, 2010).

To enable the smart grid, homes will require a smart meter unit installed to replace the current electricity meter (Larsen, 2009). The smart meter will be a highly intelligent device with the ability to provide real-time rate information, track energy usage, and send information to a database (Freiling & Jawurek, 2011). Ultimately, it will be able to signal large appliances in the home to turn them on or off on a real-time basis (McNeil, 2011). This unit will provide real-time information to both the utility and the consumer to allow energy usage optimization. It will create a vast repository of very specific information on each consumer's energy usage patterns that did not exist in the past. Furthermore, an IT network parallel to the power infrastructure will be required to send control, signaling, rate, and energy usage information in both directions (Larsen, 2009).

SMART GRID CHALLENGES

Many consumer challenges exist for the successful deployment of the smart grid or smart meter-based services. There is a strong position countering the value of the smart grid. Several groups representing consumers, politicians, academics and industry experts have begun to speak out against the smart grid. They have outlined the risks, challenges, and dangers the smart grid presents. To understand the significance of the consumer challenges and their impact on the smart grid, the challenges must first be understood. The primary challenges include privacy issues, Radio Frequency (RF) safety, and potential rate increases (Wamsted, 2012). Stakeholders such as consumers, utilities, regulatory bodies, and manufacturers have differing viewpoints about these challenges. Each one of these challenges is presented through a review of leading research and current activities as identified in the media.

Privacy

The privacy issue has been raised by many consumer advocates (Cavoukian, Polonetsky, & Wolf, 2010; Freiling & Jawurek, 2011) and the International Energy Agency (Heffner, 2011) as one of the most significant concerns in the deployment of the smart grid. The smart meter conceptually will allow both the consumer and utility to see electrical load fluctuations at a discrete level, potentially down to fifteen minute intervals (McNeil, 2011). In essence, the smart grid will have the ability to track and capture detailed electricity usage in each home. Over a period of several months, the utility would have enough information to develop a very specific profile of the consumer, identifying personal habits such as cleaning, cooking, sleeping, or absence from the home. In addition, it is not clear who will own this information, the consumer or the utility, and who will have ultimate rights over it. It would be very valuable in the hands of marketing firms or criminals.

Privacy leaders have expressed concerns about utilities knowing when people cook, shower or sleep (Cavoukian et al., 2010). For instance, consumers who are profiled as high users of their dryers and dishwashers may be targeted by certain businesses. In another scenario, customers who demonstrate regular intervals of low usage, implying their home is not occupied, could be targeted for theft. However, Cavoukian et al. (2010) do not believe the development of the smart grid should stop or slow down due to these risks. Rather, they believe the smart grid initiative should proceed, but privacy must be a key part of the design from the beginning (Cavoukian et al., 2010). Many utilities are focused on the testing and piloting of smart grid technologies before developing consumer protection practices. To address privacy challenges and protect the consumer, Cavoukian et al. (2010) have developed several basic principles to put 'Privacy by Design' into operation and support smart grid initiatives (Cavoukian et al., 2010). These include: proactive embedding of privacy requirements into designs, ensuring that privacy is the default, making privacy a core function, avoiding making unnecessary trade-offs between privacy and legitimate objectives, ensuring privacy is end-to-end, and designing systems with respect for consumer privacy (Cavoukian et al., 2010). They believe these principles are fundamental to the development and success of any smart grid deployment and, in the interests of consumer protection, must be integrated from the start, not after deployment.

Privacy concerns also lead to the question of who owns, protects, and develops appropriate use policy on the vast amount of detailed consumer energy usage data that will come into existence. Advocacy groups believe it will be critical that data protection and ownership be resolved before consumers become large scale supporters of the smart grid (Cavoukian et al., 2010). The utility has been trusted to protect high level customer usage and billing information. It can, however, be argued that this information has not been viewed as an asset internally by the utility, or externally by marketing firms and, potentially, criminals. As more utilities become private, this information may come to be seen as a revenue-generating asset which can be sold. Such a violation of the established trust would severely damage the consumer/utility relationship that exists today.

