Regulation and Competition

Smart Grids and Privacy

Christopher WOLF & Winston MAXWELL
Hogan & Hartson LLP, based (respectively) in Washington and Paris

Smart Grid systems increase the connectivity, automation and coordination of energy transmission and distribution between suppliers and networks, and consumers. Smart Grid technology can expand energy efficiency into the home by monitoring consumers' energy usage in real time and communicating with household devices that respond to demands to shut off during periods of non-use (e.g., during the work day, when businesses require more power resources), allowing individual consumers to control their electricity usage more effectively. Smart Grids are not unlike NGN (next generation networks) in the field of electronic communications. They represent a fundamental shift from the era of "dumb pipes" to that of "smart pipes" and the "Internet of things." The FCC sought comment on September 4, 2009 on the challenges associated with Smart Grid systems [1], asking (among other things) about how privacy aspects should be addressed.

Smart Grid systems can hugely increase energy efficiency. But the opportunities and benefits of developing Smart Grid systems also come with potential privacy risks. One contributor to the National Institute of Standards and Technology's ("NIST's") Smart Grid Cyber Security Strategy and Requirements Interagency Report (U.S.) has identified ten potential data

[1] http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2017A1.pdf

privacy concerns that should be addressed in developing Smart Grid technology standards [2]. These privacy concerns are as follows:

- Identity Theft
- Determine Personal Behavior Patterns
- Determine Specific Appliances Used
- Perform Real-Time Surveillance
- Reveal Activities through Residual Data
- Target Home Invasions
- Provide Accidental Invasions
- Activity Censorship
- Decisions and Actions Based upon Inaccurate Data
- Reveal Activities when Used with Data from Other Utilities

Clearly, a significant amount of consumer data can be obtained through Smart Grid technology. There are numerous potential users of the data, including utility companies, smart appliance manufacturers, and third parties that may want the data for further consumer interactions. Moreover, data that can be collected through Smart Meters and integrated home networks and appliances has significant value. For example, Smart Grid systems may incorporate advanced broadband and data flow metering functionality, which can collect information about how much electricity an individual uses, which rooms he or she uses most, when, and how often. Armed with this data, utility companies will be able to manage load requirements better and create a more efficient electricity distribution system. In addition, device manufacturers will be able to understand better how their devices are used, allowing them to serve their customers better. These Smart Grid features, however, raise questions about which entities will have access to individual user data and whether individual devices may be identified or tracked.

Potential Smart Grid data users, including utility companies and device manufacturers, must engage in responsible data management practices that build consumer confidence and trust.

---

[2] See "SmartGrid Privacy Concerns", at: http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf (last accessed Oct. 1, 2009).

They must recognize that they have an ongoing relationship with consumers and that continued trust from consumers is critical to maintaining that relationship and to growing the Smart Grid ecosystem. Such trust can only be achieved if consumers feel that they are receiving sufficient information about and are in control of how their personal Smart Grid data is used. Thus, Smart Grid data users must consider carefully how they will protect the integrity, privacy, and security of the Smart Grid data obtained from consumer usage patterns, and the data collected must not be excessive. In addition, Smart Grid data must be gathered responsibly, securely, and with a measure of transparency and consumer control. These principles are well known in Europe, and will be applied to (among other things) RFID systems [3] and the Internet of things.

Only if consumers have confidence about how their data is used will there be the critical growth in Smart Grid technologies. An individual consumer must be assured that information about his or her behavioral habits will be secure and used only for the purposes understood and agreed to by that consumer. In addition, the consumer must be fully aware of how the data is used and must be confident that the data is protected from improper use or dissemination. If these requirements are met, consumers will be more likely to embrace advanced Smart Grid technologies. These are also prerequisites to Smart Grid systems being compliant with European data protection laws. Without such responsible data management practices, however, there will likely be consumer resistance to Smart Grid technologies and a loss of consumer trust that could hinder Smart Grid deployment efforts, leading to lower demand for new products and reduced innovation as device manufacturers exit the Smart Grid ecosystem.

To date, regulators and device manufacturers have been clear that it is consumers who own the data to be disseminated from technologies along the Smart Grid and that those consumers must be asked for permission for any unexpected types of data use or sharing. Indeed, some parallels can be seen between data on electricity usage and traffic data in electronic communications networks, which are subject to special rules under the ePrivacy Directive [4]. However, requesting permission for data use and even communicating data management policies to users can be challenging. There needs to be research to determine how best to convey information to

[3] See, eg., the European Commission's recommendation regarding RFID systems: http://www.statewatch.org/news/2009/may/eu-com-rfid-3200-2009.pdf

[4] Directive 2002/58/EC.

users regarding the privacy decisions they will make in incorporating Smart Grid technologies into their homes and lives, and the right balance between "opt-in" and "opt-out." Utilities and manufacturers should integrate the principles of Privacy by Design, a concept pioneered by Ontario Privacy Commissioner Ann Cavoukian, into the construction of their data infrastructures. These principles can ensure that key privacy concerns are taken into account before millions of dollars are spent and before Smart Grid technologies are deployed.

Regulators should encourage positive practices by highlighting the need for strong privacy requirements for the use of Smart Grid data. They should also encourage all Smart Grid stakeholders, including utility companies, device manufacturers, consumer groups, and privacy advocates, to develop best practices for maintaining appropriate privacy and data security controls and providing consumers with sufficient control over and transparency in the collection and use of Smart Grid data. All Smart Grid data use must be conducted with privacy and security principles firmly entrenched. In Europe, some consideration should be given to how the treatment Smart Grid data and traffic data in electronic communications networks should differ, or on the contrary should be harmonized, in order to create a single coherent set of principles for so-called "smart pipes."

Conclusion

As explained by NIST in the United States, data privacy is the "Achilles' Heel" of the Smart Grid [5]. Although Smart Grid technologies may bring substantial consumer and energy efficiency benefits, they also raise numerous privacy and data security concerns. As a result, responsible data management practices by all entities involved in the Smart Grid ecosystem is an imperative.

[5] See "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)" at:
http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf
(last accessed Oct. 1, 2009).