Privacy by Design:

Fundamentals for Smart Grid App Developers

www.privacybydesign.ca

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

Quinzee

August 2013

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

Message from the Commissioner

I make every effort to reach out to those in the technology field to deliver the message that *Privacy by Design* (*PbD*) is integral to information technology systems, as was globally recognized in 2010. Regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *PbD* as an essential component of fundamental privacy protection. From start-ups to multinationals, to industry consortia, the response has been overwhelming, with the Foundational Principles of *PbD* now translated into 31 languages.

In this publication, co-written with an Ontario-based Smart Grid app company – Quinzee – I want to specifically reach out to the burgeoning world of Smart Grid app developers so they may be empowered to adopt *PbD* and gain a competitive advantage. With the increasing availability of customer energy use information through initiatives such as the Green Button, we can and should architect apps to protect fundamental privacy values. Failure to build those values in — and build them in early — may lead to negative unintended consequences for Smart Grid app developers and their users.

Your task, then, as a Smart Grid app developer, is to embed privacy values and preferences into the design and operation of your information technologies, systems, and infrastructures. I encourage you to incorporate *PbD* into all project requirements, procurements specifications, and positive-sum operations. Any size of organization can implement *PbD*, even a one-person company. By doing so, I guarantee you will be recognized for your innovative solutions, without having to sacrifice your customers' privacy – win/win!

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

Innovation in the API Economy

Even before the Internet, Application Programming Interfaces (APIs) was important for business and technology market dynamics. An API is defined as:[1]

> *the specific method prescribed by a computer operating system or by an application program by which a programmer writing an application program can make requests of the operating system or another application.*

Competitive battles (termed 'API wars') can add fuel to a company's growth. For example, Microsoft's API allowed application developers to write applications for MS Windows, which lead to a wide selection of Windows-based applications available to consumers. As a result, many consumers chose the Windows operating system over other systems. In the Internet age, APIs create business value more than ever. The web browser is no longer the exclusive gateway to view content on the web thanks to a proliferation of devices such as smartphones, tablets, and other gadgets. Companies now choose to actively unlock their digital assets from the confines of their websites via an API. Once assets are freed up and accessible from any device, then the business growth can increase.[2] However, the applications[3] written to collect personal information from APIs as well as end users are recognized as raising a number of privacy issues.

Before we explore the application of privacy guidance to the Smart Grid app context, below is a brief overview of APIs within the Smart Grid.

APIs and the Smart Grid

The Smart Grid refers to the modernization of the current electrical grid to provide a bi-directional flow of information and electricity so consumers can have greater choices as to how, when, and how much electricity they use. In addition, it is anticipated that a Smart Grid will be self-healing in case of physical disturbances and cyber-attacks, as well as natural disasters. Such a grid could also link with a wide array of energy sources, such as renewable energy producers. Moreover, it is anticipated that a Smart Grid could provide better power quality, and enhance the efficient delivery of electricity.

[1] Whatis.com. "Definition: Application Program Interface (API)." http://searchexchange.techtarget.com/definition/application-program-interface.

[2] 3scale Networks S.L. "What Is an API? Your Guide to the Internet Business (R)Evolution." 2011.

[3] Throughout this paper we refer to "applications" as including those downloaded and installed onto one's computer, or downloaded to a mobile device operating system (such as Android, iOS, or Blackberry OS), or accessed via mobile or web browser.

The Smart Grid is enabled by new infrastructure, including the installation of Smart Meters which provide two-way communication, in near real-time. A Smart Meter is a digital electric meter that automatically records and reports electricity consumption information for monitoring and billing purposes, such as time-of-use pricing.[4] Smart Meters can identify consumer consumption in far greater detail than a conventional meter which is typically read monthly. Smart Meters can also communicate customer energy use information back to the electricity distributor, and can range in terms of interaction with the electricity distributor from a daily, hourly or near real-time basis. Smart Meters also have the following qualities: they are more tamper-resistant; can be remotely connected or disconnected; and can help with the detection of outages, as well as detect any unauthorized removal or meter bypass. In Ontario, Canada, there are now 4,764,466 million smart meters installed on households; approximately 4,567,708 million meters bill using hourly readings under the time-of-use program.[5]

In the context of the Smart Grid, supported by infrastructure such as Smart Meters, profiles of individual energy use have the potential to be a source of very detailed behavioral information, such as the lifestyle habits and behaviors of customers. Privacy concerns arise due to the potential for this information to be mishandled. In 2009, Dr. Cavoukian identified privacy in the Smart Grid as a “sleeper issue” that needed to be addressed as one of the critical success factors to implementing the Smart Grid. In a short time, following the white papers and guidance documents, efforts are being made to protect consumer privacy in the Smart Grid in Ontario and around the world. There is much reason to be optimistic about a future where we can have privacy while engaging in Smart Grid energy conservation initiatives.