Current billing and power information resides in an isolated database and is aggregated manually through site visits and meter readings by utility personnel. In the smart grid model, the power usage and appliance control information would be sent back via the power grid itself, a parallel network, or the Internet (Blasco, 2009). This infrastructure would look similar to IT networks which employ the TCP/IP protocol (Blasco, 2009). TCP/IP is the foundation of the Internet and of private corporate networks that have been successfully attacked (Laudon & Traver, 2012). For instance, the Canadian government was successfully attacked for information regarding the PotashCorp takeover (Weston, 2011). Although a proprietary communications technology could be developed, smart grid designers believe the TCP/IP protocol provides the greatest potential for integrating existing technologies (Blasco, 2009). However, it also increases the potential for hacking into the smart grid electricity infrastructure, placing consumer privacy at risk and significantly jeopardizing the established customer trust.

The Canadian government has very high standards for security, demonstrating that highly 'secure' IT networks, when targeted by professionals, can be penetrated. These successful attacks give credence to security concerns about the power infrastructure employing a TCP/IP network with signaling and control capabilities. The traditional power infrastructure was inherently secure, as it did not carry communications or TCP/IP capabilities. With the implementation of the smart grid, the risk of hackers controlling power and accessing consumer information would rise significantly. The addition of bi-directional communication provides many new features, but also presents increased risks of the kind already experienced by private IT networks. As outlined in the existing research (Cavoukian et al., 2010; McNeil, 2011; Freiling & Jawurek, 2011), the significance of privacy as a consumer adoption challenge is material.

RF Safety

Another key concern raised by consumer groups is the safety impact of the RF signals transmitted by the smart meter to communicate with the equipment on the pole (Wamsted, 2012). In North America, smart grid initiatives primarily require the development of a communications infrastructure or network parallel to the power grid (Larsen, 2009). Many of these parallel networks have employed wireless communications from the home to the pole through a RF technology. There are several RF technologies under consideration, from wi-fi and Z-Wave to ZigBee (Mulligan, 2011). ZigBee is emerging as the predominant choice; this RF technology functions in the ISM frequency of 915MHz in North America and provides a secure wireless mesh network (Swirbul, 2011). The utilities have chosen this technology over a physical infrastructure as it is low cost, quick to deploy, and can be secured (Swirbul, 2011). In addition, it meets several technical requirements, including speed, security, and IP support (Mulligan, 2011). The ZigBee Alliance is setting standards to allow In-Home Devices (IHD) to directly connect via ZigBee, potentially placing RF devices in the home (Fodor, 2011). Regardless of the final RF standard, there is a definite preference on the part of utilities for RF-based connections over hard-line wired interfaces.

The RF tie to smart meters has created a significant backlash against forcing wireless signals into homes, especially in California (Wamsted, 2012). The resistance is based on safety concerns associated with RF signals being broadcast throughout the day in the home. RF signals can be strong enough to be harmful and can, in essence, cook human tissue. The Health Canada Safety Code 6 recommends the whole body average specific absorption rate be no greater than 0.4 watts per kilogram of human tissue in controlled environments (Health Canada, 2009). It is expected that equipment manufacturers and utilities will be required to comply with this code through regulatory bodies and their associated inspections. However, the question of long term low levels of exposure remains unanswered. The Health Canada Safety Code 6 states the following:

Proposed effects from RF energy exposures in the frequency range between 100 kHz and 300 GHz, at levels below the threshold to produce thermal effects, have been reviewed. At present, these effects have not been scientifically established, nor are their implications for human health sufficiently well understood. (Health Canada, 2009)

