



Automation Insight.

December 2009.

Privacy and the smart grid: A quagmire of questions vexes the industry

By Will McNamara



As exciting and promising as the smart grid revolution is proving to be, along with it comes an array of questions and concerns about protecting the privacy of consumer energy data, assuming of course that there can ultimately be agreement on what

data should be considered private. Put another way, a major part of the challenge in determining how to secure advanced metering infrastructure (AMI) / smart grid infrastructure is determining what aspects need to be made secure, including consumer data. The argument over what data should be considered “private” and what data should be considered “utility property” undoubtedly will continue to polarize stakeholders.

The debate over consumer privacy is pertinent regardless of how extensively a utility plans to remodel its infrastructure. Even without full smart grid deployment, privacy is still a consideration whenever existing meters are replaced with smart meters. The core purpose of AMI is to collect information related to a particular household or business. As the evolution to smart meters progresses, the kind of information that can and will be collected becomes more granular. In general, meters already can collect a unique meter identifier, timestamp, usage data, and time synchronization every 15 to 60 minutes. Smart

meters, generally speaking, can also collect outage, voltage, phase, and frequency data, along with detailed status and diagnostic information from networked sensors and smart appliances. When analyzed, this data offers insights as to whether people were present at a specific location, when they were present, and what they were doing (how they were consuming power).¹

While related, cyber security and privacy issues generally are being addressed separately by stakeholders who have a role in policymaking. The industry hears a great deal about cyber security and protecting AMI / smart grid infrastructure from hackers attempting to wreak havoc on industry infrastructure in a wide-scale fashion. We refer to this as a national security issue, which indeed it is.

However, also concerning, but not as often discussed, is the issue of consumer privacy—keeping personal information in the hands of the consumer, and away from utilities, advertisers, third parties, or entities that might use such consumer data for criminal means (i.e., identity theft). In fact, privacy concerns seem to be taking a back seat to security concerns for the smart grid. A recent report from the National Institute for Standards and Technology (NIST) Smart Grid group concluded that most utilities are lacking privacy policies and state public utility commissions have not done much to enact formal policy guidelines for the smart grid. In the absence of state public utility commission (PUC) mandates, the onus to develop policy standards likely will fall on utilities themselves, who might be reticent to act on this issue until forced to do so.

Due to the lack of policymaking on the state level, where arguably it is best placed due to what is typically

¹ Mark Foley. “The Dangers of Meter Data (Part 1).” Smart-Grid News.com Jun 2, 2008

state PUC oversight over utilities, the privacy debate is mostly taking place on the federal level. Although obviously unanticipated in the era it was written, the U.S. Bill of Rights included language that is now the basis for the privacy debate permeating smart grid deployment. In fact, privacy of the home was considered such an important value in our society that its protection was guaranteed under the Bill of Rights with the following language: “The right of the people to be secure in their ... houses ... shall not be violated.” This language is now being interpreted by privacy advocates to lobby for increased protections against the consumer data that would be increasingly collected and analyzed via smart meters and other smart grid technologies.

Without question, policymaking on consumer privacy and cyber security has an urgency associated with it. Deployment of smart grid technology across the country continues to advance forward. Most estimates suggest that more than 50 million smart meters will be deployed in the U.S. alone by 2015, adding to the more than 8 million that already have been deployed. Meanwhile, privacy issues—along with the larger subject of cyber security—are being vetted with only incremental resolution, raising a red flag among some observers that a number of significant problems loom on the horizon. With meters and smart grid technologies being deployed, internet attacks, malware, and privacy breaches have become a bigger risk when the appropriate defenses are not engineered into the system from inception.

Recent examples validate these concerns. Just last month, reports surfaced that 179,000 e-billing accounts of Toronto Hydro customers had been illegally accessed. Customer information that was “taken” included names, addresses, customer account numbers, and some billing information, all of which can be valuable material for identity theft offenders. At this point, while Toronto Hydro was quick to launch an investigation, the origin of the breach is still unknown. “Nobody knows if it was a rogue employee or somebody else. It’s a big question mark,” Ann Cavoukian, Ontario’s information and privacy commissioner, said in an interview. Cavoukian added that the situation at Toronto Hydro is a wake-up call for other utilities that need to modernize their networks and keep a constant eye toward safeguarding their customers.²

In a report developed in response to the security breach, Cavoukian also stated, “The 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.” And the report also reiterated that the kinds of information that will be made available is likely to change as well. “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 of occupants, when they are present, as well as when they are awake or asleep. For many, this will resonate as a ‘sanctity of the home’ issue, where such intimate details of daily life should not be accessible.”²

Further, as Jules Polonetsky, co-author of the Ontario report, wrote, “The success of the smart grid will be completely dependent on consumers trusting that their data is being handled responsibly. If companies do not get privacy right from the start, billions will have been spent in vain.” The report says that the utility industry needs several key initiatives, including: “privacy laws, regulation and independent oversight; accountability and transparency; audit and assessment; market forces, education and awareness; data security; and fair information practices.”²

We have not seen a similar security breach involving consumer data on the scale of Toronto Hydro occur here in the United States, as of yet, but some might argue that such an occurrence is inevitable. Certainly it is clear that the U.S. government has made cyber security a priority. In the first round of federal stimulus funding applications under FOA 58, the deadline of which occurred in August, the Department of Energy (DOE) included a provision specifically requiring utilities to outline how they will address cyber security in their smart grid projects. If a utility did not include a cyber security plan as part of its funding application, the DOE reserved the right to reject that application. In addition, the NIST and its member groups, including the Institute of Electrical and Electronic Engineers (IEEE), are working to even the playing field by making all technology, devices and systems involved in the grid interoperable, which theoretically would include greater safeguards against external hackers who seek to access consumer data.