API opportunities on the Smart Grid

Application developers are some of the first to unlock the opportunities to connect masses of data from the Smart Grid with those who can benefit from it. Applications that collect consumer energy usage data generated by Smart Meters, smart thermostats and smart appliances are in their infancy. However, consumers themselves are slowly becoming aware of the possibilities of what can be learned from the analysis of their energy consumption, from reducing their carbon footprint, to saving money on their electricity bill. In a recent survey, it was found that 7 per cent of U.S. adults (16.8 million) use a mobile device to manage and monitor their electricity usage.[6]

In Ontario, companies offering Smart Grid services are gathering together under the umbrella of the MaRS Discovery District’s Data Catalyst Project. The project aims to facilitate the consent-based disclosure of Smart Meter data to innovators in a secure, privacy-protective and usable way, to drive energy conservation and spur economic growth. A key feature is the development of APIs to facilitate

[4] Time-of-use pricing refers to an electricity pricing structure which takes into account the time of day that electricity is consumed by segmenting hours into off-peak, mid-peak, and on-peak pricing periods. “Off-peak [is] when demand for electricity is lowest […] Mid-peak [is] when demand for electricity is moderate. These periods are during the daytime, but not the busiest times of day. On-peak [is] when demand is highest […] Generally when people are cooking, firing up their computers and running heaters or air conditioners.” http://www.ontarioenergyboard.ca/OEB/Consumers/Electricity/Electricity+Prices#tou

[5] IESO. “Smart Metering Entity (SME) Time-of-Use Mandate Progress Report through April 30, 2013.” http://www.ontarioenergyboard.ca/OEB/_Documents/SMdeployment/SME_TOU_Mandate_Progress_Report_Apr2013.pdf.

[6] Zpryme Smart Grid Insights. “June 2013 U.S. Electricity Monitoring Survey.” http://smartgridresearch.org/news/4-8-of-americans-monitor-electricity-usage-on-a-smartphone-zpryme-reports.

consent-based disclosure of customer energy usage data. Initiated by the Ontario government, this project is called "Green Button" and aims to allow electricity customers to download their own energy usage data in an easy-to-use format. The aim of the initiative is for consumers to be better educated about their energy decisions and encourage consumers to make investments to reduce their energy costs. There are two facets to Green Button:

- *"Download My Data"* – customer energy usage data goes directly from the utility to the customer.
- *"Connect My Data"* – customer energy usage data is transferred from the utility to a third party with the customer's consent and authorization.

Under a Connect My Data scenario, a subsection of Smart Grid app companies can deliver services focusing on consumer energy use behaviour change. Much of the value of Smart Meters and other types of home-management data arises when comparing users to various groups, such as exerting social pressure on the user through a subtle or not so subtle 'nudge'. (E.g. your friend/neighbour just replaced all of his lights with CFLs/LEDs; 84% of your neighbours program their thermostat). The most common functionality in these applications is the ability to view electricity usage in near real-time as well as historically. It is also common to be able to see this usage in the context of other sets of individuals, whether that means comparing to those who live nearby or have similar homes/buildings or lifestyles. Further, applications often have tips and suggestions for users, sometimes generic in nature, while other apps provide personalized advice based on user profiles. Personalized advice increases the relevance of tips provided and thereby engages and challenges the user to act on the insights and advice.

Regardless of their objectives, many Smart Grid applications will require some degree of personal data and developers will have to adopt a privacy protective approach to the collection of personal information.