In essence, Health Canada states it does not know the health impact of long term low level transmissions as the science has not been established. This leaves the assessment of RF safety to the consumer. If left unresolved, this concern has the potential ability to slow down or even shut down RF-based smart grid initiatives. The RF concern is so powerful that it is fueling anger and action; in British Columbia (BC), several grassroot groups have formed to stop smart meter deployment, with thousands of people engaged (Brown & Petrovich, 2011). BC Hydro's position states the RF smart meters have less impact than a 30-minute cell phone call over a twenty-year span and that there are no demonstrable health or environmental effects from exposure to low level radio frequency signals (BC Hydro, n.d.). However, Health Canada indicates the long-term low level effects are unknown, thus contradicting BC Hydro (Health Canada, 2009).

Interestingly, the ZigBee frequency is in the same frequency range as cordless phones, microwaves, and wireless Internet devices. Furthermore, cell phones and microwaves both generate more RF signals than smart meters (Wamsted, 2012), as depicted in Table 1. These wireless consumer devices are now positively received and widely deployed. In fact, many Internet Service Providers (ISPs) bundle wireless RF units with their Internet service, which broadcasts twenty-four hours a day throughout the home without consumer backlash.

Table 1: RF Power Density Levels of Common Devices

RF Power Density Levels of Common Devices

	Minumum	Maximum
Microwatts per centimeter squared		
Cell Phone (at ear)	1000	5000
Microwave Oven (2 feet)	50	200
Smart Meter (3 feet)	40	40
Smart Meter (10 feet)	4	4
WiFi Router (3 feet)	0.2	1
FM Radio/TV Broadcast	0.005	1
After (Source: Wamsted, 2012)		

The primary difference is choice. Consumers choose each of these RF devices, but often not RF smart meters. Where they are forced to change over to RF-based smart meters, there has been resistance, as seen in the case of British Columbia. The RF safety concern is negatively impacting support for the smart grid.

Rate Increases

There is a belief within consumer advocacy organizations that the smart grid will drive rate increases and negatively impact the vulnerable in society (Wamsted, 2012). This view stems from the increased utility costs to purchase and deploy smart meters and the time-of-use rates being implemented in correlation with smart meters. The significance of this is material to adoption and support of the smart grid. The following two sections provide the details behind this position.

Increased Utility Costs

There are many incremental costs with the smart grid, from new infrastructure to deployment and management. According to the Canadian Electricity Association, a non-profit organization consisting of the Canadian power utilities and related industry providers, Canada needs to invest $293.8 billion CDN between 2010 and 2030 in the grid (Conference Board of Canada, 2011). This is in order to satisfy the current infrastructure demands and support future growth. Of the $293.8 billion CDN, $35.8 billion CDN would be for the power grid's transmission infrastructure, $62.3 billion CDN for the distribution infrastructure, and the remaining $195.7 billion CDN for power generation (Conference Board of Canada, 2011). In the US, the estimate to deploy the smart grid alone is $165 billion US over the next twenty years (Jaffe, 2010). The challenge that the utilities face is that a large percentage of these costs will go towards maintaining the current grid regardless of the smart grid initiative. Some costs are directly associated with the smart grid; for instance, the smart meter unit costs from $300 to $500 US per consumer (Fox-Penner, 2010). Both the infrastructure and additional smart grid costs will need to be recovered. The utilities have a long term time horizon and deprecation model spanning twenty years, which allows the impact on consumers to be minimized (Fox-Penner, Faruqui, & Grasso, 2011). However, this is not common knowledge or information that is shared with the consumer, thus feeding the consumer belief that rates would increase. Regardless of smart grid initiatives, power rates are increasing due to aging infrastructure, new planned power plants, and incentive-based renewable energy feed-in tariffs (Dubinsky, 2011). These increases in power costs diminish the smart grid value proposition. In fact, in November 2011, the Ontario Energy Board changed the power rates for Ontario consumers with flat rate increases of between 1.0% and 1.6%, as well as time-of-use rate increases from

