

Who Has My Data?

Illuminating Renters' Smart Meter Privacy Concerns

Germaine Irwin, Nilanjan Banerjee, Amy Hurst
University of Maryland
Baltimore County (UMBC)
1000 Hilltop Circle
Baltimore, MD 21250 USA
(germaineirwin, nilanb,
amyhurst@umbc.edu

Sami Rollins
University of San Francisco
2130 Fulton Street
San Francisco, CA 94117 USA
srollins@cs.usfca.edu

1. INTRODUCTION

Smart meter installations have increased in the United States as energy companies seek to gain greater control over energy consumption of its customers. Numerous consumer benefits are touted for gathering this information, however, renters whose utility costs are included within their monthly housing payment are overlooked in these discussions. These renters often do not have access to their own utility consumption data. Often, this information is in the hands of their landlord or even a third party billing company. Are these renters aware of who owns and controls this data or that this information can be used maliciously? This work seeks to understand the privacy and usability issues of smart meter data collection for this population.

2. BACKGROUND

With the advent of the smart grid for energy aggregation and distribution, many states have seen deployments of smart meters to their homes. Smart meters collect granular data on energy consumption habits within each home. They enable two-way communication between the meter (and the inhabitants activities) and the electric company's central system. Energy companies have been touting the benefits of smart meters, including [1]:

- Energy budgeting and tracking
- Personalized energy efficiency tips
- Peak event reports and savings summaries
- Peak event web notifications
- Smart energy pricing programs

While the above has advantages for consumers, there are many privacy and security issues that have been uncovered, including discovering personal habits of residents, when residents are home or not, what activities they are doing when they are at home, regulation of energy by the electricity company and selling personal data.

Unfortunately, residents are often unaware of the privacy issues that arise from these installations. Such issues as collecting granular data that illustrates daily habits, enabling owners of the data to potentially sell the information [7].

3. RENTERS' DATA INTEGRITY

Much research has been completed regarding privacy issues and concerns that have arisen in the wake of smart

meter deployments. Many have discussed ways to increase security via hardware [2], such as new types of authentication schemes, and others have discussed novel encryption methods for sending and receiving this data [3, 2, 6].

Most of the solutions mentioned, however, do not engage the consumer at all. Unfortunately, these solutions still leave many questions as well a privacy gap within non-traditional household and billing structures.

3.1 Landlord & 3rd Party Access

While conducting a recent interview study on energy consumption context [5], three renters out of 10 stated they do not have access to their energy bills or data because utility costs were included in their rent. We also learned from 2 participants who lived in subsidized housing that their utility costs were also paid for by city or federal governments. This type of billing begs the question as to who has access to this data. If the household is equipped with a smart meter, the landlord then has the ability to discern activities within each of his/her housing units [7, 8]. This data collection can provide detailed information about household activities without involving the user at all. Possibilities exist within the smart grid to extract patterns of usage from smart grid/smart meter data without having any prior training with statistical methods [8].

“Any entity that has fine-grained energy consumption data can infer the customers' lifestyles and habits (e.g., times of absence and even concrete activities like watching TV or cooking)” [7] Thieves can monitor movement to discover best times to conduct a burglary. Marketers could buy this data to understand user habits in order to sell more products.

Motivated by the above observations, this work studies the following research questions:

Who should have access to renters' smart meter data? We would like to understand the options for access to this data by landlords and tenants, which would include determining the feasibility of multiple accounts being created for each household. Also, if the data is aggregated (because it is building costs, not per unit costs), then discovering options to make residents aware of privacy issues when renting.

What is the prevalence of 3rd party billing? From our interview study [5], we also discovered that some housing management offices utilize a 3rd party to manage utility billing and collection. In this case, who has access to residential data? Does this mean the 3rd party can now also

discern residential habits, such as when people are home or not, what kind of utilities they use at what times, their usage of certain appliances, even movement through the house or when they walk the dog. This is a concern since another entity that is unknown to the renter can see the habits of the household residents. There is a potential for them to sell this data and, if they can access the data, they have control or lack of control of the data, meaning potential for additional security breaches.