Privacy overview

Privacy is an issue of control – the need to maintain personal control over the collection, use and disclosure of one's personally identifiable information. It is a concept that is best reflected in the German right of "informational self-determination" which holds that the individual should be the one to determine the fate of his or her personal information. Recognizing privacy as an exercise in control has always been important, but it is critical today in an age characterized by far-reaching online social media and ubiquitous computing. Too often, issues of privacy and the protection of personal information are regarded as the domain of large corporations – those with a Chief Privacy Officer or formal privacy infrastructure. This is not the case. The Internet has proven to be such a tremendous leveller – today, relatively small organizations and even individual application developers may control disproportionately large volumes of personally identifiable information. All should bear a responsibility to understand their relationship with personally identifiable information and strategize accordingly. The Information and Privacy Commissioner

> *The Internet has proven to be such a tremendous leveller – today, relatively small organizations and even individual application developers may control disproportionately large volumes of personally identifiable information.*

of Ontario, Canada has written about the privacy implications of moving towards greater use of devices, increased flow of digital assets, and the practical ways that privacy can be built into these systems. For example, in "The Roadmap for *Privacy by Design* in Mobile Communications", the Commissioner recommended that application developers practice data minimization, use privacy-protective default settings, and maintain user awareness and control of data collection and use. In "*Privacy by Design* and the Emerging Personal Data Ecosystem" the Commissioner described how personal information is the new "oil" of the Internet and how it largely resides with organizations – removed from the individual's sphere of control. The Personal Data Ecosystem will move towards placing control of one's personal information into the hands of the individual.

Typically, many will think of personal information as one's name, address, and telephone number. However, personal information can include much more, such as any identifying number. That's because the definition of personal information is defined as any information about an identifiable individual. To be prudent, consider personal information as including IP address, photographs, contact lists, social networking connections, location information, any information that reveals patterns or habits, and any information that can link a device to its owner (i.e. device identifier). Even if information on its own does not identify an individual, consider whether if in combination with other information, it could reveal an individual's identity. Be aware that information collected from other sources and linked to that individual's profile becomes their personal information as well. In the Smart Grid app context, you'll want to identify the data elements being collected (e.g. Kw/h, date, time, etc.). This information must be considered personal information when obtained through an API with customer consent. Any additional information collected from the consumer is also considered personal information (i.e. credit card information, location information, device identifiers, description of home, family, behaviour, etc.).

Energy data and app developers

The privacy issues arising from the larger world of desktop and mobile applications will, by necessity, bear upon any Smart Grid app development initiative. These include all privacy issues associated with computers, ISPs as central hubs, combining significant computing power with portability, wireless communication (e.g. signal interception), location data privacy, the "always-on" nature of some technologies (especially mobile phones), and the propensity for small portable devices to be lost or stolen.

The importance of building-in privacy

Many would agree that the sensitivity around personal data collected and transmitted by software applications on desktops and mobile phones is warranted. Such programs can uncover very intimate information, and can reveal the patterns of our lives, from travel, to disease, sexual preference, and political views.[7] Apps collecting personal information have received strict scrutiny from government bodies as well as the media regarding their impact on privacy. You do not want to be the subject of

[7] Natasha Singer. "A Tumultuous Trip to Mobile App Transparency." The *New York Times*, December 8, 2012.

a negative front page headline, nor government criticism or investigation,[8] nor a lawsuit launched by users or a regulator such as the U.S. Federal Trade Commission.[9] For example, the Wall Street Journal exposed 56 popular apps that transmit a mobile phone's unique ID to third parties without the user's knowledge or consent. Moreover, it was found that 47 of those apps sent the phone's location without permission, and five sent age, gender and other personal information without asking the user.[10] Another report found that 100,000 Android Apps were suspicious or questionable with regards to their collection of personal information.[11] U.S. House of Representatives committee hearings on Apple apps and privacy,[12] and California Attorney General actions to protect privacy in apps[13] are examples of obvious concern by government. Already, Apple, Google, Amazon, Microsoft, Hewlett-Packard and Research in Motion require app developers to have privacy policies in response to such investigations.[14] In the litigation context, several app makers were sued when it was revealed that a user's contacts were surreptitiously collected and used.[15] Social networking app "Path" settled with the U.S. Federal Trade Commission for deceiving consumers and improperly collecting personal information contained in users' mobile address books. Path agreed to a comprehensive privacy program, and to obtain independent privacy assessments every other year for 20 years. They also agreed to pay $800,000 for collecting children's personal information without parental consent.[16]

Apps collecting personal information have received strict scrutiny from government bodies as well as the media regarding their impact on privacy.

Unique aspects of energy use data

In terms of personal information collected by Smart Grid apps, Smart Meter data is the most common data available at present, but this will inevitably diversify to include other types of data from an increasing number of connected devices in homes (thermostats, appliances, lights, windows and electronics). Beyond device data, app developers may also ask users to contribute further information in order to receive more personalized functionality from the app. In the social benchmarking context, such information could include personal and household demographic information, lifestyle information and home characteristics. Much of this information is personally identifiable either on

[8] Stephanie Bodoni. "Mobile Apps Put Users' Privacy at Risk, EU Regulators Say." *Bloomberg News*, March 14, 2013.