0.9% to 2.1% (Toronto Hydro, n.d.). The increases are more significant for those on smart meters. The average smart meter user, consuming 1000 Kwh/month, will see an increase of $2.70 CDN, while non-smart meter users will see a decrease of $1.25 CDN (Toronto Hydro, n.d.). The Ontario Energy Board has explained that increased reliance on nuclear and renewable energies is behind the rise in rates. In fact, Ontario has the most generous renewable feed-in tarriff in North America, at 80.2 cents/Kwh CDN (Ontario Power Authority, 2010). However, the Ontario Power Authority has not explained why smart meter users will pay more than non-smart meter users.

Dynamic Pricing (Time-of-Use)

The dynamic pricing concept implies that the rates may fluctuate throughout the day based on peak demand and generation capacity. For instance, the rates may drop in the evening or at night when demand has fallen. They may drop when there is greater wind capacity and excess power generated. Ideally, the utility would deploy smart meters with demand-response capability, implying the utility would turn on the customer's dryer or dishwasher or increase/decrease the air conditioning or heating to automate the optimization of power rates. In reality, this presents several challenges to consumers. How do they know when the optimal rates are? How do they take advantage of them? Can they control when they need additional heat or A/C? If they cannot, what does this do to their power bill? The smart meter In-Home Devices (IHD) would tell consumers when the optimal rates are, but this does not necessarily enable consumers to take advantage of these rates. The demand response concept would allow utilities to control large, power-intensive appliances to assist in the optimization of power usage. For instance, consumers would simply load their dryers or dishwashers and go to sleep; as the power rates drop, the appliance would be automatically run, and thus the cost to the consumer would be reduced. Integrating and automating appliances to low power rates, however, does not address the challenge of tying weather and power rates. In an ideal scenario, the temperature drops at night, the heating is turned up, and this coincides with a drop in the power rates.

The opposite scenario, where the temperature drops and the rates increase, can create a situation where the consumer has no choice but to purchase power at premium rates. This was a contributor to the California energy crisis at the turn of the century. Californians experienced the 'perfect storm' that led to rolling blackouts, large utility bankruptcies, and ultimately burdened the government with significant debt (PBS, n.d.). California had deregulated the wholesale market (PBS, n.d.), was in an economic boom, and energy supply was short due to the lowest run-off of the Columbia River since 1929 (Columbia River History, n.d.). California had frozen consumer rates to allow utilities to recover past investments in a transition period. The expectation was that once these investments were recovered the rates would drop to competitive rates seen in nearby states. However, when the rates were unfrozen, they doubled instead of dropping (Borenstein & Bushnell, 2000). These contributing factors in the deregulated market yielded the worst case scenario for the consumer. It is the memory of these situations that has created further concern regarding the smart grid and associated price variations.

There are many different models for dynamic pricing. These include real-time pricing (RTP), time-of-use (TOU), critical peak period (CPP), peak time rebates (PTR), and variable peak pricing (VPP) (Faruqui & Palmer, 2011). Time-of-use rates are the simplest of the dynamic pricing models; they are for fixed intervals and are often set a year in advance (Faruqui & Palmer, 2011). However, time-of-use rates bring challenges with them. Consumer advocates are most concerned about the vulnerable, such as the poor, disabled, or pensioners, who may not have the flexibility to run energy intensive appliances such as dryers or dishwashers at night (Heffner, 2011). The smart grid would provide savings to the wealthy but would drive up rates for the vulnerable sector. Residential customers who support time-of-use rate models tend to be higher-income with larger homes who believe they can realize savings (Makovich, 2011).

DISCUSSION AND RECOMMENDATIONS

The literature review and media documents demonstrate that each of the three key smart grid consumer adoption challenges are prevalent in certain locations and societies. As detailed earlier, they are privacy, RF safety, and rate increases.

