DRAFT: To appear in *International Journal of Technoethics.*

Citizen perspectives on the customization/privacy paradox related to smart meter implementation

Jenifer Sunrise Winter
Associate Professor
School of Communications, University of Hawai‘i at Mānoa
2550 Campus Road, Crawford 325
Honolulu, HI 96822
email: jwinter@hawaii.edu

ABSTRACT

This paper employs the framework of contextual integrity related to privacy developed by Nissenbaum (2010) as a tool to understand citizen response to implementation of residential smart metering technology. To identify and understand specific changes in information practices brought about by the introduction of smart meters, citizens were interviewed, read a description of planned smart grid/meter implementation, and were asked to reflect on changes in the key actors involved, information attributes, and principles of transmission. Areas where new practices emerge with the introduction of the smart grid were then highlighted as potential problems (privacy violations). Issues identified in this study included concern about unauthorized use and sharing of personal data, data leaks or spoofing via hacking, the blurring distinction between the home and public space, and inferences made from new data types aggregated with other personal data that could be used to unjustly discriminate against individuals or groups.

Keywords: Data Discrimination, Privacy, Surveillance, Smart Grid, Smart Meters, Framework of Contextual Integrity, Internet of Things

INTRODUCTION

The smart grid is a next-generation electrical power grid intended to upgrade and replace aging infrastructure, enhance energy conservation, and provide real-time information for decision making, allowing energy companies “full visibility and pervasive control over their assets and services” (Farhangi, 2010, p. 19). Whereas the existing power grid is an inefficient, unidirectional pipeline that is unable to access information about its endpoints (e.g., residences receiving power) in real-time, the smart grid represents the marriage of information and communication technologies and power systems, adding new communication and data management capabilities (Depuru, Wang, Devabhaktuni & Gudi, 2011). The smart grid can be seen as an aspect of broader sociotechnical developments focusing on the sensoring of everyday objects, the Internet of Things. The Internet of Things is described as a “backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and retrieve information from the Internet to facilitate their adaptive functionality” (Weber & Weber, 2010, p. 1). It is an emerging architecture intended to enable billions or trillions of heterogeneous objects to interact over the Internet. A key component is the development of machine-to-machine communication to automate the exchange of information, goods, and services. These developments represent the integration of the physical world with the virtual world, enabling the increased instrumentation, tracking and measurement of natural processes. The new types and massive volume of data created in this environment are mined to enhance decision-making in business and government and offer citizens increased convenience and safety (Uckelmann, Harrison, & Michahelles, 2010). One aspect of the Internet of Things is the development of smart cities that, via ICT integration, allow advanced infrastructure monitoring, including smart grid management to govern cost- and resource-efficient use of energy (Khan, Khan, Zaheer, & Khan, 2012; Atzori, Iera, & Morabito, 2010). Smart homes can include automatic lighting and power allocation (CERP-IoT, 2010). This use of ICT to lower environmental impact has been referred to as “Green ICT” (Vermesanet al., 2011).

Smart meters, a component of the smart grid, are energy meters installed at residences by electric utilities to capture energy consumption with more granularity than a traditional electrical meter. This data is captured in real-time and transmitted to the utility via a wireless network. In addition to allowing a constant stream of data about a home’s energy use, smart meters also allow a utility to send commands to the meter, such as turning off the power due to nonpayment of tariffs or reducing the amount of energy available to a home based on the time of day or type of energy use. Energy use data is stored and analyzed by the electric company to identify energy usage patterns and related pricing schemes. In the United States, the *American Recovery and Reinvestment Act* of 2009 funded more than $3.4 billion in grants for smart grid development (Department of Energy, 2011). As of July, 2013, nearly 40% of households in the United States were equipped with a smart meter (Innovation Electricity Efficiency Institute, 2013). Resistance to smart meters has already been documented in a number of communities. For example, Pacific Gas and Electric's introduction of smart meters in Northern California has been met with protests and publicity campaigns warning of potential threats to health and liberty (Barringer, 2011). When considering how shifting information practices related to residential smart meters might be perceived as violations of social norms, the field of technoethics illuminates the complex relationship between technologies and ethics. It represents an effort to ground inquiry about this relationship in a framework that is holistic, rather than fragmented among multiple, technical disciplines (Luppicci, 2009). Placing this relationship at the center of intellectual inquiry, technoethics enables us to reflect on both anticipated and unexpected outcomes related to emerging information and communication technologies (ICTs) (Stahl, B.C., et al., 2010).

The Smart Grid/Smart Meters in Hawaii

Hawaii is by far the most petroleum-dependent state in the United States, with almost 85% of total energy consumption in 2008 fueled by petroleum, compared with a national average of 37.5% (State of Hawaii, Department of Business, Economic Development & Tourism, 2011). The existing power grid is limited in regards to incorporation of clean energy sources such as solar or wind power. In 2008, recognizing the long-term economic effects of, and ongoing vulnerabilities imposed by, reliance on oil, the State of Hawaii, in collaboration with the United States Department of Energy, created the Hawaii Clean Energy Initiative (HCEI). The goal of this initiative is to transform Hawaii's economy to one 70% clean-energy-based by 2030 and for the electricity sector to meet 40% of demand by this date. To accomplish this, in addition to alternative fuel sources such as solar and wind power, the HCEI focuses on the deployment of the smart grid. As part of the HCEI agreement between the Hawaiian Electric Company (HECO), the state's largest provider of electrical power, and the State of Hawaii, HECO began testing smart meters in 2006, and in 2008 entered a 15-year definitive agreement to deploy smart meters state-wide (Hawaiian Electric Company, 2008). HECO plans to deploy 448,200 smart meters throughout its service territory by 2018 (Innovation Electricity Efficiency Institute, 2013). This was partially funded by a grant from the ARRA of over 5 million USD (Department of Energy, 2011). Smart meter rollout has begun in select neighborhoods in the Honolulu area, with installation at 5,200 households between April and July, 2014 (Shimogawa, 2014).

