Social Science Research 51 (2015) 64–76

Contents lists available at ScienceDirect

Social Science Research

journal homepage: www.elsevier.com/locate/ssresearch

Privacy, technology, and norms: The case of Smart Meters

Christine Horne [a,*], Brice Darras [a], Elyse Bean [a], Anurag Srivastava [b], Scott Frickel [c]

[a] Department of Sociology, Washington State University, United States
[b] School of Electrical Engineering and Computer Science, Washington State University, United States
[c] Department of Sociology, Brown University, United States

ARTICLE INFO

Article history:
Received 18 October 2013
Revised 30 September 2014
Accepted 4 December 2014
Available online 16 December 2014

Keywords:
Social norm
Privacy
Smart Meter
Technology

ABSTRACT

Norms shift and emerge in response to technological innovation. One such innovation is Smart Meters – components of Smart Grid energy systems capable of minute-to-minute transmission of consumer electricity use information. We integrate theory from sociological research on social norms and privacy to examine how privacy threats affect the demand for and expectations of norms that emerge in response to new technologies, using Smart Meters as a test case. Results from three vignette experiments suggest that increased threats to privacy created by Smart Meters are likely to provoke strong demand for and expectations of norms opposing the technology and that the strength of these normative rules is at least partly conditional on the context. Privacy concerns vary little with actors' demographic characteristics. These findings contribute to theoretical understanding of norm emergence and have practical implications for implementing privacy protections that effectively address concerns of electricity users.

1. Introduction

In recent decades scholars across disciplines have sought to explain the emergence of norms – informal rules governing behavior that are socially enforced (Horne, 2001). A prominent approach focuses on the consequences of behaviors (Demsetz, 1967; Coleman, 1990; Fehr and Gächter, 2002; Heckathorn, 1989; Yamagishi, 1986). It suggests that if a behavior creates negative consequences for others, then people are likely to view the behavior negatively; in other words, there will be a *demand* for norms that constrain the behavior. People will presumably also *expect* that others will view the behavior negatively. But, some researchers have also argued that norms are conditional (Fine, 2001; Hechter and Opp, 2001; Jasso and Opp, 1997). That is, the same (harmful) behaviors may lead to different reactions and expectations depending on the social context (Ocantos et al., 2013; Edmonds, 2014). Relatively little research explicitly tests this argument, however. In this paper, we seek to address this gap by examining the effects of behavior consequences across contexts in a substantively important domain – privacy and technology.

Technological innovation has created unprecedented potential for invasions into individuals' privacy (Culnan and Bies, 2003). While voices in popular media argue that privacy is dead (e.g., Hill, 2010), scholars find that Americans are very concerned about privacy and engage in strategic actions to try to protect it (e.g., boyd and Marwick, 2011). Privacy is thought to create boundaries that are essential for structuring social interactions (Nippert-Eng, 2010). And many believe that social life is not possible (or enjoyable) without some level of privacy – privacy is necessary for human flourishing (see, e.g., Cohen, 2000; Gandy, 2007).

* Corresponding author at: Department of Sociology, 204 Wilson-Short Hall, Washington State University, Pullman, WA 99164, United States.
E-mail address: chorne@wsu.edu (C. Horne).

http://dx.doi.org/10.1016/j.ssresearch.2014.12.003
0049-089X/

The connection between technology and privacy is widely recognized (see, e.g., Rule, 2007; Bennett, 2008; see also Marx, forthcoming on technology and control). However, despite the large literature identifying threats to privacy that new technologies create, we have much to learn about the links between technological innovation, privacy threats, and emerging norms (Marx and Muschert, 2007).