² “Smart grid saves power, but can it thwart hackers?” August 3, 2009. The Toronto Star

Also on the federal level, the Cyber-Security Act of 2009 (S. 773) remains the most controversial technology-related legislation before the current Congress. Introduced by Senators Jay Rockefeller, D-West Virginia, and Olympia Snowe, R-Maine, in April and redrafted late this summer, the bill would create a national cyber security adviser under the authority of the president to coordinate cyber security efforts. Rockefeller and Snowe drafted the legislation in response to years of post-9/11 complaints that neither the private sector nor government officials were doing enough to adequately protect the nation's critical cyber infrastructure.

The bill has yet to be the subject of a full Congress debate or vote. However, provisions of the bill have been interpreted as an attempt to extend government surveillance allowed under the Electronic Communications Privacy Act (ECPA) and the Privacy Act of 1974. Privacy advocates and some industry associations have expressed concern about a provision in the bill that would allow access to "relevant data" of private sector information systems and preempt all other laws.

The Scope of Customer Data

The scope of personal data that falls under the discussion of privacy is significant, given that "personal information" refers to any recorded information about an identifiable individual. In addition to the more standard information that one would expect to already be submitted to a utility (e.g., customer name, contact information, and perhaps bank account data), other information about individual preferences, transactional history, record of activities or travels increasingly holds value for third parties that may want to leverage that information for sales of services or other activities.

At present, there are essentially three sources of consumer data that are the focus of privacy policymaking:

- **Smart meters:** 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. The data may be sent to the utility provider either over the wires or wirelessly.
- **Smart appliances:** Smart appliances generally include thermostats, clothes washers and dryers, microwaves, hot water heaters and refrigerators. They may be configured by the end-user to communicate information directly to the utility operator

for efficient and more productive use of electricity. Such appliances could be equipped with a device that communicates with a facility's energy management system to adjust temperature controls based on energy prices.

- **Dynamic pricing:** Dynamic pricing 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. Time of use pricing (TOU), critical peak pricing (CPP), and real-time pricing (RTP) structures are the more common forms of dynamic pricing. How customers participate in such pricing programs, and respond to the pricing signals offered to them, represent valuable data.

The increase of data associated from the above areas creates enhanced value for all stakeholders, including consumers, utilities, and third parties, selling an array of services. However, the increase of data also increases the potential for misuse and / or criminal activity that leverages such information. Recent discussions of the greatest potential threats associated with consumer data have focused on the following areas:³

1. identity theft
2. determining personal behavior patterns
3. determining specific appliances used
4. performing real-time surveillance
5. revealing activities through residual data
6. targeted home invasions
7. providing accidental invasions
8. activity censorship
9. decisions and actions based upon inaccurate data
10. revealing activities when used with data from other utilities.

Within the electric power sector, any of the problems currently associated with other online services could potentially pose problems for utilities, including such issues as poor password protection, unsolicited marketing directly to end-users, etc.

The Value of Customer Data

A fair question is why consumers should be concerned about the release or distribution of their personal infor-

³ Rebecca Herold, privacy expert, is attributed with identifying these areas of concerns. <http://www.privacyguidance.com/myblog.html>

mation. In the age of technology, so much of personal data is now transmitted online that some may question

why the data associated with energy consumption even rises to the level of a national debate. The most common response is that, while smart grid technology improves network management and efficiencies, the data around consumer electric usage patterns have the potential to do far more. For example, marketing firms may find valuable market penetration data in consumer electric usage patterns, and law enforcement could use information about electricity usage to pinpoint potential sites of criminal activity.

The privacy concerns that exist around the smart grid sector can vary greatly depending on the type of technology that is deployed. In his testimony before the Colorado Public Utilities Commission, Elias Quinn, a representative of the Colorado Law School's Center for Energy and Environmental Security, referred to how "smart grid and smart metering will open up an unprecedented library of information in the home, potentially down to the brand name and make of an appliance. Consumers tied into smart grid should be aware of what they're getting into."⁴ Potentially, smart grid information could be used to find out when homeowners are away or security systems are on or off, he said. Nevertheless, wherever technology is utilized that targets individual consumers, there is invariably a dramatic increase in the amount of personally identifiable information that is collected and stored, leading to very real concerns regarding privacy.

Companies such as Google, IBM and Microsoft, along with technology and software firms like Comverge, Tendril, GridPoint and others, stand to gain from clear rules on who can provide them with access to customer usage data. But those rules are made on a state-by-state basis for investor-owned utilities, and some states have not addressed such issues.