Security and Privacy Concerns about the Smart Grid/Smart Meters

The introduction of residential smart meters poses a number of ethical challenges related to security, privacy, and "ensuring social justice both in terms of access and cost of electric power service" (Kostyk & Herkert, 2012, p. 25). First, the granularity of data will greatly increase, enhancing the surveillance capacity of these systems (Bleicher, 2010). Each appliance gives off a signature based on its energy use, making it uniquely identifiable. Even the specific television programs or movies one watches can be deduced via this monitoring (Mills, 2012). Further, manufacturers are increasingly introducing "smart appliances" to the market with features such as remote control from a smartphone or the ability to text and appliance to learn about its state. Smart meters can also interface with these "smart appliances" and control them (e.g., turn off certain appliances during peak energy-use periods) (McDaniel & McLaughlin, 2009). Hence, many new types of data can be collected. Further, without secure protection schemes, consumer data may potentially be transferred or sold, willfully or not, and may be aggregated with other data about an individual. Hacking is another issue that has been well-documented (e.g., Weber, 2012), and there is potential for spoofed energy usage or surveillance for the purpose of committing crimes. For example, security researchers hacking smart meters were able to determine how many personal computers or televisions were in a home, as well as what media were being consumed (Brinkhaus et al., 2011). These changes threaten to transform the home into a site of surveillance and pose a variety of potential informational injustices. In particular, these new data types and the ways that they can be shared, stored, or mined may reveal patterns about personal behaviors or attributes that could be used to discriminate economically or politically. If the data are not protected due to lapses in security or policies that do not restrict their sale or sharing with other entities, they may be aggregated with other personal data and subject to advanced analytics. In addition, the machine-to-machine communication and processing that is used to collect and analyze these data will greatly increase both the amount of data collected and the analytic capacity used to explore it, introducing an enhanced risk of data error (Winter, 2014). These changes are not just a matter of scope and scale. As Floridi (2005) notes, modern communication technologies are part of an "unprecedented transformation in the very nature (ontology) of the information environment" (p. 186). They do not merely increase the quantity and quality of data collected; they transform humans into informational agents, and each person is essentially constituted by his or her personal information. Informational breaches of this information are thus seen as aggression towards personal identity.

Because smart meter usage in the home represents a dramatic change in the types and amount of data collected about personal energy use, and there is uncertainty about how this data will be shared or stored, it is anticipated that there will be continued citizen concern, and possible refusal to adopt, smart meters. This type of data collection in the home also challenges the long-standing concept of two privacy spheres: public and private. Because most law in the United States is based on this dichotomy, novel technologies that do not fit well with this split may lead to conflict. While the United States' Fourth Amendment is intended to protect against unreasonable search and seizure, novel technologies have previously highlighted this conflict. For example, in *Kyllo v. United States*, the Supreme Court ruled that law enforcement's use of heat scanners (at the time a novel technology) to detect energy use and identify homeowners cultivating marijuana was unconstitutional because, "In the home… *all* details are intimate details, because the entire area is held safe from prying government eyes" (Christakos & Mehta, 2002, p. 473). In this way, novel technologies such as smart meters can be "disorienting as they reveal the inconstancy of boundaries and fuzziness of definitions" (Nissenbaum, 2010, p. 101).

This paper examines citizen response to implementation of residential smart metering technology. It is motivated towards understanding how we can better foster the development of new systems, practices, and policies that balance the positive potential of smart grid technologies with citizens' rights to privacy and freedom from data-based discrimination. Technologies are not neutral objects, but rather actors in complex, sociotechnical systems. Therefore, new technologies must be examined in the specific contexts of their use (Kling, 2000). To better understand citizen attitudes about smart meter implantation, this study uses the framework of contextual integrity related to privacy developed by Nissenbaum (2010). Following this framework, the study seeks to identify and understand specific changes in information practices that will be brought about by smart meter implementation and may be perceived as violations of personal privacy and explore the underlying norms that shape these perceptions. Because there have been large roll-outs of smart grid technology over the past several years and numerous concerns have been raised, it is particularly important to understand citizen perspectives in order to design technical systems and related policies that will have moral legitimacy. In the next section, the framework of contextual integrity related to privacy developed by Nissenbaum (2010) is introduced. Then, the method used to explore normative conflicts related to smart meter implementation in residences is described, followed by a results and discussion section that outlines conflicts with novel practices related to the smart meters in the home.

The Framework of Contextual Integrity

Although privacy is often cited as a key human right, there are many conflicting beliefs about what it entails (Solove, 2010). Increasingly, there has been acknowledgement that personal conceptions of privacy emerge from rich social contexts. Nissenbaum (2010) argues that privacy is context bound and should be conceived of, not as a right to secrecy or control, but to an “appropriate flow of personal information” in particular contexts (p. 127). This concept is referred to as contextual integrity. The framework of contextual integrity related to privacy is intended to guide assessment of novel practices arising from ICTs. Like Floridi (2005), Nissenbaum argues that previous conceptions of privacy are not able to address the radical changes brought about by systems such as the smart grid and smart meters.

