Trans Atlantic Consumer Dialogue

DOC No. INFOSOC 44-11 DATE ISSUED: JUNE 2011

Resolution on Privacy and Security Related to Smart Meters[1]

For decades, water, gas, and electric utility service providers have used meters to record household energy (gas and electricity) consumption for billing and management purposes. Typically these meters require utility companies to send personnel to physically collect data, which could be at intervals as long as two years. Next-generation "smart meters" are being installed in homes in great numbers in the US and parts of the EU, replacing old meters as the means by which consumer electricity usage data is recorded and collected. These smart meters include new features, which can provide an end to estimated billing and enable households to monitor their energy use over a period of time — thus, it is argued, providing a tool to assist in the public policy goals of affordable energy and carbon reduction. Consumer organizations stress that if smart meters are deployed they must provide improved social assistance to vulnerable[2] and low-income households.

However, TACD members also have grave concerns related to the privacy, data protection and security implications of smart meters. The dramatic increase in the granularity of data available and frequency of collection of household energy consumption means that the smallest detail of household life can be revealed, with potential risks for consumers including identity theft, augmenting private and data broker consumer profiles (US), real-time surveillance, and unwanted publicity. In addition to these smart meter privacy risks there may also be security risks — e.g., software or firmware, programming or installation, interoperability conflicts with other smart-grid-enabled technologies, and the threat of cyber attack.

Smart meters must be reliable, secure and enable all customers to better manage their energy use. They must also maximize meaningful consumer choice, drive down prices and enable consumers to make well-informed and effective purchasing decisions — all without sacrificing essential consumer and human rights to privacy and data protection.

Recommendations

TACD resolves that EU and US government should:

1. Enact or revise data protection and privacy legislation to:
   a. Forbid utilities from installing smart meters without consumers' informed consent
   b. Prohibit use of utility consumer consumption data for marketing, selling, sharing, or reuse without the customer's specific and unambiguous consent

[1] To be read in conjunction with the TACD Resolution on Smart Grids CC 04-11, June 2011

[2] Those who for reasons of age, health or disability are at greater risk if disconnected from the power supply.

c. Establish data retention rules regarding utility usage data
d. Define utility consumption data as personally identifiable information (PII)
e. Ascertain that consumers have control over their data in terms of what PII data is exported out of the smart meter, who collects and processes that data, how that data is used, and how long it will be retained
f. Encourage privacy and security by design, including data minimization, anonymisation and aggregation, and models that focus on consumers' maintaining control of their utility consumption data
g. Ensure that customers have access to their transfer log files in order to see which data was transmitted to whom at what time
h. Carry out privacy and security impact assessments on all aspects of smart meters and grids before they are developed
i. Require utility companies to establish a balanced and effective social marketing strategy to engage and educate consumers on new smart meter functionality and benefits
j. Require utility companies to develop a strategy for monitoring and enforcing data privacy rules including:
    - Creating effective complaints and redress mechanisms
    - Collecting and making available data on consumer privacy and security complaints and their resolution
    - Taking timely action to address the causes of those complaints
k. Require that additional (such as energy management) services by utility companies or third parties only be provided with the express authority of the consumer
l. Require third party energy management service providers to protect consumer personal information, utility service provider information, and utility usage data from access by non-authorized persons, abuse, or misuse through effective processes and established encryption technologies
m. Require utilities to develop a secure transport protocol for utility usage data that does not only rely on anonymisation, but also on use of effective encryption technologies
n. Mandate independent internal audits of energy suppliers' security and privacy processes to evaluate risks around their practices
o. Develop upgradeable technical standards and systems to safeguard future-proved, end-to-end security
p. Ensure that all customers have free access to their energy consumption information in a format that enables them to better manage their energy use and compare all energy deals available in the market.
q. Establish clear roles and responsibilities around data security and privacy, and strong enforcement mechanisms for failure to deliver the appropriate standards or service.

2. Initiate pro-active cooperation between relevant EU and US agencies to achieve better harmonization of utility privacy protection practices. This is particularly important as smart meter technology and utility service delivery may involve large geographic areas across physical national borders. Differing national data protection and privacy regulatory practices may create confusion for users and reduce the potential benefits of improved utility infrastructure.

3. Raise utility provider and public awareness regarding the benefits and potential risks of smart meters on privacy and consumer rights.

4. Harmonize privacy protective statutes and regulations through universal ratification of Convention 108[3].

TACD resolves that EU and US smart meter operators should:

1. Integrate privacy and security by design. This means that the default settings and usability features for smart meters should ensure maximum privacy for users' energy consumption data.