Smart grid privacy literature has demonstrated that the ability to develop detailed usage profiles will be part of the smart grid (Cavoukian et al., 2010; Freiling & Jawurek, 2011; McNeill, 2011). The usage and protection of this information has not been formally defined, understood or legislated. In addition, there is limited research regarding consumer privacy and the smart grid. The existing research focuses specifically on consumer privacy and the smart grid and often cites the work of Cavoukian et al. (2010). Their research indicates that the following is required to ensure smart grid consumer privacy; 'Privacy by Design'; law, regulation and independent oversight; accountability and transparency; market forces, education and awareness; audit and control; data security; and fair information practices (Cavoukian et al., 2010). These are still very high level concepts that require further in-depth analysis, research and definition. However, they provide the framework upon which smart grid consumer privacy can be built.

Furthermore, it has been identified that the smart grid, by employing TCP/IP, will become a greater target for attacks similar to those experienced by corporate IT networks. However, these same IT networks currently protect credit cards, bank accounts, taxation, and personal information (Laudon & Traver, 2012). Society has accepted the existing level of security along with inherent weaknesses in data protection. Will society accept the power infrastructure at the same level of security? The highest existing level of IT security standards, policies, and systems is employed by corporations such as banks. The utilities may consider employing the existing security framework implemented by similar high target IT networks. Further research needs to explore society's willingness to accept a power infrastructure with the same security/stability level of a bank.

The second key challenge for adoption of the smart grid, RF safety, has proven to be a serious one for utilities, as can be seen by the kind of public demonstrations experienced in California and BC. Utilities may need to offer choice to those who do not want RF devices within their home. The State of Maine Public Utilities Commission decided in May 2011 to require power companies to offer a choice to 'opt out' of smart meters (Wamsted, 2012). However, utilities are resistant to this option since the realization of the smart grid's benefits requires mass penetration and the capabilities of the smart meter. There are smart meter options that do not include RF technologies, such as hard-wired telecom lines or Internet-based connections. These non-RF options may drive up costs in the short term; they may also build support and resolve a significant consumer concern. Further research may help understand the return-on-investment (ROI) on these access options in terms of adoption rate vs. increased access costs.

The final primary consumer challenge or resistance to the smart grid is associated with the belief that rates will increase with the deployment of the smart grid. There is no doubt that additional infrastructure costs will need to be recovered, possibly over several decades. In the case of Ontario rates increased for those employing time-of-use rates with a smart meter vs. those on flat rates. The concern regarding vulnerable consumers may be a valid one. One possible method to protect them is to develop a policy that offers everyone the first 1000 Kwh per month, the average consumption per month in Ontario (CNW, 2008), at the flat-rate, then shifts to time-of-use. This protects the vulnerable and allows the heavy energy users to develop time-of-use practices to reduce costs and consumption. The ability to provide this advanced tier of pricing is one of the advantages the smart grid technology provides. Another way to garner consumer support is to provide 'shadow bills', which show what consumers' bills would be in a dynamic pricing model in comparison to current flat rate bills, demonstrating the potential savings. Both of these concepts—the first 1000Kwh at a flat rate and shadow bills—merit further research in support of policy that will address this challenge.

This review combined fragmented and disconnected components including publications and media documents to provide a manageable integrated review applied to smart grid consumer adoption challenges. This provides direction towards future research that can yield tangible and impacting outcomes. It provided a qualitative understanding of the impacts of the consumer challenges of the smart grid. It further demonstrated that these challenges have a negative impact on the adoption of the smart grid. The review, however, did not identify the magnitude of the impact or provide a quantitative analysis.