As a descriptive and heuristic tool, the framework of contextual integrity fosters insight into citizens’ reactions to novel, or changing, ICTs that affect flows of personal information. The framework is also intended to assist in evaluation of moral and political values embedded in systems and practices. Because norms are context-bound, novel systems can create conflict between moral and political values. These might include informational harms, such as unjust discrimination, or threats to personal autonomy and liberty (Nissenbaum, 2010). There is a potential for political or economic discrimination on the part of governments or corporations, who might offer different services, products, or prices, to individuals based on their data profile (Turow, 2006; Turow, 2011; Winter, 2014). To evaluate a novel technology via the contextual integrity decision heuristic, one uses the following steps: 1) describe the existing practices in context; 2) describe the novel practice in context, along with changes in actors, attributes, and transmission principles; 3) identify the entrenched norms and note how the new technology may come into conflict with existing ones. (If informational norms have been breached, this represents a violation of contextual integrity); 4) evaluate the new informational practices based on moral and political factors, such as implications for justice or democracy; 5) evaluate the moral and political factors in relation to contextual values; and 6) argue for, or against, specific systems or practices based on this analysis (Nissenbaum, 2010).

When assessing a new technology, focus is placed upon whether, in a particular context, it comes into conflict with existing norms. Norms are embedded in systems, and Nissenbaum (2010) highlights their prescriptive nature – that is, they relate to expectations of how one *should* behave in a particular context. The process begins by documenting the existing (prior to the novel technology) practice and identifying the informational norms related to actors who handle the information, attributes of data collected, and how the information is stored or transmitted. Then, to address whether violations have occurred, a comparison must be made between the existing practice and the new practice: "if the new practice generates changes in actors, attributes, or transmission principles, the practice is flagged as violating entrenched informational norms and constitutes a prima facie violation of contextual integrity" (p. 150). While the term "violation" has a negative connotation, a violation of contextual integrity does not always indicate that development is unjust or lacks moral legitimacy. Instead, it highlights the change so that it can be further assessed in order to determine whether the new practice is morally acceptable, or whether it should be challenged. Nissenbaum (2010) emphasizes that it is possible for the violation, after consideration, to be approved as a morally superior practice. Violations merely pinpoint where there is a conflict between norms: If the new development is more effective in "supporting, achieving, or promoting relevant contextual values," then there is moral justification to replace the entrenched practice (p. 166).

Establishing whether a new informational practice is morally or politically superior requires consideration of general moral and political arguments about privacy. Nissenbaum (2010) notes that these come from a broad array of perspectives addressing the value of privacy (e.g., protecting citizens against informational harms, maintaining personal autonomy, ensuring fairness, justice, and equality, and support of democratic institutions and publics). It is necessary to consider the specific values, ends, purposes, and goals relative to the specific context in order to make this judgment.

This analysis can aid in understanding citizens' reaction to ICT reshaping personal information flows. Where there is resistance or fear in relation to adopting a new technology, it can help to understand the underlying concern (rather than fail to acknowledge it or trivialize it). This makes it useful for predicting when novel technologies are likely to lead to anxiety or rejection, and it highlights these uncertainties for ethical evaluation, opening the process for negotiation between stakeholders.

METHOD

The framework of contextual integrity, outlined in the previous section, was employed in this study to identify areas of concern related to emerging practices related to smart meter implementation, highlighting them for ethical evaluation. This study addressed normative conflicts related to smart meter implementation in the home. Smart meters were chosen for analysis because they are a novel technology that alters existing flows of personal information. They are important to evaluate because they are beginning to be widely deployed in other settings, but there has been little public discourse or awareness about them in Hawaii.

To explore citizens' perceptions about context-specific norms of privacy related to smart meters in the home, the researcher conducted in-person, semi-structured interviews. Interviews were chosen because they can elicit more in-depth responses, while permitting the flexibility to follow unexpected directions. Participants were selected based on the following criteria: 1) age of 18 or above; 2) resident of the State of Hawaii, living on Oahu; and 3) living in a dwelling that is serviced by electric power. Maximal variation sampling was employed to select participants reflecting a diversity of perspectives based on age, ethnicity, gender and socioeconomic status. This study focused on the Island of Oahu, which contains the State's largest urban district, Honolulu. Recruitment was performed online by posting invitations on a local discussion site frequented by a variety of citizens and was on a volunteer basis. As demographic categories (gender, age, ethnicity, and level of education completed) were saturated, participants in other categories were sought. Interviews were conducted in public locations, at the discretion of the interviewees, and lasted between twenty-five and sixty-five minutes.

The development of interview questions and analysis was guided by the analytic framework of contextual integrity (Nissenbaum, 2010). Interviewees were first asked about their expectations in regards to existing meters so that the prevailing conditions could be documented. Interview questions then sought to gain insight into their perception of *information attributes*, what types of data they thought might be collected about them during such interaction. This included their perception of 1) what types of data may have been collected about them; 2) their presence at any given time, and the presence of any other individuals; 3) what appliances they used; and 4) any other information about their activities in their homes. A second set of questions asked participants about the *actors* involved, who they thought had observed these behaviors (human or electronic), and who had handled this information. Other questions addressed *principles of transmission*, whether the participants thought that data was recorded and transmitted. Once the existing practices and expectations were discussed, participants read a short explanation of planned smart grid/meter expansion. The description was not presented as a threat; rather, it described how participants might encounter smart meters in the near future.

After reading about the smart grid, a final set of questions addressed changes to existing practices (and expectations) of privacy. These questions were mirrors of the first set asking about perceptions of information attributes, actors, and principles of transmission in the new environment. Areas where new practices occurred with the IoT were then highlighted by participants as violations of contextual integrity, and these areas were discussed at length to probe for underlying norms.

Interviews were recorded in person with a digital audio recorder and transcribed. In some cases, follow-up clarifying questions were asked of participants to review for accuracy, strengthening objectivity and credibility. Qualitative analysis of the complete transcripts was used to develop themes as they emerged. Transcripts were analyzed and inductively coded using ATLAS.ti Scientific Software. After coding was finalized, data were summarized thematically.