[9] Olga Kharif. "Google to Apple Gird for FTC-Led Mobile-Privacy Crackdown." *Bloomberg News*, February 26, 2013.

[10] Scott Thurm, and Yukari Iwatani Kane. "Your Apps Are Watching You." *Wall Street Journal*, December 17, 2010.

[11] Jordan Robertson. "100,000 Android Apps Collect Too Much Data, Security Firm Finds." *Bloomberg News*, November 1, 2012. See also John Leyden. "Free Android Apps Often Secretly Make Calls, Use the Camera." *The Register*, November 1, 2012.

[12] E.g. Committee on Energy & Commerce. "Ranking Members Waxman and Butterfield Launch Inquiry into Information Collection and Use Practices of Social Apps for Apple Devices." March 22, 2012.

[13] Office of the Attorney General, State of California. "Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law." October 20, 2012.

[14] Geoffrey A. Fowler. "Tech Giants Agree to Deal on Privacy Policies for Apps." *Wall Street Journal*, February 23, 2012; Katy Bachman. "Mobile App Developers Getting Privacy Savvy, Per Study." *Adweek*, July 11, 2012.

[15] Meghan Kelly. "Path, Apple, Facebook Named in Mobile Privacy Class-Action Lawsuit." *Venture Beat*, March 17, 2012.

[16] Federal Trade Commission. "Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books." http://www.ftc.gov/opa/2013/02/path.shtm.

its own or in combination with other information that is freely available (e.g. Google, the Postal Code system). The type and amount of information that a user may be encouraged to provide will depend on the application. For example, Smart Grid apps may request personal information to deploy messaging techniques that may lead to energy conservation behavioural changes. Some of these messaging techniques are:

- Delivering a message from the right messenger;
- Understanding a user's pre-established norms;
- Setting the user's default choices;
- Delivering salient messages;
- Appealing to the user's emotions;
- Understanding a user's public promises and catering to them; and,
- Delivering messages or opportunities that will make a user feel better about themselves.

App developers should be conscious of a number of unique characteristics of energy use data, most notably that access to this type of data is relatively new and there is little societal knowledge around what information poses a real privacy threat to users, and what does not. There are still many misperceptions about what energy use data can reveal about an individual, household or business, thus, educating users is particularly important when offering services that rely on access to this data. It will be increasingly important for application developers to ensure they educate users from a personal privacy perspective. Without a basic level of understanding and comfort with privacy, Smart Grid data driven apps will remain at a handicap for widespread adoption and ultimately fall short of their immense potential. In addition to loss of customers, a bad privacy reputation can also affect other commercial opportunities for Smart Grid app developers, such as winning a bid on a contract, or partnering opportunities with established members of the electricity sector.

Privacy by Design:

The Fundamentals for Smart Grid app developers

Engendering trust is critical for the success of any Smart Grid application collecting energy usage data. Employing *Privacy by Design* principles, described below, can help to stimulate clear privacy goal-setting; systematic, verifiable methodologies; practical, demonstrable results; as well as vision, creativity, and innovation. Sometimes app companies collecting personal information are very small, and it is difficult for them to cover all their privacy bases. We hope this section assists Smart Grid app developers with understanding how to apply *Privacy by Design*. Naturally, *Privacy by Design* applies to energy usage data and the personal information attached to a user's account.

Developed back in the 1990s by Commissioner Ann Cavoukian, Ph.D., *Privacy by Design* involves embedding privacy into information technologies, business practices, and networked infrastructures, as a core functionality, right from the outset. This means building in privacy right up front intentionally and with forethought. *PbD* may thus be defined as an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls. At the same time, however, the *Privacy by Design* approach provides a framework to address the ever-growing and systemic effects of ICTs and large-scale networked data systems with enhancements to traditional Fair Information Practice Principles.

PbD may thus be defined as an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls.

These fundamentals are meant to compliment, and are in addition to, the requirements of platforms such as Apple, Android, Facebook, Google, etc., with respect to the protection of personal information, as well as applicable laws.

