

SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation



November 2009

THE FUTURE OF PRIVACY FORUM
WWW.FUTUREOFPRIVACY.ORG



Information and Privacy Commissioner,
Ontario, Canada

Acknowledgements

The authors of this paper gratefully acknowledge the work of Catherine Thompson, Regulatory and Policy Advisor at the Ontario Information and Privacy Commissioner's Office, and Matthew Gruenberg, Smart Grid Policy Fellow at the Future of Privacy Forum, in preparing this report.



**Information and Privacy Commissioner,
Ontario, Canada**

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

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

Table of Contents

Foreword.....	1
I Introduction.....	3
II What is the Smart Grid?	4
III SmartPrivacy for the Smart Grid	12
IV Conclusion	18
Appendix A – 7 Privacy by Design Foundational Principles.....	18
Appendix B – Smart Grid Components	21
About the Authors.....	22

Foreword

Recognizing that a multiplicity of forces act upon an organization's ability to protect its customer's data or subject's privacy, I developed the term *SmartPrivacy* to describe the holistic approach necessary to realizing the objective of all encompassing data protection.

SmartPrivacy represents a broad arsenal of protections, encapsulating everything necessary to ensure that all of the personal information held by an organization is appropriately managed. These include: *Privacy by Design*; law, regulation and independent oversight; accountability and transparency; market forces; education and awareness; social norms; data security; and fair information practices. Each of these elements is important, but my concept of *Privacy by Design* represents its sine qua non. Those who fail to envision privacy requirements early in the development of technology, business practices or physical space and infrastructure will be less likely to provide comprehensive protection, despite the presence of the other elements.

Privacy by Design or *PbD* is a concept I developed in the '90s. Building on the elements discussed, it ensures the protection of privacy through the use of privacy-enhancing technologies — embedding them into the design specifications of information technology, business practices, physical environments and infrastructure — making privacy the default. Recently, I evolved the concept of PETs, extending it to PETs *Plus* by adding a new dimension of a positive-sum (win-win) paradigm to replace the traditional zero-sum approach. Building on PETs *Plus* we advance the view that it is not necessary to trade off privacy against equally important goals such as security, transparency or other functionality.

The objectives of *Privacy by Design* — ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the seven foundational principles outlined in Appendix A.

I am pleased to have collaborated with the Future of Privacy Forum in preparing this report. The Future of Privacy Forum is a think-tank made up of Chief Privacy Officers, privacy advocates, and academics interested in promoting responsible data practices. We believe that taking a *Privacy by Design* approach to the Smart Grid will benefit from cross-industry and cross-discipline co-operation.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

I Introduction

The current electrical grid is seen by some as the greatest engineering achievement of the 20th century, and is considered to be the largest machine on the planet. However, it is increasingly out of date and overburdened, leading to costly blackouts and brownouts. For example, the 2003 blackout in the northern and eastern U.S. and Canada caused a \$6 billion loss in economic revenue.¹ Utility providers struggle to monitor the grid's performance, and in many areas, they depend on customers to report power outages. This is because the grid was designed to meet one main goal — to ensure that the lights kept glowing — before much of the technology that depends on it existed. It was not originally designed to incorporate other goals such as energy efficiency, reduced environmental impacts, incorporating alternative energy sources, allowing for more consumer choice, and robust cyber security.

Modernization efforts are underway to make the current electrical grid “smarter.” The infrastructure that will support the future Smart Grid will be capable of informing consumers of their day-to-day energy use, even at the appliance level. While this is beneficial and supports valuable efforts to curb greenhouse gas emissions and reduce consumers' energy bills, it introduces the possibility of collecting detailed information on individual energy consumption use and patterns within the most private of places — our homes. We must take great care not to sacrifice consumer privacy amidst an atmosphere of unbridled enthusiasm for electricity reform. Information proliferation, lax controls and insufficient oversight of this information could lead to unprecedented invasions of consumer privacy. We recognize the value of the information on the grid, which will give consumers more control over their electricity usage and give utilities the ability to manage demand requirements, but the dissemination of data must be done in a trustworthy and transparent manner.

Customers' relationships with power utilities are generally borne out of necessity — unless an individual can generate their own power, they must either obtain power from a utility or go without it. The expectation, however, is that the utility will supply electricity only, and not to monitor customers' behaviours and activities. Much in the same way that we do not expect the postman to look inside our windows when he is delivering the mail, or the cable person to monitor the TV shows we watch after he has completed the cable installation, so too do customers not expect there to be any surreptitious profiling of their in-home energy-related behavioural patterns.

Utility regulators have an important role in setting best practices for electricity generation and distribution, such as the National Association of Regulatory Utility Commissioners' resolution passed in 2000 on the privacy of utility customer information.² As the Smart Grid develops and the nature of information exchanges on it become clearer, utility regulators can look to the insights gained in other areas where technology has prompted a privacy debate and can learn from their successes and mistakes.

-
1. U.S. Department of Energy, “The Smart Grid: An Introduction” (Prepared by Litos Strategic Communication, 2008), pp. 8.
 2. NARUC, “Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information” (2000): http://www.naruc.org/Resolutions/privacy_principles.pdf accessed November 10, 2009.

This paper will introduce the reader to the Smart Grid and its benefits, as well as the questions that should be explored regarding privacy. SmartPrivacy will also be explained and applied to the Smart Grid scenario. Now is the time to *bake privacy into* the Smart Grid, while it is in its nascent stages.

II What is the Smart Grid?