RESULTS AND DISCUSSION

A total of nine participants representing both genders, and a variety of age groups, education levels, and ethnicities participated in the in-depth interview process. Five were male and four female. Three were college graduates, three had completed high school, two had graduate degrees, and one had completed middle school. Three participants were Asian, one African-American, four were mixed ethnicity (Polynesian/Asian or Polynesian/Caucasian), and one was Polynesian. Ages ranged from early twenties to early sixties. All participants resided on the island of Oahu in the State of Hawaii. They represented a variety of professional, service, and technical career paths. To preserve confidentiality, all respondents are represented by a pseudonym in the following discussion.

Existing Practices and Expectations

In order to understand how shifting information practices might be perceived as violations of norms, it was first important to establish informants' perception of the information flows related to their current electric power use at home. A series of questions addressed what data about their energy use they thought was collected, who had access to this data, and how it was stored and transmitted.

Despite announcements on the HECO website and trade news stories, only one of the participants was aware of HECO's smart meter plan (Keala). Two participants, Pono and Alana lived in neighborhoods where smart meter implementation is scheduled this year. These areas have been targeted by HECO with mailers introducing the smart meter implementation. In these two instances, there was awareness of an “upgrade” to the electrical system, but no special details were recalled. In addition, three of the participants had some awareness of smart meters used on the United States mainland or internationally. Keahi, for example, had lived in South Korea for several years and was familiar with their use there.

In relation to what data they expected is presently collected about their home energy use, it was understood by all that their energy utility, in this case HECO, would use this to measure their overall energy use for billing purposes. This was described as a monthly reading that would not offer any specific information other than the total kilowatts-per-hour (kWh) consumed. Keahi also thought that it was possible that some of his smart appliances might measure his energy use and transmit this, and other data, to the manufacturer. However, he acknowledged that this was not currently occurring via the energy utility.

When asked about who would have access to their data, it was agreed that individuals at HECO, who worked in the billing departments, as meter readers, or as policy analysts, would have access to their data. For example, Hau‘oli mentioned that she would not have any concern if the information was “in the right hands… People who specifically need to evaluate, maybe the cost of the electricity or energy that we use.” In addition, Keahi, Hau‘oli, and Makana pointed out that they felt would be appropriate to analyze this data as a way for HECO to offer improved service to consumers. In three cases, an interviewee described a living situation where they paid their electric bill via a proxy – a landlord or tenant association. This is a common situation in Hawaii, where rentals or homeowner/condominium associations may include the cost of electricity in a monthly fee. In these cases, participants agreed that landlords or homeowner associations would also have access to their energy use data. Makana and Keala also noted that aggregate data might be shared with federal or non-profit agencies (e.g., the United States Department of Energy) to study energy use trends for the purpose of developing sustainable energy solutions. Another expectation was that neighbors or passers-by might be aware of energy use (although not having direct access to the data itself unless they looked at the meter). These were seen as unwelcome, but not particularly intrusive, instances and not likely to be shared in any fashion. These were the only actors that they believed had access to their energy data at present.

Finally, it was understood by all that electronic databases held this data and that it was searchable by the utility. However, it was emphasized by multiple participants that this was acceptable only in relation to the specific actors and purposes mentioned above.

Conflicts with Novel Practices Related to Residential Smart Meters

A number of changes in the types of data collected, actors involved, and transmission techniques led to concerns by the participants. The main themes identified were related to unauthorized use and sharing of personal data, hacking, erosion of the private sphere, inferences about personal behaviors or ideas, and possible discriminatory practices based on analysis of personal data in aggregate form.

First, in all but two cases, there was enthusiasm for some of the promised benefits of smart meters. Energy companies' provision of smart meter displays that provide real-time, personalized feedback to customers so they could monitor and adapt their own energy-related behaviors were cited as appealing by five of the participants. This "green button" data can be provided to electricity customers, providing access to their personal usage data in an easy-to-understand format (Chopra, 2011). "With this information at their fingertips, consumers would be enabled to make more informed decisions about their energy use and, when coupled with opportunities to take action, empowered to actively manage their energy use" (para. 4). This was seen as a way to potentially lower cost to the consumer via energy use feedback. It was also noted that it would help more fairly address energy costs in a shared household. Another benefit of smart meters that was cited was how personalized feedback, coupled with behavioral changes, could lead to energy conservation and lessening reliance on imported oil. Pono noted the environmental benefits of smart meters, and said that he had heard about smart meters and smart homes "for a decade now. It's about time we got them."

Unauthorized Use and Sharing of Personal Data

Participants expressed concern that other, possibly unknown, actors could use their personal data without explicit consent. There was an awareness of increasing amounts of data being collected and analyzed, as well as uncertainty about who might see it. For example, Keala observed that companies already share data and that energy data might be used for targeted marketing:

> From what I have seen in the past, companies that collect information tend to share information with other companies. The selling of data -- particularly companies that are attempting to market certain things to people. So, if HECO were to sell their demographic information to marketing firms who would do things like send ads based on personal information that would disturb me.

Hau'oli added that "I think when you do have data that's not restricted to paper documents, but things that are online, other people definitely have access to it, unfortunately." Further, participants were concerned that, even if the data were not deliberately shared, they could be accessed without their consent. Keahi noted that there is a great deal of uncertainty about what happens to personal data once they are captured. "Ideally, I hope there are constraints on the sharing of this information, that there is this wall of consent that you have to go through, even though it's annoying… but who knows? It's so hard to anticipate how information will move, because there are ways it can be leaked."