There exist a number of resources and requirements to aid in the protection of personal information in the design of apps (See Appendix A) including a dedicated website by the Future of Privacy Forum (www.applicationprivacy.org). Custodians of APIs are often taking a leading role in making such resources available to app developers.[17] Governments also have their own initiatives,[18] as are industry associations.[19]

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

You're likely reading this because you have an innovative idea for an app to help energy consumers track and reduce their energy footprint. Great! Before starting to "code," however, recognize whether your Smart Grid app will be collecting, using and disclosing personal information. Many times the app development cycle occurs at breakneck speed with little regard to privacy.[20] Once the app is coded, engineering privacy is often too late. First ask, are you providing personalized services? Do you need personal information at all? And if you are, what is the core information you need and why would you need more? By asking these questions, you are putting to use the first principle of *Privacy by Design* "***Proactive* not Reactive; *Preventative* not Remedial.**" You are taking actions to anticipate and prevent privacy invasive events before they happen. Instead of waiting for privacy risks to materialize, you aim to prevent breaches before they occur.

It's important at this stage to see privacy as holistic. That means integrating privacy into the development cycle of your product or service, and practicing data minimization techniques. Also, you'll want to do this as early as possible. Do not bolt privacy on after-the-fact (i.e. do *not* launch without having a holistic privacy program in place). Privacy must be incorporated as you develop

[17] For example, Mozilla has developed a tiered permission model, and tips for designing apps with privacy in mind. https://blog.mozilla.org/privacy/2013/04/04/app-app-make. See also Vodafone. "Guidelines for All Applications," http://developer.vodafone.com/develop-apps/privacy/guidelines-all-applications.

[18] E.g. the U.S. Department of Commerce's Mobile Application Transparency Process, http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[19] For example, it is the Application Developers Alliance's position that "Developers will succeed only if consumers trust that the apps they enjoy are not secretly abusing their personal information", http://appdevelopersalliance.org/policy. The Mobile Entertainment Forum (MEF) has initiated a "Privacy in Mobile Applications Initiative" which aims to create a framework for mobile app privacy policies, best practices and tools for obtaining consent, as well as a privacy rating system for consumers. See http://www.mefmobile.org/activities-and-analytics/Initiatives_home/privacy.

[20] Christine Dobby. "Glossing over Privacy Considerations Can Bite a Developer in the App." *Financial Post*, November 7, 2012.

the solution, and in your prototyping. You'll soon become familiar with Privacy Impact Assessments (PIAs), privacy and security gap analysis, and Threat Risk Assessments (TRAs) which will help you utilize and document appropriate privacy and security practices. See where you stand in relation to Privacy Maturity Modelling (PMM), and commit to trying to achieve higher PMM levels.[21]

2. Privacy as the *Default Setting*

The second foundational principle of *Privacy by Design* is "**Privacy as the *Default Setting***." This means that you'll be seeking to provide privacy assurances by delivering the maximum degree of privacy. To do so, you'll ensure that personal data are automatically protected in any given IT system or business practice used to create your smart grid app. No action should be required on the part of the energy customer to protect their privacy – it should be built into the system, automatically – by default. This is important because in most cases the default setting is the condition that will prevail. User privacy can thus be greatly affected simply by designing privacy-friendly default settings. Keep in mind though, that even when you have permission from the user to access their data, you should still ensure its proper and limited handling. Apps must be designed so that they collect information fairly, lawfully, and limited to that which is necessary for specified purposes of your app. It does not hurt to take the extra step of getting consent for information that the user might consider sensitive, such as financial, medical, political views, sexual preference, etc. Avoid using mobile device identifiers as the default – allow the individual to reset their identifier, much in the way that users can delete cookies. You should also be aware that Smart Grid applications made available in the U.S. could fall under "Do Not Track" initiatives.

3. Privacy *Embedded* into Design

Aim to embed privacy requirements into the design and architecture of IT systems and business practices. This avoids having to bolt them as add-ons, after the fact, when in many cases it is too late to effectively protect privacy. Pinpoint the core functionality of your app – privacy should be an essential component. The **Privacy *Embedded* into Design** principle will result in your Smart Grid app avoiding any unexpected and unnecessary uses of personal information. High profile examples exist of apps that unnecessarily collected or disclosed mobile phone contacts, text messages, photos and videos, and geo-location for various secondary purposes such as advertising. E.g. A "find friends" feature should not send a user's friends' contact information to third parties. Your Smart Grid app should also automatically limit the linking of additional data with personal information, and un-link when no longer required.