“Smart Grid” refers to the modernization of the current electrical grid so that there is bi-directional flow of information and electricity in order to achieve the following goals: provide consumers with more choices on how, when, and how much electricity they use; self-heal in case of disturbances, physical and cyber attacks, and natural disasters; link with a wide array of energy sources, in addition to energy produced by power plants, such as renewable energy producers; provide better power quality, and more efficient delivery of electricity. Communications technology and infrastructure is at the heart of improvements to the electrical grid, which will collate data provided by smart meters, sensors, computer systems, and many other devices into understandable and actionable information for consumers and utilities.³ The overall vision for the Smart Grid is that it will possess the following qualities:⁴

- **Intelligent** – capable of sensing system overloads and rerouting power to prevent or minimize a potential outage; of working autonomously when conditions require resolution faster than humans can respond and cooperatively in aligning the goals of utilities, consumers and regulators
- **Efficient** – capable of meeting increased consumer demand without adding infrastructure
- **Accommodating** – accepting energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas; capable of integrating any and all better ideas and technologies – energy storage technologies, for example – as they are market-proven and ready to come online
- **Motivating** – enabling real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns
- **Opportunistic** – creating new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate

3. See “Building the energy internet,” *The Economist* (May 11, 2004), and “Building the smart grid,” *The Economist* (June 4, 2009). Choices regarding communications improvements “will rely on a variety of technologies including cellular spectrum, fiber optics, power line carrier (including broadband over power line), microwave, radio (licensed and unlicensed), WiMax, WiFi and others.” Ontario Smart Grid Forum, “Enabling Tomorrow’s Electricity System” (February 2009) 34: <http://www.ieso.ca/smartgridreport/> accessed November 10, 2009. “Broadband over power line” or BPL, would help utilities monitor and manage various elements of their electric power distribution operations, and may provide broadband internet access over electrical lines, helping to provide broadband internet access to rural areas. See for example, Federal Communications Commission, Memorandum and Opinion, FCC 06-113 (August 7, 2006).

4. *ibid.*, *The Smart Grid: An Introduction*, pp. 17.

- **Quality-focused** – capable of delivering the power quality necessary – free of sags, spikes, disturbances and interruptions – to power our increasingly digital economy and the data centers, computers and electronics necessary to make it run
- **Resilient** – increasingly resistant to attack and natural disasters as it becomes more decentralized and reinforced with Smart Grid security protocols
- **“Green”** – slowing the advance of global climate change and offering a genuine path toward significant environmental improvement.

Smart Grid technologies are expected to produce valuable cost and energy efficiencies all along the electrical distribution system. One of the first and most important will be to meet peak energy demand more efficiently and with less detriment to the environment. Since storage of electricity is currently very costly, electricity must be consumed the moment it is created. As a result, estimating the correct amount of demand of electricity is very difficult. Without the benefit of this knowledge, electricity providers must use “peaker plants” when energy demand threatens to exceed supply levels. Peaker plants tend to be older, expensive to bring online, and require fuel to operate, which further creates greenhouse gases.⁵

Additional benefits of the Smart Grid will include: incorporating into the grid cleaner sources of energy; providing consumer control over energy usage and cost; bringing more transparent pricing strategies that can lead to up to five to fifteen per cent in energy consumption reduction; increasing reliability of power supply meaning fewer power outages, and outages that are shorter in length (currently, half a million Americans spend a minimum of two hours without electricity every day); lessening power quality fluctuations; and lowering expenses for grid operators who are better able to use their assets, and more efficiently run the grid.⁶

Consumers are an important focus of grid improvements because they represent almost a quarter of all energy consumed.⁷ So how does the Smart Grid vision relate to identifiable individuals?⁸

5. *ibid.*, *The Smart Grid: An Introduction*, pp. 14. A Lopez-Pacheco, ‘Energy-Wising Up’ *The National Post* (August 29, 2009).

6. Illinois Smart Grid Initiative, ‘Empowering Consumers Through a Modern Electrical Grid’ (April 2009); *ibid.*, *The Smart Grid: An Introduction*.

7. Energy Information Administration, ‘Annual Energy Review’ (2008) pp. 38.

8. *ibid.*, *Ontario Smart Grid Forum*. See also, Ecoalign, ‘A Day in the Life of a Customer in 2015: Visualizing The Smart Grid’ <http://www.ecoalign.com/clients/videos> accessed November 10, 2009, and ‘Socket to me,’ *The Economist* (March 6, 2009).

With Smart Grid technology people will be able to:

Understand how their household uses energy, manage energy use better, and reduce their carbon footprint.

And they will do it by:

- 1) Logging into their energy use account and seeing how much energy they are using in real time, and as compared to their neighbours, as reported by smart meters installed at each household.
- 2) Using smart devices, such as a smart thermostat that shows minute-by-minute price of energy. The thermostat could be programmed to make decisions about the house's heating and air conditioning levels. If the price of energy is high, and no one is home, the thermostat could be set to adjust automatically to use less energy. Smart appliances could also be programmed to run when energy is cheaper, such as a dishwasher running at night.
- 3) At peak energy usage times, allowing the utility to lower energy consumption of smart devices, such as adjusting a house's air conditioner by a few degrees.

Control expenditure on electricity.

- 1) Accessing their account balance, and seeing how many units are being used per day, and which appliances are costing the most money.
- 2) Taking advantage of energy saver plans offered by the utility to keep energy use in line with a person's budget. For example, if a heat wave hits and the price of electricity peaks, the individual could be notified that they may exceed their budget. The individual would then be in control regarding whether the utility could adjust the temperature of the air conditioning a few degrees when peak energy consumption occurs.

Experience fewer and shorter power outages, and to be notified when the power will come back on.

- 1) Having the Smart Grid pinpoint the location of the outage and dispatch workers to the scene immediately. Power will be routed around the outage, so that less individuals are affected by the power outage.
- 2) Signing up to receive alerts when the power goes out via text message to a mobile phone regarding when the power will be back on. Additional messaging services could provide alerts regarding a loved one's energy restoration time.

Control energy devices in the home.

- 1) Tying all energy devices that give energy back to the grid, such as a plug-in hybrid vehicle and solar panels, to a central household control which provides up-to-the-minute indication of energy use.
- 2) Monitoring whether their home is using more energy than it is producing, and adjusting devices so they use less energy. The smart meter tracks this activity, and any surplus in energy shows up as a credit on the person's utility bill.
- 3) Controlling smart devices and account information over the Internet, allowing individuals to monitor and adjust their house's energy usage remotely.