2. Enable consumers to remain "masters of their data" by allowing them to:
    a. Manage their own utility usage
    b. Change technology for utility usage management or third party service providers (e.g., when moving house, or requesting assistance in their management of energy usage)
    c. Port or delete data free of charge
    d. Request that service providers or user management systems delete their information after they have changed technology or management assistance entities. There should be statutory deleting periods.

3. Develop common binding ethical codes for the design, deployment and provision of utility smart meter management services, including data protection and security.

[3] See: http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Background

Smart meters and related technology will create opportunities for consumers to better manage electricity usage, while also creating new privacy risks. We are outlining in this section areas for additional attention by policy makers as they move to regulate the deployment of smart meters as they relate to electricity service provision.

Privacy and security challenges posed by smart meters
Smart meters are one piece of a larger effort to integrate computing technology and networking capacity into the end-to-end infrastructure of electricity generation and delivery. Utility companies' stated goals are a just-in-time provision of electricity service, and enhanced accuracy in the calculation of customer billing.[4] These objectives will be reached via features such as:

- Real-time statistics on energy consumption available to the consumer
- Remote delivery of that data, as frequently as every 15 minutes or less
- Remote instruction and reconfiguration
- Remote changes of tariffs changes or payment methods
- Remote disablement/enablement

Using more advanced metering systems, utilities may also communicate directly with customers via an in-home display unit. Smart meter communications may take place via existing mobile (cell-phone) operator networks, fixed telephony networks or electricity grids.

The power generation and delivery system melded with a high capacity communication infrastructure is referred to as a "smart grid." It is estimated that it will be 100 to 1000 times larger than the Internet.[5]

Privacy concerns about smart meter and grid technology center on the collection, retention, sharing or reuse of energy consumption information on individual households or offices. Such energy data processing could provide insight into personal behavior patterns, (when someone watches TV, plays video games or goes to bed); occupation of premises, household composition, consumer appliances in the home, home security, etc. Over time these technologies will mature, providing details about consumers that may not be immediately apparent.

In the near future, smart meters will also be able to collect more specific personally identifiable information when paired with Home Area Network (HAN) enabled appliances. Currently, smart meters cannot differentiate energy consumption between two different appliances. Like a GPS tracking device attached to a car recording its every move, a HAN-enabled appliance transmits specific information related to the use of that individual appliance. A HAN-enabled clothes washing machine can transmit the time of day a consumer washes his or her clothes as well as the wash cycle and water temperature settings. While utility companies or third party energy manage service providers can collect this information under the guise of energy efficiency management, this information can also reveal very private, personal consumer habits. For example, data that would become available could include when someone is or is not at home; the time of arrival indicated by a change in electricity consumption may reveal the age or health

[4] http://www.ferc.gov/industries/electric/indus-act/smart-grid/gao-report.pdf
[5] http://news.cnet.com/8301-11128_3-10241102-54.html

situation of the occupants; as well as other information that would otherwise not be available outside of the home.

This scale of data storage and collection is vulnerable to both commercial and criminal interests – for example consumer profiling and targeting for marketing purposes, identity theft, real-time surveillance, targeted home invasions or unwanted publicity or embarrassment.

There is increasing recognition in the EU and US that privacy and security are issues that must be taken seriously; the episodes in the Netherlands and in California, in which privacy concerns contributed towards the halting of smart metering rollouts and subsequent legislative/regulatory efforts to manage future deployments, are stark reminders of the importance of tackling consumer concern about a "spy in the home."[6] Such awareness not only to protects consumers, but also strengthens consumer engagement. It is essential that privacy risks be addressed as a matter of urgency, as millions of consumers already have smart meters.

Smart meter data collection should be limited to data that is consumer-consumption-specific, operational and critical to utilities in providing the correct amount of electricity to end users. Smart meter data reporting should be based on the use and purpose of the data collection. Operational data may be stripped of identifying information and communicated securely and more frequently, while consumer data may be communicated less frequently, but more securely than operational data.

Actions taken by the EU

In the EU, the gas and electricity directives of the third Energy Package, adopted in 2009, require member countries to prepare a timetable for the introduction of intelligent metering systems. In the case of electricity, at least 80% of consumers should be equipped with smart meters by 2020, subject to an economic assessment analyzing the reasonability and cost-effectiveness of intelligent metering. Additionally, the EU Directive on energy performance of buildings also requires countries to encourage introduction of smart meters in new or renovated buildings. Many EU countries have set up regulatory frameworks to roll out smart meters; Sweden was the first to install smart meters for all its consumers, by end of June 2009. Netherlands' initial regulation mandating universal use of smart meters with quarter-hourly meter readings was blocked by Parliament due to privacy concerns (now replaced with more privacy-friendly rules and the right to refuse the smart meter); Italy, Ireland, Norway, France, Spain, Finland and the UK are all implementing regulated smart meter roll-out programs.