Further research is required in the following areas:

- test each of the consumer adoption challenges—privacy, RF Safety, and rate increases—separately with quantitative measures
- test the willingness to accept a power infrastructure with the security/stability level of a bank

- test the impact that proactively educating the public would have on smart grid adoption

The smart grid is a relatively young concept; there is limited published research in the field. To perform this research, it is further suggested that it be conducted in several stages. First, a small pilot should be conducted through interviews with a basic survey to establish the optimal tools, research methodology, and sample specific to each adoption challenge. For instance, testing the RF safety challenge implies a base level of knowledge of RF before one can ask the question regarding RF safety. The pilot will help establish the tools and specific questions, research method, and knowledge base of the sample. This will provide guidance if education is required regarding RF before performing the survey and any potential bias that may be introduced. Similarly, as part of the first step, independent pilots would be conducted for the two other adoption challenges. Dependent upon the outcome of the pilot, a second step may be to conduct a larger scale formalized survey utilizing the tools from the survey with further refinement. The outcome of the research in the consumer adoption challenges with quantitative measures would allow the utilities and policy makers to employ the research to make policy decisions.

Testing the willingness of consumers to accept the security and stability of a bank in the power infrastructure would begin with a refined literature review and drawing from related fields. Significant research has been conducted in the area of security from many perspectives. This research should be reviewed for applicability to the power infrastructure. In addition, opportunity exists to draw on parallel industries such as e-Commerce that have had to introduce the concept of security.

Finally researching the impact of proactively educating consumers would provide guidance towards future investments and the type of education to be provided by utilities and government bodies. The first step in this area of research would be to draw on existing research and publications. Furthermore, researchers could again draw on similar industries such as e-Commerce that converted the public from fear of online purchases to a wide based acceptance (Laudon & Traver, 2012).

Through detailed research of each challenge area, it would be possible to further map the significance level into quantitative models in order to understand more clearly the magnitude of the impact. This additional research would support policy to protect the consumer and enhance the smart grid. It would also allow utilities to prioritize these challenges and develop solutions.

AUTHOR INFORMATION

Anu Gupta, P.Eng, MBA has twenty years of experience in engineering and marketing fields in the public and private sector. He has guided many projects in the areas of systems development, IT infrastructure, and network management. He has taught for fourteen years at the University of New Brunswick in the areas of IS, IT, and renewable energies. He holds an undergraduate degree in Electrical Engineering and a Masters in Business. He researches, lectures, and writes in the field of the smart grid. He is currently pursuing his doctorate in the field of smart grid adoption. E-mail: anu.gupta@live.ca

REFERENCES

1. BC Hydro (n.d.). Radio frequency & smart meters. *BC Hydro*. Retrieved June 17, 2012 from http://www.bchydro.com/energy_in_bc/projects/smart_metering_infrastructure_program/faqs/radio_frequency.html
2. Blasco, J. (2009). IP-based standards support future smart grid. *POWERGRID International, 14*(10), 60.
3. Borenstein, S., & Bushnell, J. (2000, August 27). In the dark California consumers haven't seen benefits of deregulating the electrical industry – what went wrong? *San Jose Mercury News*. Retrieved June 24, 2012 from http://www.ucei.berkeley.edu/ucei/Recent_Presentations/sjmerc.pdf
4. Brown, C., & Petrovich, C., (2011, Dec 22). Smart meters ignite fierce debate in B.C. *Canadian Broadcasting Corporation.* Retrieved June 17, 2012 from http://www.cbc.ca/news/canada/british-columbia/story/2011/12/22/bc-smart-meters.html?cmp=rss