Significant development towards achieving a vision for a Smart Grid is occurring widely in North America and Europe. For example, the U.S. economic stimulus plan included the passing of the *American Recovery and Reinvestment Act of 2009*,⁹ which is allocating billions of dollars to fund improvements to the electrical grid. The Department of Energy has dispersed 3.4 billion in Smart Grid grants which will lead to the rollout of 18 million smart meters, 1 million in-home management systems, and advanced load management devices.¹⁰ In Boulder, Colorado, Xcel Energy has instituted “SmartGridCity”, a joint consortium of eight information technology companies to develop and implement Smart Grid technologies for Boulder’s residents.¹¹ Homes will be outfitted with smart metering devices and each ratepayer will have access to an in-home energy management website, which will monitor energy use and provide information and recommendations for lowering energy use and costs.¹² Xcel Energy has also installed infrastructure that will protect against blackouts and reroute power around electricity bottlenecks.¹³ In Europe, the European Parliament passed the 3rd Energy Package in April 2009 which proposes that 80 per cent of electricity customers have smart meters by 2020.¹⁴

Ontario is pursuing a culture of conservation by encouraging Ontarians to lower their consumption of electricity during peak periods, and to incorporate alternative energy sources such as wind and solar. The Government of Ontario has committed to installing a smart meter in all Ontario homes and small businesses by the end of 2010, and passed legislation to facilitate the program.¹⁵ It is estimated that the cost of grid improvements in Ontario will be approximately \$320 million in the first five years.¹⁶ Several conservation and grid initiatives are already underway. For example, Toronto Hydro has energy saving programs (clothesline giveaway, LED Festive Light Exchanges and CFL rebate), as well as load management programs (Peaksaver and PowerShift). Toronto Hydro also has a Renewable Energy Standard Offer Program where residential customers generate electricity which they sell back to the grid.¹⁷ The Ontario Centres of Excellence have 14 projects relating to Smart Grids with investments at approximately \$12 million.¹⁸

Smart Grid technology is also being supported by significant private investment. Companies are pursuing new products in the area of electric vehicles, smart appliances, and energy production technology, such as solar panels for household roofs, as well as new service offerings in the management of energy capacity, location, time, rate of change and quality. Significant private sector investment is occurring with Smart Grid venture capital, valued at over \$900 million between the years 2000 and 2008.¹⁹ Morgan Stanley estimates that the Smart Grid market will be \$100 billion in 2030.²⁰

9. Pub. L. No. 111-5.

10. K Fehrenbacher, “Smart Grid Stimulus Funding Revealed!” *earth2tech* (October 27, 2009): <http://earth2tech.com/2009/10/27/smart-grid-stimulus-funding-revealed>.

11. Smart Grid City: <http://smartgridcity.xcelenergy.com/index.asp>; “Smart move,” *The Economist* (March 19, 2009).

12. C Proctor, “Xcel launches Boulder as first ‘smart grid’ city,” *Denver Business Journal* (September 8, 2009): <http://denver.bizjournals.com/denver/stories/2009/09/07/daily12.html> accessed November 10, 2009.

13. *ibid.*

14. “EU Energy Package comes into force,” *Metering.com* (September 4, 2009): <http://www.metering.com/node/16015> accessed November 10, 2009.

15. Ontario Smart Meter: <http://www.smartmetersontario.ca>

16. Ontario Smart Grid Forum, “Enabling Tomorrow’s Electricity System” (February 2009) pp. 14.

17. Toronto Hydro: <http://www.torontohydro.com>

18. *ibid.*, *Enabling Tomorrow’s Electricity System* pp. 3.

19. U.S. Department of Energy, “Smart Grid System Report” (July 2009) 25. For example, in 2008 investments were made into: Optimal Technologies International, Inc. (\$25 million); SmartSynch, Inc. (\$20 million); Trilliant Incorporated (\$40 million); Tendril Networks (\$12 million); Fat Spaniel Technologies (\$18 million); GridPoint, Inc. (\$15 million, with total funding over \$100 million); and eMeter Corporation (\$12.5 million).

20. “Wiser wires,” *The Economist* (October 8, 2009).

Personal information and the Smart Grid

“Personal information” refers to any recorded information about an identifiable individual. In addition to one’s name, contact and biographical information, this could include information about individual preferences, transactional history, record of activities or travels, or any information derived from the above, such as a profile or score, and information about others that may be appended to an individual’s file, such as about family, friends, colleagues, etc. In the context of the Smart Grid, the linkage of any personally identifiable information with energy use would render the linked data as personal information.

Modernization of the current electrical grid will involve end-user components and activities that will tend to increase the collection, use and disclosure of personal information by utility providers, as well as, perhaps, third parties. The following are some of those components:

Smart meters: A smart meter is a meter that can record and report electricity consumption information automatically. Smart meters identify consumption in greater detail than a conventional meter and communicate that information back to the electrical utility for monitoring and billing purposes. Smart meters will range in terms of interaction with the utility and the distribution component of the grid, from relaying information on a daily, hourly or real-time basis. Smart meters are more tamper-resistant, can be remotely connected or disconnected, help with the detection of outages, as well as unauthorized removal and meter bypass. The data may be sent to the utility provider either over the wires or wirelessly. As mentioned above, in Ontario, every home and business will have a smart meter by the end of 2010.²¹ In the United States, more than 8.3 million smart meters have already been installed,²² and the number is projected to reach 52 million by 2012.²³

Smart appliances: Smart appliances may be configured by the end-user to communicate information directly to the utility operator for efficient and more productive use of electricity. Consumer investments in “smart” devices could save them money on energy consumption in the future. Smart devices include thermostats, clothes washers, dryers, microwaves, hot water heaters, and refrigerators. “For example, a ‘smart’ water heater could be equipped with a device that coordinates with a facility’s energy-management system to adjust temperature controls, within specified limits, based on energy prices.”²⁴ This practice is called “dynamic pricing.”