What is done with the information on each household? As stated, renters are often unaware that this data exists, who has access to it, or the potential security issues surrounding the situation. How can renters be made aware that a 3rd party has access to their data and what could possibly be done with the information? We intend to extend the study in order to understand the prevalence of 3rd party billing and if there are contracts in place for the data.

Are there ways to share data with landlords and protect the privacy of the household? Prior research suggests anonymizing the data as it is being exchanged between the consumer's meter and the electric company. Additively homomorphic encryption is suggested as a solution, which entails "hiding" individual consumer behaviors behind smart meter grouping [4, 7, 6]. Similarly, Efthymiou and Kalogridis [3] describe using a "third party escrow" service provider that would anonymize the data so that individuals and their corresponding habits would not be discernible.

Perhaps providing a visual interface to the landlords that provides enough information to understand billing details would be sufficient. Therefore, the course grained data could be reserved for the actual home residents. Separate interfaces could be a solution.

Another approach is masking data from the billing side, thus preserving metering goals of the utility companies [8]. The authors suggest a three phase billing protocol for masking data using Zero-Knowledge protocols. These phases include registration, in which the data is encrypted with tags and keys, tuple (usage data) gathering without revealing which tuples correspond to which smart meter, and reconciliation (the billing phase).

Chim et al [2] propose an authentication scheme to preserve consumer privacy within the smart grid. In their system, consumers receive a smart appliance that connects to a tamper-resistant device "...for generating pseudo identities and signatures on message". This system addresses privacy issues with transmission of data from the consumer's home to the electricity supplier as well as attacks from any outside systems. Usability of these devices, however, add a layer of complexity to the resident as well as potential space issues within the home if the devices have to be connected to each smart appliance.

3.2 Smart Meter Benefits

Besides this privacy black hole, when residents do not have control of their data, the usability of a system that purports to benefit consumers is called into question. How can residents gain energy efficiency, tracking, budgeting and usage feedback if they do not have access to their own data?

How can we increase renters' smart meter usability? These rental residents do not have an opportunity to see advantages of the smart grid/smart meter technology. They are losing out on understanding their usage and potentially making energy usage changes. They may be envi-

ronmentally conscious and want to know this information in order to positively effect their environs.

Since renters are unaware of this data and how it may be used, perhaps policy changes at the utility level regarding external accounts should be considered. Further research could determine if and why landlords may need this information for billing purposes or other reasons.

At the very least, this is a usability concern since users should have control of their data so they can realize how they are using energy and gain from potential feedback for savings and potential to be more environmentally aware.

4. CONCLUSIONS

While privacy of the smart grid and smart meter deployments have been much discussed as well as argued, the situation of renters who don't have control over utility bills has been overlooked. They often do not know who owns or has access to their data. There could be 3rd party involvement without their knowledge, which could expose their personal habits and choices on display for malicious attacks and marketing tactics. Finally, they are denied knowledge of energy usage that could be used to benefit their home lives. Further research would provide much needed answers.

5. REFERENCES

- [1] BGE (<http://www.bge.com/smartenergy>) May 14, 2014.
- [2] T. Chim, S. Yiu, L. C. Hui, and V. O. Li. Pass: Privacy-preserving authentication scheme for smart grid network. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 196–201. IEEE, 2011.
- [3] C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 238–243, Oct 2010.
- [4] F. D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *Security and Trust Management*, pages 226–238. Springer, 2011.
- [5] G. Irwin, N. Banerjee, A. Hurst, and S. Rollins. Understanding context governing energy consumption in homes. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*, pages 2443–2448. ACM, 2014.
- [6] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda. Privacy for smart meters: Towards undetectable appliance load signatures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 232–237. IEEE, 2010.
- [7] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Pérez. Do not snoop my habits: preserving privacy in the smart grid. *Communications Magazine, IEEE*, 50(5):166–172, 2012.
- [8] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *In Proc 2Nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, BuildSys '10*, pages 61–66, New York, NY, USA, 2010. ACM.