In terms of who would possibly want, or have access to the data, there were several ideas. Unethical individuals, corporations, and government agencies were all mentioned multiple times. In regards to the government, there was concern that:

> Government agencies could use this data, not for me specifically, but there are people who perhaps are against certain government policies or practices and are in organizations that might want to make changes and perhaps the government might want to keep information on these individuals. It's certainly happened in the past. [Keala]

Recent news coverage revealing the existence of widespread Internet surveillance efforts by the National Security Agency in the United States may be a factor in this concern. In 2013, the Pew Research Center for the People and the Press (2013) credited news stories about NSA surveillance with growing public awareness and anxiety about government surveillance. Of particular note is the finding that 70% of respondents believed that NSA surveillance data is used for reasons other than investigating terrorism. Only one participant, Makana, said that he was not concerned about abuse of his energy data: "I can see potential for concern with something like a smart meter or access to your electric usage, but overall I think it is good. I think concerns would be among those who think aliens exist or who think 9-11 is a conspiracy put on by the government."

Moving beyond green buttons, data from the smart grid have also been entering public analysis as companies and smart grid research consortia have begun to make data available to researchers or citizen hackers (St. John, 2014). There are increasing calls from the open data community to provide application programming interfaces (APIs) to anonymized energy data to enable civic hackers to create apps (Tendril, 2012; Raferty, 2013). In these cases, the data sharing has been opt-in and data are anonymized. However, many other anonymized large data sets have been compromised through re-identification. A recent example is the re-identification of individuals based on anonymous DNA sequences and public data on the Internet (Gymrek, McGuire, Golan, Halperin & Erlich, 2013). Given the concern about the environment and the consensus that it would be appropriate for energy companies or non-profits to look for patterns in the data for community improvement, this may emerge as an area where citizens will find sharing these data sets to be acceptable. However, citizens may not be aware of the risk of anonymized data, so the issue of public awareness and means to better guard against re-identification should be further investigated.

Whether assurances to not share data are upheld or not, some participants also expressed concern that their information could be intercepted or hacked, either on-site, during transmission, or during storage. Although no participant specifically mentioned knowing of instances of smart meter hacking, four participants mentioned this as a concern. Makana stated that,

> With everything I've seen… news stories or articles…about hackers and terrorists taking down our power grid or the Internet in the U.S. I'd assume anyone good with computers could get their hands on that information… The smart meter, if I was a homeowner, would kind of make me want to push towards getting my own solar system just to avoid as much of this as I could.

It should be noted that Makana was the one participant least concerned with his data being observed, because he felt that no one would be interested. He was more concerned about people spoofing energy data, severing his connection to electrical power, or taking control of appliances in his home. This was one instance where concern about negative consequences related to the security of private information led a participant to consider opting out, or resisting, the technology.

This concern about the security of personal data was also addressed. Keala noted that he was "not so sure about the security of the databases that those companies use. People might be able to gather data about me or others that we were unwilling to share." Highlighting the complexity of this problem, the National Institute of Standards and Technology analyzed smart grid technologies and identified over 130 possible logical interfaces that link actors and will require secure standards for protection (National Institute of Standards and Technology, 2010a). A great deal of technical research related to the smart grid has focused on issues of security, but there are still critical vulnerabilities and no beginning-to-end protection schemes.

Erosion of the Private Sphere

Smart meters are expected to link a variety of everyday behaviors in the home to communication networks, making the home, traditionally the private sphere, a potential site of surveillance. The blurring of the public and private spheres due to ICT increases the probability of sensitive personal information related to political views, religious practices, health, and intimate practices being shared beyond their original intent or context. Respondents noted that the use of smart meters posed an intrusion into the private sphere, their homes. In fact, this may lead to an erosion of this distinction:

> Honestly I don't personally feel that I am doing anything, like, unethical or illegal in my home, but I know there are people that feel that what they do in their own home should not be information that should be available to people outside the home… [Keala]

One participant also noted a related threat from the integration of smart appliances and the smart grid (bridging the discussion into greater concern about the Internet of Things). Keahi noted, "If they collect energy data and then, sort of, glean other data from the devices themselves, I could see that would be a troublesome aspect for me." The erosion of the private sphere is of particular consequence due to the fact that existing laws and regulations in the United States are based on this dichotomy.

Inferences and Data Mining

Participants also raised the question of inferences that could be made about them due to the granularity and volume of data collection. The explosion and availability of real-time user data has enabled sophisticated user modeling, and there are many efforts to mine, model, and personalize these data (Jaimes, 2010). In this case, the gathering of novel data types, coupled with the ability to store and share them with relative ease, dramatically alters personal information flows. All but Makana and Kukane reacted to these changes with anxiety:

> I don't like that. Because they can basically tell someone was there, or maybe because of the changes, I bought something. Just the detail of it makes me feel nervous because it's kind of monitoring my daily life in terms of energy consumption. And that could actually reflect…. It's frightening. [*What types of things could it reflect?]* The fact that it's, like, monitoring… it could be anything. Yea, energy consumption, they have to monitor it, but I don't like the fact that any type of information can be collected. It seems very intervening to my life [Niele].

For Niele, the uncertainty about the scope and granularity of data was a concern, and she criticized the collection of data that was not specific to the purposes she had identified as appropriate (i.e., using it for billing). Keala explicitly linked these inferences to privacy and contrasted the two metering approaches:

> I see this as an erosion of privacy, not a complete lack of privacy, but you would be able to infer certain things about a person, I think, by looking at this information. As an overall group, you are seeing trends but you are not necessarily seeing what an individual is doing. But if you have my data you know what I'm doing when I am there. In the past, the amount of power we use in the home, that's a fairly general thing. I don't really see that as that much of an invasion because you can't really determine the sort of thing a person is doing other than using energy. In the smart meter, you can tell [a lot of things]; you can infer a lot about this person's personal life based on [this]. I think that's a little too much.