Many smart appliances are designed to communicate frequently with the grid to indicate how much energy they are using, as well as understand and respond to price incentives, which will provide detailed information on their use and status. Several major appliance manufacturers are already working on appliances to be used on a Smart Grid. General Electric Co. will introduce smart water heaters by the end of 2009 and will roll out “smart” versions of each of its appliances over the next

21. *ibid.*, *Ontario Smart Meter*.

22. J. St. John, “8.3 Million U.S. Smart Meters and Counting,” *Seeking Alpha* (July 20, 2009): <http://seekingalpha.com/article/149728-8-3-million-u-s-smart-meters-and-counting> accessed November 10, 2009.

23. *ibid.*, *Smart Grid System Report* pp. vi.

24. *ibid.*, *Smart Grid System Report*.

several years.²⁵ Whirlpool Corporation will produce one million smart clothes dryers by 2011.²⁶ These appliances will be able to automatically turn off during times of high electricity demand and will be equipped with software that will allow the appliance to communicate with metering devices and other appliances in the home.²⁷ The technologies will work in conjunction with tiered electricity pricing to allow the consumer to use power in a cost-efficient manner.²⁸

Dynamic pricing: Dynamic pricing is a type of economic incentive, and the consumer's response to those incentives is called "demand participation" or "demand response." Dynamic pricing uses technology that will provide the customer with pricing information for current or future time periods, and will allow the customer to modify his/her demand in accordance with this pricing information. Dynamic pricing can take the form of:²⁹

- *Time-of-use pricing:* Energy prices are higher at pre-designated peak times.
- *Critical peak pricing:* The most critical peak hours are identified and a much higher price level is set for those hours, however the total number of hours with higher prices is a comparably smaller number of hours than time-of-use.
- *Real-time pricing:* Prices vary by the hour according to the utility's cost to purchase the energy.

Consumer access to energy-related information: Consumers will have access to energy pricing information, status of their usage, and other energy-related information. Companies are advancing energy use tracking tools and software applications so consumers may monitor their electrical consumption with a view to saving money and reducing their carbon footprint (e.g., Google's PowerMeter, Microsoft's Hohm, and GridPoint Inc.). Hydro providers are also setting up their own customer web interfaces.

Load management: Load management will grant active or passive control of customer smart appliances such as air conditioners, water heaters, and pool pumps to the utility company so it may reduce or smooth demand for electricity during peak energy demand periods. Please see Appendix B for additional description of Smart Grid components.

Privacy Concerns

Modernization of the grid will increase the level of personal information detail available as well as the instances of collection, use and disclosure of personal information. Instead of measuring energy use at the end of each billing period, smart meters will provide this information at much shorter intervals. Even if electricity use is not recorded minute by minute, or at the appliance level, information may be gleaned from ongoing monitoring of electricity consumption such as the approximate number

25. R Smith, "Stimulus Funds Speed Transformation Toward 'Smart Grid'," *The Wall Street Journal* (September 28, 2009).

26. *ibid.*

27. *ibid.*

28. *ibid.*

29. *ibid.*, pp. 15.

of occupants, when they are present, as well as when they are awake or asleep.³⁰ For many, this will resonate as a ‘sanctity of the home’ issue, where such intimate details of daily life should not be accessible.

There are many significant privacy concerns and issues relating to the U.S. Smart Grid according to a high-level privacy impact assessment (PIA) by the Privacy Sub-Group of the Cyber Security Coordination Task Group responsible for addressing privacy on the Smart Grid, particularly in the area of consumer-to-utility information exchanges. The PIA stated that:³¹

- the privacy implications of the Smart Grid are not yet fully understood
- there is a lack of formal privacy policies, standards, or procedures by entities who are involved in the Smart Grid and collect information
- comprehensive and consistent definitions of personally identifiable information do not generally exist in the utility industry
- distributed energy resources and smart meters will reveal information about residential consumers and activities within the house
- roaming Smart Grid devices, such as electric vehicles recharging at a friend’s house, could create additional personal information
- smart meters and the Smart Grid network will be able to use personal information in unlimited numbers of ways
- despite the 2000 resolution adopted by the National Association of Regulatory Utility Commissioners urging the adoption of privacy principles, few state level utility commissions have begun to assess privacy and the Smart Grid
- future research is necessary and conducting further PIAs is crucial.

Privacy concerns arise when there is a possibility of discovering personal information such as the personal habits, behaviours and lifestyles of individuals inside dwellings, and to use this information for secondary purposes, other than for the provision of electricity. Electric utilities and other providers may have access to information about what customers are using, when they are using it, and what devices are involved. An electricity usage profile could become a source of behavioural information on a granular level.³²

30. *R. v. Gomboc*, 2009 ABCA 276 at 17. See also A Maykuth, “‘Utilities’ smart meters save money, but erode privacy,” *The Philadelphia Inquirer* (September 6, 2009), and A Jamieson, “Smart meters could be ‘spy in the home’” *The Telegraph* (October 11, 2009).

31. U.S. Department of Commerce, “NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)” (September 2009) 83-84; U.S. Department of Commerce, “Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements” (September 2009) 8-14. See also U.K. Department of Energy and Climate Change, “Impact Assessment of smart/advanced meters roll out to small and medium businesses” (May 2009) pp. 23-24.