In this paper, we draw on theory and insights from the norms and privacy literatures to explain norms that arise in response to emerging technologies, using Smart Meters as a test case. Smart Meters are a key part of the Smart Grid, an assemblage of new technologies designed to increase the efficiency and reliability of the electric power grid. Installed in peoples' homes, Smart Meters transmit information about consumer electricity use to utility companies at short intervals of 15 minutes or less. In the aggregate, this information may help utility companies to increase the efficiency and reliability of the grid (Quinn, 2009). But detailed information about household electricity consumption generated by Smart Meters can also be used to estimate the composition and behavior of individual households (Smart Grid Interoperability Panel, 2010). Further, technology can enable utility companies to remotely control smart appliances within the home. Implementation of Smart Meters is expanding rapidly, with over 25 million U.S. homes currently using Smart Meters (Karlin, 2012) and 65 million predicted by 2015 (Edison Foundation, 2013). As a result, utility companies across the country are gaining unprecedented access to information about customers as well as the technical ability to intervene in residents' homes. Concern with such potential threats to privacy has been associated, in some cases, with failure of Smart Grid initiatives (see, e.g., Connecticut Light and Power's Plan-It Wise Energy Program; and U.S. Energy Information Administration, 2011).

Drawing on the privacy literature, we identify potential threats to individual privacy that may be created by smart technology. Building on the research on norm emergence, we predict that these threats will produce a demand for norms as well as norm expectations opposing Smart Meters, and that this effect is conditional. We test our hypotheses using a series of vignette experiments that examine how demand for and expectations of norms shift in response to varying levels of privacy intrusion and contributions of the technology to the shared goals of the actors involved. We also conduct exploratory analyses that examine whether the effects of privacy intrusion differ depending on the demographic characteristics of participants. Our results suggest that the increased risks to privacy created by Smart Meters are likely to provoke opposition, that these effects persist across age groups and other demographic characteristics, and that they are at least partially conditional. These findings contribute to understanding of technology and norm emergence and have practical implications for addressing consumer privacy concerns.

2. The Smart Grid context

The U.S. electric grid infrastructure is operating near capacity and needs a major upgrade (Joskow, 2012). Unanticipated changes in consumer demand in a system operating near the margin with increasing loads, aging infrastructure, increased integration of renewable energy, and lack of coordination can result in major system failures, such as the 2003 Northeastern blackout which left over 50 million people without power for up to two days (and in some cases up to a week) and cost an estimated seven to ten billion dollars (Electricity Consumers Resource Council, 2004). In that situation, because utility companies lacked immediate access to information about the state of the system and were therefore unable to quickly or effectively reroute electricity flow, functioning power lines overloaded quickly, causing an outage of significant scale.

In response to these and other problems, Congress passed the Energy Infrastructure and Security Act of 2007 (EISA) (Graab, 2011). Intended to move the U.S. toward greater energy independence and security, Title XIII of EISA focused specifically on the Smart Grid, calling for a range of technological improvements as well as creating a Smart Grid Task Force (Graab, 2011). Two years later, the American Recovery and Reinvestment Act of 2009 allocated $4.5 billion for Department of Energy projects focused on Smart Grid development. Utility companies matched the federal funds with an additional $5.5 billion of private industry funding, accelerating development and deployment of Smart Grid technology (Joskow, 2012). The Smart Grid's enhanced monitoring capabilities address problems of the old grid (such as its limited response capability), while also making it easier to incorporate renewable energy resources such as wind and solar power into the energy system.

Smart Meters are a significant part of the larger Smart Grid infrastructure, and have been installed in over 25 million U.S. homes (Karlin, 2012). Smart Meters transmit information about consumer electricity use to utility companies at vastly shorter time intervals than before. Data can be transmitted to the utility company on a minute-to-minute basis, rather than being read once a month by a meter reader going to each home. This information helps utility companies to coordinate power supply and demand, detect outages, implement time-of-use and dynamic pricing, and in other ways improve system efficiency and reliability (Quinn, 2009). Smart Meters have the potential to enable users to closely monitor their power use through the internet or smart phone applications, giving home owners and business managers information that may help them to reduce their energy consumption. In the aggregate, these savings can significantly reduce national energy use and curb energy emissions while addressing pressing geopolitical and environmental concerns related to energy security and sustainability (Graab, 2011). Thus Smart Meters contribute to the technical capacity of utility companies to manage demand (through demand response programs), incorporate renewable sources of electricity into the system, and increase the overall efficiency and reliability of the system. The system-level benefits of the Smart Grid are clear – at least for policy-makers and energy professionals. The reactions of end-users of electricity, and the implications of privacy threats associated with Smart Meters for norms, are more difficult to predict.