THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP/US
July-August 2012 • Volume 12 • Number 6

Smart grid technology: Privacy and data security issues

By Walter Delacruz, CIPP/US

The adoption of smart grid technology into sustainable building property management strategy requires meaningful planning for the secure treatment of captured enriched data. Captured enriched data is consumer electricity use information that may also include proprietary business information related to a business's energy consumption. The problem is that this data could be a target for unauthorized exploitation by marketers and other third parties and for data breaches by criminals. As shall be further discussed below, queries and complaints raised by consumers may underscore the need for substantial due diligence and consumer education in connection with the implementation of smart grid technology.

Smart grid technology significantly improves the ability of electric utility companies to upgrade the efficiency of their infrastructure. Digital wireless devices allow the automated collection of detailed measurements of a customer's electric usage within their premises and allow two-way communication of such information between the digital meter and the utility on a regular or constant basis.

The benefits of such technology to both the energy supplier and user include more exact measurement of usage--by time of day and by appliance--and better demand forecasting, which allows for the more efficient management of power distribution. System health and outage reporting are enhanced by automated trouble ticketing processes. Proponents further point to increased power reliability and enriched consumer choices regarding consumption; e.g., energy consumers could elect to run electricity intensive activities or processes during non-peak hours as a cost savings measure. In many cases, if a building is certified or needs to comply with local law energy use reduction initiatives, this technology will facilitate certification and compliance requirements.

However, notwithstanding the perceived benefits, well-advised landlords and building managers alike should be aware of potential problems including those related to privacy that may arise with any smart grid implementation program.

The privacy implications of smart grid technology have begun to attract the attention of regulators in the U.S. and other jurisdictions. The public utility service commissions of California, Colorado, Connecticut, Maryland, Ohio and Vermont have begun to examine the privacy implications of smart grid technology in order to formulate proposed rules. On March 9, 2012, the European Commission published a recommendation regarding the implementation of smart metering systems in the European Union including specifications for common minimum functionalities and data protection and security requirements. Many of the concerns raised by the

implementation of this technology appear in a case filed recently in Illinois (See *Naperville Smart Meter Awareness v. City of Naperville,* No.1:11-cv-09299, N.D. Ill. filed Dec. 30, 2011). Complaint filed on December 30, 2011, amended complaint filed on March 27, 2012. In *Naperville,* the complaint filed by the 501(c) 6 not-for-profit corporation Naperville Smart Meter Awareness (NMSA) sought to enjoin the defendant City of Naperville from implementing the city's smart grid technology initiative.

Prior to NMSA's filing of the lawsuit, the city had begun to implement its smart grid initiative, which was funded in part by a grant provided by the U.S. Department of Energy under the American Recovery and Reinvestment Act of 2009. The city's system comprised 57,000 smart meters to be located within customers' homes linked to a wireless RF communications network including repeaters on utility poles, which communicated ultimately to the utility company.

NMSA claims that numerous health, safety, security and privacy concerns, the violation of due process and the prohibition against unlawful search and seizure under the Fourth, Fifth and Fourteenth Amendments to the United States Constitution preclude the city from lawfully implementing its program. NMSA's court papers cite radio frequency health hazards, the failure of the city to provide information regarding a cybersecurity plan regarding collected data and failure of the city to observe the Illinois Open Meeting Act as fatal defects in the city's plan. While this case is being decided, it may be useful to focus on ways to successfully implement a smart grid initiative program that addresses the issues raised in the litigation so that landlords and property managers do not face claims against them for illegal tenant data disclosure.

What should happen before any proposed implementation of a smart grid technology program?

To successfully implement a smart grid initiative program and minimize privacy and data security concerns, landlords and property management companies need to know the answers to a number of privacy and data security related questions. These questions include:

- What kinds of data are being captured?
- How and where are the data being stored?
- Are third parties involved in the storage, use or analysis of data?
- What kind of data security program does the utility have in place?
- What are the restrictions on the use of data by third parties?
- What record retention and data deletion policies apply regarding the data?

Consumers, businesses and regulators can be expected to ask the questions identified above and raise other privacy and data security issues reasonably related to smart grid technology and the collection and use of captured enriched data. As of this writing, the *Naperville* case has not yet been decided. However, given the issues raised by the case, planning for the use of smart grid technology will require thoughtful review and preparation.

Walter Delacruz, CIPP/US, is of counsel in Moses & Singer LLP's Intellectual Property, Global Outsourcing and Procurement, Privacy and Cybersecurity and Advertising practices. Prior to joining Moses & Singer in 2007, he worked in New York City government in technology and telecommunications positions for Mayors Koch, Dinkins and Giuliani. He is the author of numerous articles, including several recent pieces on cloud computing and cybersecurity. He also serves as Chairman of the Board of Directors at the Ryan Chelsea Clinton Community Health Center and is a member of the Wall Street Technology Association.

MOSES & SINGER LLP

Disclaimer

Viewing this or contacting Moses & Singer LLP does not create an attorney-client relationship.

This is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.