The data protection and privacy aspects of smart meters in the EU are subject to existing data protection legislation, in particular the Data Protection Directive of 1995 (currently under revision), and the ePrivacy Directive (reviewed 2009). Member countries implement both of these directives with various degrees of strictness. However, the legal bases for processing smart meter/grid data are not as yet properly defined on the European level and interpretation may vary from country to country, with resulting gaps in the available protections.

A taskforce set up by the European Commission is currently looking at issues specifically related to smart-grid data handling, security and consumer protection. This review includes an overview of legislation on data protection, and whether or not further protective measures

[6] http://www.bigbrotherwatch.org.uk/home/2010/01/privacy-concerns-scotch-smart-meters-plan-in-holland.html, http://www.dailyfinance.com/2010/07/19/the-california-smart-meter-revolt/

should be put in place, including through standardization[7]. Similar work is ongoing on national levels; for example, in the UK the government has an ongoing program of consultation with stakeholders prior to finalizing policy, including privacy and data protection.

Actions Taken by US Government

In September 2007, the Department of Energy's Research and Development Division's Office of Electricity Delivery and Energy Reliability published its "Transforming Electricity Delivery Strategic Plan,"[8] and in December 2007, the Energy Independence and Security Act of 2007 was enacted as Public Law 110-140. The law, among other things, directed that smart grid technology be studied for its potential "to maintain a reliable and secure electricity infrastructure that can meet future demand growth."[9]

In 2009, the Obama Administration began its first term with a strong commitment to global climate change policy, which began with funding in an economic stimulus bill for $3.4 billion in funding for smart grid deployment.[10] This level of policy and regulatory activity around the issue of climate change was a dramatic and a marked departure from previous administrations.

As directed by Public Law 110-140, the National Institute of Standards and Technology (NIST) in the Department of Commerce conducted an open process that engaged the utility industry, civil society and federal agencies in the development of recommendations regarding smart grid deployment.[11] In June 2010, NIST published "Guidelines for Smart Grid Cyber Security: Privacy and the Smart Grid."[12] These guidelines address critical security concerns and make sound recommendations on ways to address them; such as conducting privacy impact assessments; and development of formal documented privacy policies that establish a set of fair information practices for smart meter PII. The document also includes a comprehensive review of privacy concerns that arise from the "many new data collection, communication, and information sharing capabilities related to energy usage." Over 23 civil society organizations participated in the public commenting opportunity regarding the deployment of smart grid.[13]

In October 2010, the Federal Energy Regulatory Commission (FERC) began rulemaking proceedings on the NIST recommendations as required by Section 1305 of the Energy Independence and Security Act of 2007.[14] However, FERC has not identified a means of monitoring whether companies will be in compliance with the standards once they are developed and issued by the agency.[15]

In addition to the federal government's efforts, each of the 50 states has oversight of utility service generation and provision; for example, the State of California has drafted regulations

---

[7] The European Commission issued Standardisation Mandate M/490 to the European Standards Organisation in March 2011, which includes *inter alia* requirements to address privacy and security.

[8] http://www.oe.energy.gov/DocumentsandMedia/RD_Strategic_Plan_Final07.pdf

[9] http://epic.org/PL110-140-Smartgrid_section.pdf

[10] http://online.wsj.com/article/SB125663945180609871.html

[11] http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[12] http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[13] http://epic.org/privacy/smartgrid/EPIC_Smart_Grid-Cybersecurity_12-01-09.2.pdf

[14] http://www.ferc.gov/media/news-releases/2010/2010-4/10-07-10.pdf

[15] http://www.ferc.gov/industries/electric/indus-act/smart-grid/gao-report.pdf

regarding the deployment of smart meters in that state.[16] Which government entity will have regulatory authority over smart meters is unclear, but the interest of many state and federal government agencies highlights its importance to policy and decision makers at this point in time.

For these reasons, US actions on energy issues to date are marked by their lack of coordination.

Conclusion

Privacy and personal security protections are essential to consumer trust and acceptance of smart meters in their homes and businesses. Failure of the US and EU governments to develop effective security and privacy policies for smart meter deployment may hinder adoption of these new devices and their related applications and services.

It is both imperative and timely for consumer advocacy organizations to open a dialogue with decision makers on the development of consumer security and privacy standards guiding the design and implementation of smart meters.

[16] http://www.cpuc.ca.gov/PUC/energy/smartgrid.htm