Other businesses, some that are not even presently identified, will also be interested in AMI data. System sensors, smart appliances, sophisticated signal analysis techniques on voltage and current wave forms, unusual power consumption, or duty cycle characteristics could reveal information about the presence, absence, or use of systems as small as hair dryers, waterbeds, and indi-

vidual burners on a stove. Such data make it possible to monitor changes in the operating signature of individual appliances and therefore, to predict their loss of efficiency or imminent failure. As a result, appliance manufacturers may want AMI data to learn about how their products are actually operated. Retailers of appliances, extended warranties, or repair services may want AMI data to provide advertising or discount offers days or hours before an appliance fails. Insurers may want to look for evidence of unauthorized conduct, to determine when a loss occurred, or to deduce who was present.⁴

Going Forward

The privacy debate cannot and will not be resolved any time soon. Technology is changing too quickly—there is uncertainty regarding state versus federal jurisdiction, and the fundamental question of who "owns" consumer data has no easy answer. All of these factors indicate that the agreement on the privacy discussion will not be easy to achieve. However, meanwhile, as AMI / smart grid deployments continue, there are immediate steps that utilities, technology vendors, and other participants in the sector can take and will likely be encouraged to take.

For instance, it is likely that technology vendors will be pushed to consider privacy safeguards as they develop smart appliances with strict adherence to Section 5 of the Federal Trade Commission Act, which requires companies to maintain privacy policies and engage in fair privacy practices—such as providing notice to end-users regarding the personal information that will be collected or shared, and allowing end-users the option of blocking the distribution of such information. Up to this point, it has arguably been the case that technology vendors have been unregulated with respect to incorporating privacy safeguards into their AMI solutions. In addition to taking into account existing laws, companies that develop smart grid technology would be wise to anticipate consumer reaction to privacy impacting systems and features, and the policies and laws that continue to develop in this area. At a minimum, companies developing smart grid processes and devices should consider how to provide consumers notice about what information is collected from and about their homes and households, who is getting the information, and for what purposes the information will be used.

From the utility standpoint, it is anticipated that utilities will be encouraged to develop clear policies regarding

⁴ Ethan Howland. "Colorado regulators eye privacy issues of creating a 'smart' electricity grid." September 14, 2009. Inside Energy

if or how they will share information they obtain about customers with third parties. In the absence of clear state guidelines that would impact all utilities within a particular state (given the inherent PUC regulation), these policies could vary from utility to utility. When new customers sign on to utility service or are the recipient of a new smart device, it is likely to be an imminent requirement that utilities disclose their intention with regard to customer data. Furthermore, in general, most utilities provide an “opt out” option to customers, meaning that an end-user must take action if they wish to prevent the utility from accessing their data that is not essential to the utility’s ability to provide service. However, without exercising this opt out option, such information would be fair game and generally considered the property of the utility as being necessary to operate its system and provide service to the customer.

Questions To Be Addressed

The Federal Communications Commission (FCC) recently published a request for public input, presumably desiring input from utilities specifically, regarding how demand response deployments will use real-time data and how access to that data is being developed and protected. Questions on where the FCC is seeking input include:

- In current smart meter deployments, what percentage of customers have access to real-time consumption and/or pricing data? How is this access provided?
- How should third-party application developers and device makers use this data? How can strong privacy and security requirements be satisfied without stifling innovation?
- What are the implications of opening real-time consumption data to consumers and the energy management devices and applications they choose to connect?
- Which types of devices (e.g., appliances, thermostats, and energy displays, etc.) will be connected to smart meters? What types of networking technologies will be used? What type of data will be shared between smart meters and devices?
- Which types of devices (e.g., appliances, thermostats, and energy displays, etc.) will be connected to the internet? What types of networking technolo-

gies will be used? What type of data will be shared between these devices and the internet?

- Should detailed electricity usage information be protected? If so, how?
- How do constitutional or statutory protections impact the use of consumers’ detailed electricity usage information collected as part of smart grid initiatives? What protections should be put in place even if they are not covered by constitutional or statutory provisions?
- What are the necessary components of effective privacy regulation of consumer electricity usage patterns? For example, should disclosure of consumer information to third-parties be on an opt-in or an opt-out basis, or should the consent requirement depend on the nature of the party receiving the information?
- How much information about consumer electricity usage do electric utilities and “edge service providers” require to facilitate more efficient network management, load forecasting, asset management, bill control, demand side load management, efficiency consulting, energy savings contracting, etc.?
- How do privacy regulations affect electric utilities and “edge service providers” in their efforts to provide enhanced electricity management services?
- Who “owns” customer information?
- What should be a utility’s obligation to “unbundle” metering in homes and businesses?

Contact the author at will.mcnamara@kema.com.

About Automation Insight

Automation Insight is a complimentary monthly publication written specifically for the utility industry and those serving the utility industry.

To join the Automation Insight distribution list, or to share your comments, ideas and suggestions for this and future issues, please e-mail automation.insight@kema.com.

www.kema.com/automation_insight