Before downloading your Smart Grid app, the user must have the opportunity to read your privacy policy and terms of use.[22] Your information practices must be clear. Also, it must be obvious what access rights the user is granting to hardware components and other software already installed on their computer or device. Information must be provided on how to de-install the app. When seeking consent for potentially problematic functions, such as use of location data, geo-tagging photos, or

[21] American Institute of Certified Public Accountants (AICPA), and Canadian Institute of Chartered Accountants (CICA). "AICPA/CICA Privacy Maturity Model Based on Generally Accepted Privacy Principles." http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/docs/item48094.pdf.

[22] One-Click App Installation May Not Be Enough to Amount to Personal Data Processing Consent." *Out-Law News*, March 15, 2013.

automatic information sharing, design the app so that you are getting consent first. Specifically ask consent for each feature and do not bury the consent for the feature in a privacy policy or terms of service.

Be careful if you are accepting software tools to build your Smart Grid app, or to facilitate coding meant to include advertising or analytics in the app. These tools are sometimes created by advertising networks, and could work against your goal of embedding privacy if the code created sends information back to the ad network without the user's permission or knowledge.[23]

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

The principle of **Full Functionality – *Positive-Sum*, not Zero-Sum** seeks to accommodate legitimate interests and objectives in a positive-sum, 'win-win' manner, not through a zero-sum (win/lose) approach, where unnecessary trade-offs to privacy are made. Avoid the pretense of false dichotomies, such as privacy vs. security – to demonstrate that it is possible to have both. In designing your Smart Grid app, an aspect of full functionality would be to allow for the collection of limited personal information tied to specific purposes, but also, to allow users to manage the information they have shared in an easy-to-find and understandable interface. Also, this principle addresses the enormous research potential of data on the Smart Grid, including how individuals use applications to save energy. Full functionality in that case would allow innovative research to be done on de-identified data. There are innovative ways to derive useful information from such data sets, even if the information cannot be linked back to an individual.[24]

5. End-to-End Security – *Full Lifecycle Protection*

Security is a key aspect of privacy. The principle of **End-to-End Security – *Full Lifecycle Protection*** ensures cradle-to-grave, lifecycle management of information, end-to-end, so that at the conclusion of the process, all data are securely destroyed, in a timely fashion.Consider yourselves the custodians of the personal information your Smart Grid app collects with a duty of care to protect it end-to-end.

Implement security practices, and clearly document them to restrict access to personal information. Restrict access to only those applications or individuals with a business need to have access. Protect personal information from loss, limit retention of personal information, and allow individuals to revoke access to their personal information. When an individual deletes their account, *delete it*, do not retain it. If that is not possible (e.g. due to legal requirements), then explain the retention up front before the user downloads your Smart Grid app.

All data held should be periodically assessed to determine the necessity of retaining each data element in consideration of the purposes for which it was collected, with destruction or anonymization occurring as necessary. Have a retention schedule, and when data is no longer needed, securely destroy it. Try embedding into data one or more expiry conditions so that following a defined use, or specific time limit, the data would be no longer accessible to you as the Smart Grid app provider. Any downstream uses of de-identified data must require that there not be attempts to re-identify the information.

[23] Federal Trade Commission Staff Report. "Mobile Privacy Disclosures: Building Trust through Transparency." 2013, p. 24.

[24] See, for example, the De-identification Centre. http://www.privacybydesign.ca/index.php/de-identification-centre.

Excellent advice exists on how to ensure security of personal information that can be applied to your Smart Grid app.[25] Important security tools include: encryption, de-identification, and user authentication. Protect data in transit by encrypting all communications to your server (SSL/TLS). Protect data at rest by encrypting stored data, especially any information used for authentication such as username, password, and e-mail. Test and update the security of your app before and after you collect personal information.[26]

6. *Visibility* and *Transparency* – Keep it *Open*

This principle involves assuring stakeholders that whatever the business practice or technology involved regarding your Smart Grid app, it is, in fact, transparent to the user, and operating according to the stated promises and objectives, subject to independent verification. When we say "stakeholders," that includes everyone from the user, to partners you would like to work with, or even investors. Your stakeholders can trust you, but ultimately they will want to verify that your assurances hold up to scrutiny. Remember, trust but verify.