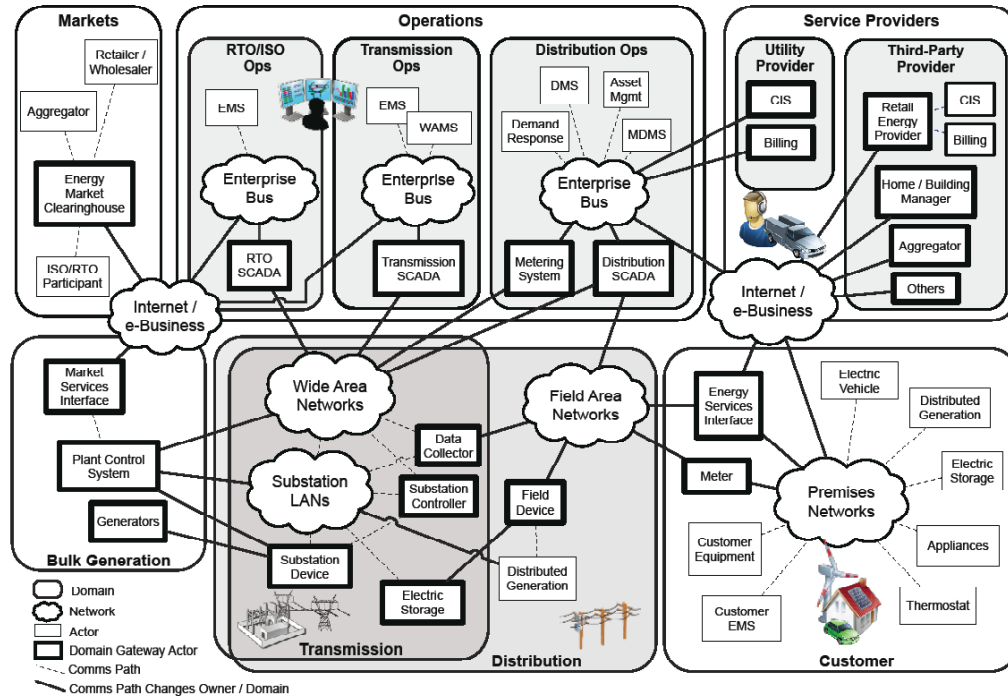
32. With regard to the 4th Amendment and s. 8 *Charter* issues, here note that further analysis must take place to determine the appropriate standards for government access to the data and for civil subpoenas and search warrants. There is some legal scholarship in this area already, see *Lerner and Mulligan*, “Taking the ‘Long View of the Fourth Amendment: Stored Records and the Sanctity of the Home,’” 2008 *Stan. Tech. L. Rev.* 3.

For example, it is suggested that the following information could be gleaned with the introduction of end-user components (these issues will become more practical concerns as appliances and devices become part of the grid): Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used. Combined with other information, such as work location and hours, and whether one has children, one can see that assumptions may be derived from such information. For example: the homeowner tends to arrive home shortly after the bars close; the individual is a restless sleeper and is sleep deprived; the occupant leaves late for work; the homeowner often leaves appliances on while at work; the occupant rarely washes his/her clothes; the person leaves their children home alone; the occupant exercises infrequently.³³

The use of identifiable information beyond the primary purposes for which it was originally collected requires special considerations from a privacy perspective. There may be the temptation to bundle such information into several different data products such as energy usage or appliance data, either in identifiable customer-level, anonymized or aggregate form. Other “temptations” may include utilities and third parties using the data to seek consent for other services, and third parties seeking to engage the user directly for commercial gain (e.g., targeted advertising). Though our primary concern is with personally identifiable information, even data that is anonymized may still raise privacy issues. As has been the case in the behavioural advertising arena, users can be treated differently or marketed to specifically based on individual, but not personally linked data, raising the need for enhanced privacy protections.³⁴ In addition, researchers have documented the ease of identification of users, even when a minimum of non-personal information about them is available.³⁵

It is not yet clear who along the grid will have access to a user’s personal information and where on the grid such access will be possible. Some utilities have indicated that they have no need or desire for device level electricity usage for their grid management needs. In some current Smart Grid environments, consumers have already begun to receive information about their own electricity use, as compared to other consumers in their geographic area. When these data points become more specific (i.e., perhaps broken down by income, age, household size, etc.), what are the benefits and risks to the dissemination of more granular data? In the United States, many states already have regulations for utilities with respect to account data. It is yet unclear how this new information will be treated under the current regulatory regimes. It is important to research further the potential for such access and the treatment of personal information, given the vast information sharing components of the Smart Grid, as shown in the following diagram (see next page).

-
- 33. E. L. Quinn, “Privacy and the New Energy Infrastructure” (Working Paper Series, 2009): <http://ssrn.com/abstract=1370731>
 - 34. FTC Press Release, “FTC Staff Revises Online Behavioral Advertising Principles” (February 12, 2009): <http://www.ftc.gov/opa/2009/02/behavad.shtm> accessed November 10, 2009
 - 35. See P. Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization” (Legal Studies Research Paper No. 09-12, University of Colorado Law, 2009): http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 accessed November 10, 2009.



Information sharing components of the Smart Grid³⁶

Concerns exist that personal information on the Smart Grid could be used to make important decisions regarding individuals without their consent, such as in the case of determining insurance risk. As a result, earning the trust of consumers in the modernization of the electrical grid into the Smart Grid will be key.³⁷ Since the future Smart Grid relies on consumers to use and invest in smart technologies, the Smart Grid itself is dependent on ensuring that consumers see the value of such time and investment.³⁸ If the Smart Grid and smart appliances become synonymous with privacy invasion, visions of the Smart Grid may slow or stall altogether. However, there is another way, it starts by *building SmartPrivacy into the Smart Grid*.

III SmartPrivacy for the Smart Grid

There are a number of important and necessary uses of personal information in the Smart Grid context, such as by a utility provider in the provision of service, price notification, connecting and disconnecting power remotely, and detecting the theft of devices. In addition, the use of personal information may be used to offer beneficial services to consumers, such as energy efficiency analysis and monitoring, and load management. However, other uses of consumer information - those not directly tied to the primary purpose of collecting the data - may raise privacy concerns if consent from the individual has not been obtained.

36. *ibid.*, Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements, pp. 11.

37. "Utilities, regulators and governments will need to give consumers confidence that their usage data is being handled by authorized parties in an ethical manner. Such assurances will be the key when developing the public perception of these new technologies." World Economic Forum in partnership with Accenture, 'Accelerating Smart Grid Investments' (2009), pp. 30.