5. Canadian Electricity Association. (2010). The smart grid: a pragmatic approach, A 'state-of-play' discussion paper presented by the Canadian Electricity Association. Retrieved June 24, 2012 from http://www.electricity.ca/media/SmartGrid/SmartGridpaperEN.pdf
6. Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). Smart privacy for the smart grid: embedding privacy into the design of electricity conservation. 3, 275–294. doi: 10.1007/s12394-010-0046-y.
7. CNW. (2008, May 28). Save the watt Wednesday. *Canada Newswire*. Retrieved June 24, 2012 from http://www.newswire.ca/en/story/278939/save-the-watt-wednesday
8. Columbia River History (n.d.). Energy crisis of 2000/2001. Retrieved June 24, 2012 from http://www.nwcouncil.org/history/EnergyCrisis.asp
9. Dubinsky, Z. (2011, March 30). Electric shocker: Power prices set to rise sharply. *Canadian Broadcasting Corporation.* Retrieved June 17, 2012 from http://www.cbc.ca/news/canada/story/2011/03/13/f-power-2020-rising-electricity-costs.html
10. Faruqui, A., & Palmer, J. (2011). Dynamic Pricing and Its Discontents. *Regulation, 34*(3), 16-22.
11. Freiling, F., & Jawurek, M. (2011). Privacy threat analysis of smart metering. In Gesellschaft für Informatik, Lecture Notes in Informatics (LNI) - Proceedings, 192.
12. Fodor, E. (2011). Enhancing smart grid awareness with mobile technologies. *ECN: Electronic Component News*, *55*S4.
13. Fox-Penner, P. (2010, October 4). The smart meter backslide. *Harvard Business Review*. Retrieved June 17, 2012 from http://blogs.hbr.org/cs/2010/10/the_smart_meter_backslide.html
14. Fox-Penner, P., Faruqui, A., & Grasso, D. (2011). Moving to the smart grid. *Issues In Science Technology, 27*(4), 12-16.
15. Health Canada. (2009). Limits of Human Exposure to Radiofrequency Electromagnetic Energy in the Frequency Range from 3 kHz to 300 GHz. Safety Code 6 – August 2009.
16. Heffner, G. (2011). Smart grid – smart customer policy needs. Retrieved November 11, 2012 from http://www.iea.org/papers/2011/sg_cust_pol.pdf
17. Jaffe, M. (2010, Feb 14). Cost of smart-grid projects shocks consumer advocates. *The Denver Post.* Retrieved June 17, 2012 from http://www.denverpost.com/business/ci_14394848
18. Larsen, K. (2009). Smart grids – a smart idea? *Renewable Energy Focus. 9.*
19. Laudon, K., & Traver, C. (2012). *E-commerce: business, technology, society* (8^{th} ed.). Upper Saddle River, NJ: Pearson Education.
20. Makovich, L. J. (2011). The smart grid separating perception from reality. *Issues In Science & Technology, 27*(3), 61-70.
21. McKenna, E., Richardson, I., & Thomson, M. (2012). Smart meter data: balancing consumer privacy concerns with legitimate applications. *Energy Policy, 41(1)*, 807-814.
22. McNeil, S. (2011). Privacy and the modern grid. *Harvard Journal of Law & Technology. 25(1).*
23. Mulligan, G. (2011). The smart grid is coming…The smart grid is coming. *Appliance Design, 59*(6), 31-34.
24. Ontario Power Authority. (2010). Micro feed-In Tarriff program. Retrieved November 11, 2011 from http://microfit.powerauthority.on.ca/pdf/microFIT-Program-Overview.pdf
25. PBS. (n.d.). The California crisis. Retrieved June 24, 2012 from http://www.pbs.org/wgbh/pages/frontline/shows/blackout/california/
26. Swirbul, C. (2011). Smart grid communications: Strategies are forming to help sort through the exploding number of technology options, but one size won't fit all. *Transmission & Distribution World, 63*(4), 8-13.
27. Toronto Hydro (n.d.). Residential rates FAQs. Retrieved June 17, 2012 from http://www.torontohydro.com/sites/electricsystem/residential/yourbilloverview/Pages/ResidentialRatesFAQ.aspx
28. Weston, G., (2011, Nov 29). Foreign hackers targeted Canadian firms. *Canadian Broadcasting Corporation.* Retrieved June 17, 2012 from http://www.cbc.ca/news/business/story/2011/11/29/pol-weston-hacking-firms.html
29. Wamsted, D. J. (2012). Clarity for customers. *Electric Perspectives, 37*(2), 22-36.