With consumers mesmerized by new appliances, and a lack of transparency about how these new data will be used, Keahi also mentioned citizens' general lack of awareness about potential risks:

> This is a very relevant topic. As I was saying, I was watching the consumer electronics show and that's [smart appliances] just such a huge part now, especially Samsung and LG are really getting into this... so I mean right now for most people they are looking at the consumer side of it. They are *very* excited about the possibilities of electronics being more responsive and alert, and so I think that part of it is great. But I think in the long term, eventually, we have to think about how is energy data being used? What inferences can people make from it? What companies will be collecting data? That's also equally important, even if it's not as popular.

The time to create legal protections and related system design choices is before system implementation and major problems arise (Weber & Weber, 2010).

Potential for Data Discrimination

While the citizens in this study were generally enthusiastic about the benefits of smart meters, they also expressed concern that their data could be used for unacceptable purposes. First, invasive, targeted marketing was noted as a possible outcome.

> They can tell what types of devices I am using. They could use my personal data to sell stuff... That's a lot of personal data. Maybe they'll find out I use a lot of computers. We have a lot of them. They will know our appliances. They could tell if an appliance is getting old and uses more energy and try to sell us something? Also, that could be used with other kinds of data that they could get. Other people in the household, if you file tax [sic], public records, they would have more data to target me in a compromised way. [Niele]

Haggerty and Ericson (2006) describe the ways in which data surveillance can foster new advertiser-based forms of identity. They argue that an individual's place in this "new constellation of market segments" can be used to discriminate against them, as different groups will receive different commercial offers and communication. Surveillance enables monitoring of these groups, with the embedded system logic subjecting individuals or groups to different levels of scrutiny. This “social sorting” (Lyon, 2002) enabled by surveillance results in classifications that are “designed to influence and to manage populations and persons thus directly and indirectly affecting the choices and chances of subjects. The gates and barriers that contain, channel, and sort populations have become virtual” (p.13). Lyon (2006) further argues that these activities cannot be disengaged from political or ethical tasks.

Hau‘oli and Alana were also concerned that corporations would manipulate the data in order make a profit at the expense of consumers. Although both tenants and landlords noted that having personalized records of one’s data use could be helpful in assuring individuals were paying their fair share, there was also concern that it could lead to unjust discrimination. For example, a landlord might say, “‘Oh there’s too many people in that household that are using energy…a particular item or appliance… you really need to cut down.’ Or the residential community tells you to cut your appliance [use] or they’ll find other tenants” [Hau‘oli].

Although none of the participants acknowledged a medical condition that they felt would lead to discrimination, over half of them mentioned a concern about health-related data being inferred from the smart meters. Niele said that, “it’s kind of horrible, because if I am using some type of medical device, then they’ll be able to know as well. That’s a lot of personal data!” This was further elaborated by Keahi:

> I think something that would be troublesome is the type of devices that companies are collecting data from, the energy use itself would not be troublesome, but perhaps it could give clues to the types of devices that people have in their homes. So, for example, if you have a certain health problem, and a certain device is used in the home is used to help you, then companies could access or make assumptions or inferences into the types of health problems you have, then I see the trouble there.

Granular smart grid data may infer a variety of health-related data and will link behaviors occurring in the home to the previously-protected realm of medical information. Laws related to medical data, such as HIPAA (United States), do not address the data or actors in this case, as the protected health information (PHI) in the Privacy Rule is very limited. Therefore, there is little to prevent the collection or sharing of this information and it will likely be aggregated with other of search and purchasing behaviors linked to online profiles. For example, Hill (2012) notes that data aggregators, such as Target, are able to infer things about customers' health by combing through data. For example, a teenager buying unscented hand lotion, in conjunction with other seemingly-innocuous data, triggered a pregnancy-related advertisement to be sent to her home during the early stages of her pregnancy. Other data may include de-identified tracking information collected during web browsing and that may be re-identifiable when aggregated. The National Institute of Standards and Technology (2010b) notes that insurance companies would be interested in using this data to adjust health care premiums or deny coverage based on private behaviors that might indicate risk of higher health costs.

Other Sensitive Behaviors

In addition to jeopardizing the privacy of discreet personal data related to health, granular data collection and sharing may also expose sensitive behaviors related to political belief or activity, or any other personal information that could be used to disadvantage certain individuals or groups by corporations or governments. The potential issues that arise from this include political and economic discrimination, as well as limiting citizens' freedom of access to information or ability to discuss issues relevant to democratic decision-making in their communities (Winter, 2013). Therefore, this poses a grave risk to constitutional freedoms and civil liberties, and it contributes to a chilling effect on free speech, fostering a society where citizens cannot freely express their opinions due to surveillance concerns. The erosion of the private sphere threatens both privacy and anonymity when engaging in public affairs, and therefore may hinder citizen participation in democratic discourse. Niele, a foreign national who recently acquired U.S. citizenship via marriage, also imagined a scenario in which immigration officials might use energy data to corroborate her claim to be living with her husband, a U.S. citizen. She emphasized that she and her husband had been living together for over fifteen years before they married, and they themselves would likely not have been affected, but she worried that data errors or incorrect inferences could be used to deny citizenship to others.