38. "To boost adoption rate, policy-makers and energy suppliers need to be innovative to help increase customer participation..." The Brattle Group, "Unlocking the €53 Billion Savings from Smart Meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment," (October 2009): http://brattle.com/_documents/UploadLibrary/Upload805.pdf accessed November 10, 2009.

Without diminishing the benefits of the Smart Grid, it is possible to design privacy directly into the Smart Grid by making it the default (no action would not be an option) in all physical, administrative and technological aspects of the system. The vision of SmartPrivacy can be translated in terms of the vision for the Smart Grid in the following way:

Smart Grid ³⁹	Smart Grid with SmartPrivacy
Intelligent – capable of sensing system overloads and rerouting power to prevent or minimize a potential outage; of working autonomously when conditions require resolution faster than humans can respond and cooperatively in aligning the goals of utilities, consumers and regulators.	Intelligent – capable of collecting the minimum amount of personal information necessary from consumers, without diminishing the quality and range of services offered. Works transparently with consumers to communicate information regarding the collection, use and disclosure of their personal information. Plans in advance how to protect privacy and security, and builds it into the system in advance of its use.
Efficient – capable of meeting increased consumer demand without adding infrastructure.	Efficient – capable of meeting increased consumer demand without compromising the privacy and security of personal information. Securely disposes of personal information when it is no longer needed for the purpose for which it was originally collected.
Accommodating – accepting energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas; capable of integrating any and all better ideas and technologies – energy storage technologies, for example – as they are market-proven and ready to come online.	Accommodating – accepting of a variety of consumer preferences with regards to the use, retention, and disclosure of personal information - makes these options easily accessible to the individual.
Motivating – enabling real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns.	Motivating – enabling communication and notice between the consumer and utility so that consumers can tailor their personal information options, based on individual preferences. Proactively obtains consent <i>before</i> disclosing any personal information to a third party.
Opportunistic – creating new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate.	Opportunistic – creating new opportunities and markets by means of its ability to capitalize on privacy-enhancing technologies, wherever and whenever appropriate.

39. *ibid.*, *The Smart Grid: An Introduction*, pp. 17.

Quality-focused – capable of delivering the power quality necessary – free of sags, spikes, disturbances and interruptions – to power our increasingly digital economy and the data centers, computers and electronics necessary to make it run.	Quality-focused – capable of delivering information that is free of inaccuracies, and allowing individuals to access to their personal information and make any corrections necessary.
Resilient – increasingly resistant to attack and natural disasters as it becomes more decentralized and reinforced with Smart Grid security protocols.	Resilient – increasingly resistant to data leakage and breaches of personal information - reinforced with privacy and security protocols, such as privacy by default and breach notification protocol.
“Green” – slowing the advance of global climate change and offering a genuine path toward significant environmental improvement.	“Green” –by ensuring consumer trust in the Smart Grid and its associated technologies, fostering greater participation by individuals leading to environmental improvement.

Specifically in the case of utilities providing personal information to a third party with the express consent of the individual, the following are examples of SmartPrivacy defaults that offer greater protection of privacy:

- The minimal amount of information should be provided to third parties given the nature of the relevant service. For example, partial location data such as the first few digits of a zip or postal code may be sufficient for services that allow for comparison of neighbourhood averages, and other features such as weather statistics.
- Pseudonymize identity, where possible. When sharing data with a third party, consider using a pseudonym such as a unique number, which the individual would be permitted to reset at any time.
- Third parties should not request information from the utility about consumers, rather, consumers must be able to maintain control over the type of information that is disclosed to third parties by the utility.
- When data is transmitted, the risk of interception arises. We recognize there are multiple channels of communication, such as home area networks, telecommunication systems, and internet protocols. Appropriate, secure channels of transmission are necessary to ensure strong privacy protection along the Smart Grid, commensurate with the type of data conveyed.
- Third parties should agree not to correlate data with data obtained from other sources or the individual, without the consent of the individual.

SmartPrivacy’s holistic approach requires that individuals and relevant industries be made aware of how to ensure *Privacy by Design*. We agree that there should be “documented requirements for regular privacy training and ongoing awareness activities for all utilities vendors, and other entities

with management responsibilities throughout the Smart Grid.”⁴⁰ However, even if notice is provided regarding data use and disclosures, communicating the policies to consumers is not easily achieved. The emerging Smart Grid ecosystem is an opportunity for commercial entities to improve the methods by which they convey their data use practices to consumers so that consumers can make fully informed decisions regarding the use of their information.

The public must also be educated about the need to protect their privacy when engaging the Smart Grid services of third parties, who will have access to their energy consumption information. Utility providers and vendors cannot assume that individuals will inherently know how to protect their personal information. We know this is not the case. For example, Facebook has over 250 million active users, however many of them do not make use of the available privacy settings because they are not aware of their availability. The Federal Trade Commission has increasingly recognized that privacy policies are often inadequate methods of disclosing the uses of personal information by commercial entities. Utilities and third party service providers should provide clear instructions to the consumer as to how to use the privacy safeguards offered, such as a secure login and password, as well as how to un-enroll and delete their personal information.

President Barack Obama has stated, “America’s economic prosperity in the 21st century will depend on cybersecurity.”⁴¹ As such, utility providers’ efforts at identifying threats will become increasingly important as the grid becomes more complex and interconnected. With additional entry points and data paths, the vulnerabilities increase as well, involving “the potential for compromise of data confidentiality, including the breach of customer privacy.”⁴² As the risk management framework for the Smart Grid continues to develop, designers of the Smart Grid and utility providers must ensure that unauthorized access to personal information traveling through the electrical grid is minimized, as much as possible. For example, a hacker with access to smart meters could tamper with billing information, device control, privacy, identity information and communications. Wireless networks used by the utility to communicate with smart meters can expose control signals and consumption data to such treats as eavesdropping, interception, or message forgery.