Employ the ***Visibility* and *Transparency* – Keep it *Open*** principle regarding your privacy policy. Your policy will already make the user aware of how their personal information will be collected, used, disclosed, etc., and how it will be deleted or anonymized, as well as when and under what circumstances it could be transferred to other data processors or service providers. Once your privacy policy is set, you must then proactively monitor your Smart Grid app to make sure it is behaving in the manner in which you have described it in your privacy policy.

Develop a mechanism for the user to verify statements in the privacy policy. For example, the user should be able to view, review, and control their personal information. Users should be able to see at all times the information they have provided, or other information you have collected or created about them, or disclosed to third parties. Users should have the ability to modify or delete data, especially in the case of information being sent to third party ad networks. This process should not be complicated. Find ways to engage users simply and quickly in the control of their data (e.g. using universal privacy icons[27]).

7. *Respect* for User Privacy – Keep it *User-Centric*

Keep the interests of the individual uppermost when designing your Smart Grid app by offering measures such as strong privacy defaults, appropriate notice and empowering user-friendly options. Ask yourself, 'would the user assume their information would be collected in this context'. Based on this assessment, build into the app points at which you ask permission, and give notice, regarding the collection, use and disclosure of personal information. Build as many controls, options and choices in this way, and encapsulate them within your privacy policy so that the user can read about their choices all in one place.

[25] E.g. Federal Trade Commission BCP Business Center. "Mobile App Developers: Start with Security." 2013; Electronic Frontier Foundation. "Mobile User Privacy Bill of Rights." 2012.

[26] Harriet Pearson, Mark Brennan. "A Duty to Patch? FTC Settles First Case against a Mobile Device " *Hogan Lovells Chronicle of Data Protection*, February 25, 2013.

[27] E.g. see http://www.azarask.in/blog/post/privacy-icons/, https://wiki.mozilla.org/Privacy_Icons.

In your privacy policy, do not misstate your practices in any way. Not only is it disrespectful to the user, it could also get you in trouble with regulators. The same applies if your practices change; you must notify the user and give them the chance to choose whether to continue with your service. When updating your policy to more accurately reflect changes your practices, tell the user exactly what has changed and do not make them read your policy line by line to find the changes. Explore the possibility of using short form notices with a link to the longer policy.[28] Also, provide such updates prior to the change occurring. It almost goes without saying that silent app changes that diminish privacy are very disrespectful to the user.

It's important to keep in mind that there are apps emerging that can track data being sent from a user's phone or computer (e.g. www.appinformant.com, www.cluefulapp.com), so Smart Grid app developers may have no choice but to respect user privacy by being upfront about information practices. In addition there are app privacy rating tools that are allowing users to become better informed prior to downloading an application.[29] As a result, you may wish to get your app privacy certified by a reputable third party as a competitive advantage.

[28] See, for example, TRUSTe's "Free Privacy Policy for Mobile Apps" with layered privacy notice. http://www.truste.com/free-mobile-privacy-policy.

[29] See http://privacyscore.com. See also Byron Acohido. "Blackberry's New Privacy Alerts Vet Invasive Apps." USA TODAY, February 5, 2013; David Canton. "People Are More Likely to Install Apps That Respect Their Privacy." *QMI Agency*, November 11, 2012.

Conclusion

Let us end by going full circle – being reminded of the intended vision of the Smart Grid – to have greater energy efficiency through a more efficient electrical grid. It is widely acknowledged that this cannot occur without information from energy consumers, such as through smart meter data, which forms the basis of widespread smart metering infrastructure investments.

However, smart meters are on par with another essential element for the creation of a Smart Grid – privacy, which ensures consumer participation in the Smart Grid. Consumers must trust that the privacy of their smart meter data and other personal information will be strongly respected. If not, consumers may not participate in energy saving programs, or purchase smart appliances, or download Smart Grid apps, etc. When trust is broken, it is difficult if not impossible to regain it. Studies show that when a customer is offended by a particular experience, any chance of doing future business with them goes down at that moment, even if the consumer completes the transaction.

As an entrepreneur or established business developing a smart grid app, you may be struggling with choices based on how they affect your business in the short-term versus long-term. This is a common dilemma in the business world. However, being an entrepreneur in the Smart Grid is unique. If you build privacy in at the outset, not only will you gain a competitive advantage today, you will grow consumer trust in the Smart Grid itself, to ensure long-term consumer participation. In other words, incorporating *Privacy by Design* will ensure the foundation of your market base for years to come.