CONCLUSIONS

This study examined citizens' perspective about customization and privacy in the context of residential smart meters. Using Nissenbaum's framework of contextual integrity to analyze citizens' perceptions about changes in the key actors involved, information attributes, and principles of transmission, a number of points where existing norms about the collection and use of personal information will potentially be violated in everyday interaction with smart meters in the home were identified. A common theme was that participants were in favor of the feedback, potential cost savings, and potential environmental benefit of smart meter implementation, but only where the data collected and shared contributed to those specific goals: "As long as the 'smart' is for the betterment of a community of people versus profit" [Hau'oli].

This study identified several instances where existing norms about the use of one's personal data may be transgressed. In the case of such a conflict, the framework of contextual integrity calls for evidence that new practices are superior, with the onus of proof being placed on advocates of the new practice. Smart grid/meter advocates must demonstrate that citizens' freedom to express political views, engage in information seeking necessary to take part in communal decisions, and freedom to go about their legal, daily activities without fear of surveillance will be protected. In this case, the practices flagged in analysis represent an undemocratic shift in power, erosion of personal autonomy, and threat of unjust discrimination. Therefore lacking moral legitimacy, these developments should be rejected in their current form.

Citizens should have more awareness and control in managing personal data flows, be aware of what data is being collected about them, and have a say in whether it will be shared with any other entity. The findings of this study highlight the need to identify how much, and what types of, information is required to provide meaningful insights and feedback to power consumers versus what is being sold to data aggregators and has no larger community benefit (or poses a community detriment). Principles such as necessary legitimation, purpose specification and limitation, and data minimization as outlined in the European Union's data protection legislation (Pallas, 2012) would mitigate many of the threats identified in this study. In the United States there is, at present, no meaningful legal protection, particularly against corporate intrusions against personal data. In addition to regulatory protections, privacy must be introduced during the earliest stages of system development and be maintained throughout the lifecycle of personal information (Cavoukian & Kursawe, 2012). Privacy by design is a framework adhering to personal privacy protection principles while enabling necessary data collection and analysis. In their case study of smart grid implementation, Cavoukian and Kursawe (2012) concluded that utilities should be required to conduct privacy impact assessments and subsequently collect only data that is necessary for these primary purposes. Further, citizens should not be forced to choose between privacy and energy conservation. A smart grid designed with privacy at its core can serve diverse goals and contexts and provide citizens with the assurance that their data is well-protected. Uncertainties about smart grid security and the accuracy and reliability of data aggregation, and economic and political motives to gather data indiscriminately for later mining will only increase the tension between personal privacy and smart meters. Even though HECO will initially allow people to opt-out of smart meter installation, there is potential discrimination due to citizens being denied the more desirable aspects of the developments (which may include economic or other benefits). It is important to understand citizen concern and to develop systems and policies that accord with social norms and expectations. For example, technical standards, regulations, and laws, should allow more transparency and control. More attention should be focused on how the smart grid is not merely infrastructure but a network that shapes social, political, and economic relations.

REFERENCES

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*, 2787-2805.

Barringer, F. (2011 January 30). "New electricity meters stir fears. *The New York Times*. Retrieved from: http://www.nytimes.com/2011/01/31/science/earth/31meters.html

Bleicher, A. (2010). Privacy on the smart grid. *IEEE Spectrum*. Retrieved from: http://spectrum.ieee.org/ energy/the-smarter-grid/privacy-on-the-smart-grid

Brinkhaus, S., Carluccio, D., Greveler, U., Justus, B., Löhr, D., & Wegener, C. (2011). Smart hacking for privacy. 28th Chaos Communication Congress. Retrieved from: http://events.ccc.de/congress/2011/Fahrplan/attachments/1968_28c3-abstract-smart_hacking_for_privacy.pdf

Cavoukian, A., & Kursawe, K. (2012). Implementing privacy by design: The smart meter case. *Proceedings of the 2012 IEEE International Conference on Smart Grid Engineering* (pp. 1-8). Piscataway, NJ: IEEE.

CERP-IoT. European Union, Cluster of European Research Projects on the Internet of Things. (2010). *Vision and challenges for realising the Internet of Things.* Brussels: European Commission – Information Society and Media.

Chopra, A. (2011, September 15). Modeling a green energy challenge after a blue button. Retrieved from: http://www.whitehouse.gov/blog/2011/09/15/modeling-green-energy-challenge-after-blue-button

Christakos, H.A., and Mehta, S.N. (2002). Annual review of law and technology. *Berkeley Technology Law Journal, 2002*, 473.

Department of Energy. (2011, November). Recovery Act selections for smart grid investment grant award. Retrieved from: http://energy.gov/oe/technology-development/smart-grid/recovery-act-smart-grid-investment-grants

Depuru, S.S., Wang, L. Devabhaktuni, V., & Gudi, N. (2011). Smart meters for power grid: Issues, advantages, and status. *Renewable and Sustainable Energy Reviews, 15*(6), 2736-2742.

Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine, 8*(1), 18-28.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology, 2005*(7), 185-200.

Gymrek, M., McGuire, A.L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying personal genomes by surname inference. *Science, 339*(6117), 321-324.

Haggerty, K.D., & Ericson, R.V. (2006). The new politics of surveillance and visibility. In K.D. Haggerty and R.V. Ericson (Eds.) *The new politics of surveillance and visibility* (pp. 3-25). Toronto: University of Toronto Press.