Special attention should be paid to insider threats within utilities and those organizations that provide services using consumers’ energy consumption information. The Institute for Information Infrastructure Protection (I3P), is conducting leading-edge research into the area of insider threats.⁴³ These threats are unique as to how an organization can prevent, detect and mitigate their occurrence since the insider perpetrating the threat is using legitimate rights and privileges to access personal information, but for unauthorized purposes. Rogue insiders may be found at any level of an organization, including employees, contractors, business partners, auditors, and even alumni. Using a multi-disciplinary approach, I3P researchers are creating methods for the detection, monitoring and prevention of insider threats, and are advancing our understanding of the actions and range of threats posed by insiders.

40. *ibid.*, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, pp. 12.

41. The White House, “Remarks by our President on Securing Our Nation’s Cyber Infrastructure” (May 29, 2009): http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

42. Electric Power Research Institute, “Report to the National Institute of Standards and Technology on the Smart Grid Interoperability Standards Roadmap” (August 2009), pp. 41.

43. I3P, “Human Behavior, Insider Threat and Awareness”: http://www.thei3p.org/research/insider_threat.html accessed November 10, 2009.

Examples of Preliminary Privacy Questions Regarding Individual Smart Grid Components

To illustrate the breadth of the privacy issues that may arise relating to the Smart Grid, we highlight a few of the questions that need to be addressed regarding the protection of personal information at the individual Smart Grid component level.

Component	Technology or application		Privacy questions
End User Component	Smart Meters	Remote Connect / Disconnect of Meter	Will disconnection of power be based on any new sources of energy consumption data created by the use of smart meters?
		Meter Detects Meter Bypass	While this technology will reduce theft, will it produce false positives and expose innocent individuals to possible fines or criminal proceedings?
		Data Collection, Communication and Storage	Will data collection and communication be secure? Will the utility develop proper policies and procedures for maintaining data privacy?
	In-home Appliances that Communicate with the Utility Operator * Highly sensitive		Will information from the home regarding specific appliance use or disuse be relayed directly to the utility?
	In-home Devices that Communicate Usage Information to the Customer		Will these devices also share data with third parties, and if so, on what basis? ... With the consent of the customer?
	Consumer Access to Energy-Related Information		Will access to this information (e.g., username and password) be kept private and secure - not disclosed to or captured by third parties?
	Automated Feeder Equipment		Will the automated system communicate directly with smart meters, and potentially disclose personal information regarding electricity use in the home?

Component	Technology or application	Privacy questions
Electricity Distribution Component	Fault Detection	When detecting faults in the Smart Grid, will systems have access to personal information regarding electricity use in real time, without direct interface with the consumer?
	Load Management	Will the utility company shut off appliances within the home without the consent of the occupant? Will tenants have less privacy vis-a-vis landlords who participate in load management?
	“Load” or Demand Information Communicated to Smart Generators	Will generators have direct access to electricity demand information, and if so, could individual household electricity be discernible?
Electricity Generation	“Distributed” or “On-Site” Generation	When on-site generation is provided back to the power system, will customer information be kept private and secure?
	Plug-In Hybrid Electric Vehicles	Will a charging vehicle’s location be shared with the utility operator? In “authenticating” charged vehicles for billing purposes, will the authentication scheme, by necessity (Privacy by Design) address the privacy and security issues? What role will batteries play on the Smart Grid? Will there be restrictions on charging during peak demand? Will batteries exchange power with the Grid?

IV Conclusion

The inside of a dwelling is the most private of places, and is recognized at the highest judicial levels. The Supreme Court of the United States says: “In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.”⁴⁴ The Supreme Court of Canada also states: “There is no place on earth where persons can have a greater expectation of privacy than within their ‘dwelling-house’.”⁴⁵ Capturing the flow of electricity into one’s home, and the manner in which it is used over a period of time, may be revealing and highly intrusive. The overarching privacy concerns associated with Smart Grid technology are its ability to greatly increase the amount of information that is currently available relating to the activities of individuals within their homes.⁴⁶

The information collected on a Smart Grid will form a library of personal information, the mishandling of which could be highly invasive of consumer privacy. There will be major concerns if consumer-focused principles of transparency and control are not treated as essential design principles from beginning to end. Once energy consumption information flows outside of the home, the following questions may come to the minds of consumers: Who will have access to this intimate data, and for what purposes? Will I be notified? What are the obligations of companies making smart appliances and Smart Grid systems to build in privacy? How will I be able to control the details of my daily life in the future? Organizations involved with the Smart Grid, responsible for the processing of customers’ personal information, must be able to respond to these questions, and the best response is to ensure that privacy is embedded into the design of the Smart Grid, from start to finish — end-to-end.

As the Smart Grid is only in its early stages of development, now is the time to build SmartPrivacy into the Smart Grid. Consumer control of electricity consumption and consumer control of their personal information must go hand in hand. Doing so will ensure that consumer confidence and trust is gained, and that participation in the Smart Grid contributes to the vision of creating a more efficient and environmentally friendly electrical grid, as well as one that is protective of privacy. This will result in a positive sum (win-win) outcome, where both environmental efficiency and privacy may coexist.

44. *Kyllo v. United States*, 533 U.S. 27 (2001).

45. *R. v. Silveira*, [1995] 2 S.C.R. 297, at 140.

46. The “hour each night [that] the lady of the house takes her daily sauna and bath [is] a detail that many would consider ‘intimate’.” *ibid.*, *Kyllo*.

Appendix A – 7 *Privacy by Design* Foundational Principles

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

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

2. Privacy as the *Default*

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

3. Privacy *Embedded* into Design

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

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

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

5. End-to-End Lifecycle Protection

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

6. Visibility and Transparency

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

7. Respect for User Privacy

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

For more information and resources on these subjects, I would encourage you to visit www.smartprivacy.ca and www.privacybydesign.ca.

Appendix B – Smart Grid Components

Modernization of the electrical grid will bring together and make possible the operation of several important components, including end-user components (discussed at page 11), as well as electricity distribution, transmission, and generation components described below.