In this paper, we have sought to reach out to smart grid app developers by providing a primer on *Privacy by Design*, recognized as an international standard since 2010. We hope that the information provided will serve you, even if you are a one-person operation. By employing the principles we discussed in this paper, not only will your customers thank you and repay you with their business, but you will also stand out as an early adopter – leading with privacy in Smart Grid apps – by design.

About the Organizations

Information and Privacy Commissioner
Ontario, Canada

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

Quinzee

Quinzee is a web and mobile application that helps consumers track and compare their energy use. Using social benchmarking as a motivator for influencing efficient energy choices and behaviours, Quinzee is a customer engagement and communication platform for electricity utilities and other organizations that wish to encourage efficient home energy management. Quinzee was developed by Environmental Data Analytics & Communications Inc. (EDAC), a Canadian Software-as-a-Service company with specific experience in energy data analytics and communications across web-enabled platforms. EDAC's mission is to enable intelligent consumer decisions to better manage our planet's resources. EDAC believes that changes in individual choices have a significant impact on resource use, and given the right tools smarter and environmentally friendlier choices can become the norm, for all of our benefit.

Appendix A – list of resources on privacy and software app development

There are many excellent publications relevant to privacy and application development (some are listed here).

Cavoukian, Ann. "Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices." Office of the Information and Privacy Commissioner, Ontario, Canada, 2007.

———. "Mobile near Field Communications (NFC) "Tap 'N Go" – Keep It Secure and Private." Office of the Information and Privacy Commissioner Ontario, Canada 2011.

———. "Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes." Office of the Information and Privacy Commissioner, Ontario, Canada, 2011.

Cavoukian, Ann, and Marilyn Prosch. "The Roadmap for *Privacy by Design* in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users." Office of the Information & Privacy Commissioner of Ontario, 2010.

CTIA. "Best Practices and Guidelines for Location-Based Services." 2010.

Electronic Frontier Foundation. "Mobile User Privacy Bill of Rights." 2012.

Federal Trade Commission BCP Business Center. "Mobile App Developers: Start with Security." 2013.

Federal Trade Commission Staff Report. "Mobile Privacy Disclosures: Building Trust through Transparency." 2013.

Future of Privacy Forum, and Center for Democracy & Technology. "Best Practices for Mobile Application Developers."

GSMA. "Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development."

———. "Mobile Privacy Principles."

International Working Group on Data Protection in Telecommunications. "Working Paper on Mobile Processing of Personal Data and Security." Berlin, Germany, September 7, 2010.

MEF. "Privacy in Mobile Applications Initiative." 2013.

Microsoft. "Privacy Guidelines for Developing Software Products and Services." September, 2008.

National Telecommunications & Information Administration, U.S. Department of Commerce. "Privacy Multistakeholder Process: Mobile Application Transparency Code of Conduct." 2013.

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner of British Columbia. "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps." 2012.

TRUSTe. "5 Privacy Tips for Mobile App Developers." (2011).

W3C Working Group. "W3C Working Group Note 03 July 2012: Web Application Privacy Best Practices." 2012.

Appendix B – IPC Smart Grid publications

Cavoukian, Ann, Jules Polonetsky, and Christopher Wolf. "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation," 2009.

Office of the Information and Privacy Commissioner of Ontario, Hydro One, and Toronto Hydro Corporation. "*Privacy by Design*: Achieving the Gold Standard in Data Protection for the Smart Grid," 2010.

Office of the Information and Privacy Commissioner of Ontario, Hydro One, GE, IBM, and TELVENT. "Operationalizing *Privacy by Design*: The Ontario Smart Grid Case Study," 2011.

Cavoukian, Ann, Jules Polonetsky. "*Privacy by Design* and Third Party Access to Customer Energy Usage Data," 2013.

Office of the Information and Privacy Commissioner of Ontario. "F.A.Q. – Smart Grid Privacy – from Smart Meters to the Future," 2010.

Office of the Information and Privacy Commissioner of Ontario. "Shaping Privacy on the Smart Grid – You Can Make a Difference: A Roadmap for Data Protection Commissioners and Privacy Regulators," 2010.

www.privacybydesign.ca

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
Email: info@ipc.on.ca

Quinzee
632 College St., Suite 300
Toronto, Ontario
Canada M6G 1B4
Telephone: (416) 727-7081
Email: contact@quinzee.ca
Web: www.quinzee.ca

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

August 2013

Privacy by Design: www.privacybydesign.ca

Information and Privacy Commissioner,
Ontario, Canada

Quinzee