Hawaiian Electric Company. (2008). Hawaiian Electric selects Sensus FlexNet AMI: Success of pilot projects results in definitive agreement. [Press release]. Retrieved from: http://www.heco.com/vcmcontent/StaticFiles/pdf/Sensus_AMI_HECO_12-23-08_FINAL.pdf

Hill, K. (2012, February 16). "How Target figured out a teen girl was pregnant before her father did." *Forbes*. Retrieved February 22, 2012, from http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Innovation Electricity Efficiency Institute. (2013, August). *Utility-scale smart meter deployments: A foundation for expanded grid benefits*. Washington, D.C.: Innovation Electricity Efficiency Institute. Retrieved online from http://www.edisonfoundation.net/iee/Documents/IEE_SmartMeterUpdate_0813.pdf

Jaimes, A. (2010). Data mining for user modeling and personalization in ubiquitous spaces. In H. Nakashima, H. Aghajan, and J.C. Augusto, (Eds.) *Handbook of ambient intelligence and smart environments* (pp. 1015-1038). London: Springer-Verlag.

Khan, R., Khan, S.U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. 10th International Conference on Frontiers of Information Technology, pp. 257-260. DOI: 10.1109/FIT.2012.53

Kling, R. (2000). Learning about information technologies and social change: The contribution of social informatics, *The Information Society, 16*(3), 217-232.

Kostyk, T., & Herkert, J. (2012). Societal implications of the emerging smart grid. *Communications of the ACM, 55*(11), 34-36.

Luppicini, R. (2009). The emerging field of technoethics. In R. Luppicini & R. Adell (Eds.) Handbook of research on technoethics (pp. 1-19). Hershey, PA: IGI Global.

Lyon, D. (2002). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.) Surveillance as social sorting: Privacy, risk and automated discrimination (pp. 14-30). London, UK: Routledge.

Lyon, D. (2006). The search for surveillance theories. In D. Lyon (Ed.) *Theorizing surveillance: The panopticon and beyond* (pp. 3-20). Portland, OR: Willand.

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy, 7*(3), 75-77.

Mills, E. (2012 Jan 24). Researcher find smart meters could reveal favorite TV shows. Retrieved from http://www.cnet.com/news/researchers-find-smart-meters-could-reveal-favorite-tv-shows/

National Institute of Standards and Technology. (2010a). *Guidelines for smart grid cyber security: Vol. 2, Privacy and the smart grid*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology. (2010b). Introduction to NISTIR 7628: Guidelines for smart grid cyber security. Gaithersburg, MD: NIST.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Ca.: Stanford University Press.

Pallas, F. (2012). Data protection and smart grid communication – the European perspective. *Proceedings of the 2012 IEEE Innovative Smart Grid Technologies Conference*, 1-8. New York: IEEE.

Pew Research Center for the People and the Press. (2013). Few see adequate limits on NSA surveillance program. Retrieved October 25, 2013, from http://www.people-press.org/ files/legacy-pdf/7-26-2013%20NSA%20release.pdf

Raftery, T. (2013, October 10). Utilities should open up API's to their smart meter data. [Blog post]. Retrieved from: http://greenmonk.net/2013/10/10/utilities-should-open-up-apis-to-their-smart-meter-data/

Shimogawa, D. (2014, Mar 11). "Hawaiian electric to install smart meters on Oahu." *Pacific Business News*. Retrieved from: http://www.bizjournals.com/pacific/news/ 2014/03/11/hawaiian-electric-to-install-smart-meters-on-oahu.html

Solove, D. (2010). *Understanding privacy*. Cambridge, MA.: Harvard University Press..

Stahl, B.C., Heersmink, R., Goujon, P., Flick, C., van den Hoven, J., Wakunuma, K.J., Ikonen, V., & Rader, M. (2010). Identifying the ethics of emerging information and communication technologies: An essay on issues, concepts and methods. *International Journal of Technoethics, 1*(4), 20-38.

State of Hawaii, Department of Business, Economic Development & Tourism. (2011). Renewable energy in Hawaii. Periodic research and data reports on issues of current interest, economic report 2011 (June, 2011). Honolulu: Department of Business, Economic Development & Tourism.

St. John, J. (2014, March 13). Hidden treasure: Two new resources offer up massive amounts of utility data. *Greentechgrid*. Retrieved from: https://www.greentechmedia.com/articles/ read/Energy-Data-Treasure-from-Chattanoogas-Smart-Grid-Incubator-and-Pecan-Str

Tendril. (2012, January 20). NYC Cleanweb Hackathon: Crowdsourcing killer energy apps. Retrieved from: http://www.tendrilinc.com/blog/nyc-cleanweb-hackathon-crowdsourcing-killer-energy-apps

Turow, J. (2006). Cracking the consumer code: Advertisers, anxiety and surveillance in the digital age. In K.D. Haggerty and R.V. Ericson (Eds.) *The new politics of surveillance and visibility* (pp. 279-307). Toronto: University of Toronto Press.

Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and worth*. New Haven: Yale University Press.

Uckelmann, D., Harrison, M. & Michahelles, F. (2010). An architectural approach towards the future Internet of Things. In D. Uckelmann et al. (Eds.), Architecting the Internet of Things. Berlin: Springer-Verlag Berlin Heidelberg.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I.S., Mazura, M., Harrison, M., Eisenhauer, M., & Doody, P. (2011). Internet of Things strategic research roadmap. In O. Vermesan & P. Freiss. (Eds.), *Global technological and societal trends from smart environments and spaces to green ICT*, (pp. 9-52). Aalborg: River Publishers.

Weber, D.C. (2012). Looking into the eye of the meter. Presentation at DEFCON 2012. Retrieved from: https://www.youtube.com/watch?v=HeoCOVXRX0w

Weber, R.H., & Weber, R. (2010). *Internet of Things: Legal perspectives*. Berlin: Springer-Verlag Berlin Heidelberg.

Winter, J.S. (2013). Cloud-based facial recognition: Establishing the citizen at the center of policy and design. Paper presented at the International Communication Association Annual Conference. June, 2013, London.

Winter, J.S. (2014). Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. *Ethics and Information Technology*, *16* (1), 27-41.