Electricity Distribution Component

Electricity distribution is the carrying of electricity from the substation to the consumer's metering point. The distribution component consists of feeders, power lines, and transformers, which serve to change the voltage from transmission levels to consumer use levels. Smart Grid technologies in this component include the following –

- 1) **Distribution Automation.** A vital piece of the Smart Grid, this technology includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution component.
- 2) **Automation within Substations.** This automation involves monitoring and controlling equipment in substations to enhance power system reliability and efficiency.
- 3) **Automation of Feeder Equipment.** Feeder equipment is the infrastructure carrying electricity from a substation to consumers, usually in the form of power lines. Operators can remotely engage switches, regulators, and retrieve power system information from smart meters.
- 4) **Fault Detection.** The automated devices will communicate with smart meters to detect power outages without requiring a call to the distribution company. Further, the distribution grid will isolate the malfunctioning equipment and reroute power directly to the consumer.
- 5) **Load Management.** This technology will grant active or passive control of customer appliances such as air conditioners, water heaters, and pool pumps to the utility company to better reduce or smooth demand for electricity.
- 6) **Data Gathering and Storage.** The volume of data collected by utility companies from interactive Smart Meters will dwarf the current volume of data collected by several orders of magnitude.

Electricity Transmission Component

Electricity transmission is the bulk transfer of electrical energy from generators to substations via overhead power lines or underground cables. Most activity in this component takes place in substations, whose operations are controlled by the Supervisory Control and Data Acquisition (SCADA) system. Smart Grid technologies in this component will include the following –

- 1) **Real-Time Management of Lines and Substation Equipment.** The SCADA system will monitor equipment and measurements and give operators better control over the component.
- 2) **Real-Time Analysis of Energy Flow through Energy Management Systems (EMS).** Through forecasts and modeling, this analysis will ensure stability and continued flow through the transmission component.

Electricity Generation Component

Electricity generation is the process of creating electricity from other forms of energy, such as chemical combustion, nuclear fission, photovoltaics (solar), or kinetics (water and wind). Smart Grid technologies in this component will include the following –

- 1) **Communication of Performance and Quality of Service Issues.** Smart generators will be able to relay information to operators that a resource such as wind or sun is scarce and will not be sufficient to generate electricity. Similarly, a Generator will be able to communicate that it is malfunctioning or failing.
- 2) **Rerouting of Electricity.** Smart Generators will have the capability to engage in real-time rerouting of electricity to the Grid when a performance issue arises. This technology will require interconnectivity of Generation operations and interlocking infrastructure within the grid.
- 3) **“Load” or Demand Information Communicated to Smart Generators.** Information regarding customer demand will be sent back to the generators so that operators know when to bring new generators online or to scale back production during times of low usage.
- 4) **“Distributed” or “On-Site” Generation.** Electricity is sometimes created by the end-user or on-site to be used as either a primary power source or as an emergency backup to the power system. In some cases, such generation can provide electricity back to the power system. Further, the utility may be able to request or control devices to provide energy back to the electrical system to meet system demand and quality.
- 5) **“Micro grid.”** “A micro grid is a distribution system with distributed energy sources, storage devices and controllable loads, which may generally operate connected to the main power grid, but is capable of operating as an island.”⁴⁷

Emerging Technologies – Plug-in Hybrid Electric Vehicles

If and when this technology is embraced, the Smart Grid must be able to manage vehicle connection and charging. Consumers may charge at their home or place of business or charge at another location, potentially for a fee. Vehicle charging may be “optimized” by charging at times of low pricing or demand. PHEVs may interact with the utility operator by sending excess power back onto the grid during times of high demand.

47. *ibid.*, *Smart Grid System Report*, pp. 30.

About the Authors

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

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada and is a member of the Future of Privacy Advisory Board. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow *Privacy by Design* and hopes to make it go "viral."

Jules Polonetsky, Co-Chair, Future of Privacy Forum

Jules Polonetsky has served since November 2008 as Co-Chair and Director of the Future of Privacy Forum, a think-tank seeking to improve the state of online privacy by advancing responsible data practices. His previous roles have included serving as Chief Privacy Officer at AOL and before that at DoubleClick, as Consumer Affairs Commissioner for New York City, as an elected State Legislator and as a congressional staffer, and as an attorney. He has served on the boards of groups such as TRUSTe, the IAPP, the Network Advertising Initiative and the Better Business Bureau (N.Y. Region). His writing and research can be found at www.futureofprivacy.org.

Christopher Wolf, Co-Chair, Future of Privacy Forum

Christopher Wolf is the Co-Chair of the Future of Privacy Forum. He is also a partner in the Washington, D.C. office of Hogan & Hartson LLP, where he is a leader of that firm's privacy practice group. Mr. Wolf is the editor and lead author of the Practising Law Institute's (PLI) treatise of privacy law. He also is co-editor of the PLI book, "A Practical Guide to the Red Flag Rules", the identity theft prevention regulations issued by the FTC and financial regulators. Chris has served as an adjunct law professor on Internet and privacy law, and is a frequent lecturer in continuing legal education programs on the subject. Reflective of his status as a thought leader on privacy, Chris speaks and writes extensively domestically and internationally on privacy issues at major conferences, law school symposia and for the media. Chris has served as an adjunct law professor on Internet and privacy law, and is a frequent lecturer in continuing legal education programs on the subject.



Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

The Future of Privacy Forum

919 Eighteenth St. NW #925
Washington, D.C. 20006
U.S.A.
Telephone: (202) 713-9466
Fax: (202) 464-4001
E-mail: info@futureofprivacy.org
Website: www.futureofprivacy.org

The information contained herein is subject to change without notice.
The Future of Privacy Forum and IPC shall not be liable for technical
or editorial errors or omissions contained herein.

November 2009

THE FUTURE OF PRIVACY FORUM
WWW.FUTUREOFPRIVACY.ORG



Information and Privacy Commissioner,
Ontario, Canada