Ethics Inf Technol (2014) 16:27–41
DOI 10.1007/s10676-013-9332-3

ORIGINAL PAPER

Surveillance in ubiquitous network societies: normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things

Jenifer Sunrise Winter

Published online: 16 November 2013

Abstract The Internet of Things (IoT) is an emerging global infrastructure that employs wireless sensors to collect, store, and exchange data. Increasingly, applications for marketing and advertising have been articulated as a means to enhance the consumer shopping experience, in addition to improving efficiency. However, privacy advocates have challenged the mass aggregation of personally-identifiable information in databases and geotracking, the use of location-based services to identify one's precise location over time. This paper employs the framework of contextual integrity related to privacy developed by Nissenbaum (Privacy in context: technology, policy, and the integrity of social life. Stanford University Press, Stanford, 2010) as a tool to understand citizen response to implementation IoT-related technology in the supermarket. The purpose of the study was to identify and understand specific changes in information practices brought about by the IoT that may be perceived as privacy violations. Citizens were interviewed, read a scenario of near-term IoT implementation, and were asked to reflect on changes in the key actors involved, information attributes, and principles of transmission. Areas where new practices may occur with the IoT were then highlighted as potential problems (privacy violations). Issues identified included the mining of medical data, invasive targeted advertising, and loss of autonomy through marketing profiles or personal affect monitoring. While there were numerous aspects deemed desirable by the participants, some developments appeared to tip the balance between consumer benefit and corporate gain. This surveillance power creates an imbalance between the consumer and the corporation that may also impact individual autonomy. The ethical dimensions of this problem are discussed.

Keywords Privacy · Surveillance · Internet of Things · Framework of contextual integrity · Radio-frequency identification (RFID) · Location-based services (LBS)

J. S. Winter (✉)
School of Communications, University of Hawai'i at Mānoa, 2550 Campus Road, Crawford 325, Honolulu, HI 96822, USA
e-mail: jwinter@hawaii.edu

Introduction

The Internet of Things (IoT) is an emerging global infrastructure that employs radio frequency identification (RFID), near field communication (NFC), and related technologies to "enable the Internet to reach out into the real world of physical objects" (Internet of Things Conference Organizing Committee 2010). RFID is a short-range, wireless technology that allows the transfer of data stored on a chip attached to an object, while NFC is a standard enabling the exchange of data between mobile communication devices in close proximity. There is no single definition for the IoT—rather, it describes a variety of developments in which everyday objects can be tagged, and using standards enabling unique identification, communicate over the Internet. Weber and Weber (2010) see the IoT 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" (p. 1). Thus, it can be seen as a global architecture permitting enhanced intelligence to facilitate the exchange of goods and services. In addition to networking objects for supply chain management, the ubiquitous integration of tags and sensor networks may also be employed in smart appliances, smart homes, and in vivo health applications.

Visions of the IoT rely, in part, on the rapid increase in the amount of data collected and exchanged due to an explosion in the number of communication devices, what The European Commission, Information Society and Media (2008) refers to as a "data deluge" (p. 6). These data are increasingly being used in the manipulation of personal information, or "dataveillance" (Clarke 1988), in business intelligence and consumer marketing, and the IoT will likely magnify this trend. Further, the goals of IoT development include empowering computers "with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data" (Ashton 2009, para. 5). Thus, the potential impacts of automated data gathering and data mining must also be considered.

These developments are being marketed to citizens and governments as a means toward greater efficiency, safety, and convenience, as well as an important enabler for developing new services with user-generated content. In addition to the data deluge, RFID makes it possible to harvest a wide array of new data types, enabling data mining to predict consumer behavior, improve supply chain management, and monitor other aspects of the physical environment. However, a great deal of concern has been generated about privacy issues related to the IoT and related technologies. Opponents highlight issues such as the mass aggregation of personally-identifiable information in databases and geotracking, the use of location-based services to identify one's precise location over time.

Although the surveillance potential of modern information and communication technologies (ICTs) is widely acknowledged, the IoT poses several unique challenges to privacy. First, because many of its components are small and not necessarily visible, one potentially does not know when and where data is being collected. This complicates regulatory or technical schemes that rely on consumer consent. Second, because billions of everyday objects, or even the human body itself, can be equipped with sensors, there are many new types of data that can be collected. Third, because it is part of a global Internet-based system, data can potentially be aggregated and linked to other personally-identifiable records. Patterns can be sought in information that was previously not available for analysis. Increasingly, global flows of information make it possible for this personal data to be accessed by a variety of sources. As Floridi (2005) observes, modern ICTs do not merely increase the quantity and quality of data collected; they are part of an "unprecedented transformation in the very nature (ontology) of the information environment" (p. 186). Modern ICTs transform humans into informational agents. In this emerging environment, each individual is constituted by his or her personal information, and breaches of this information are seen as aggression towards a person's identity (Floridi 2005). Further, machine intelligence may be used to both collect and analyze these data, increasing both the scale and analytic capacity of these systems and introducing a greater risk of error due to imperfect algorithms used to consolidate and make sense of the data. These attributes have led to growing recognition of a need for technical standards and governance to "build trust and confidence in these novel technologies rather than increasing fears of total surveillance scenarios" (The European Commission, Information Society and Media 2008, p. 3).

When considering the IoT, it is important to acknowledge that it is an emerging environment that cannot be explicitly examined in situ. However, it is not entirely "in the future". Importantly, Dourish and Bell (2011) point out that infrastructures are messy and in constant flux—"thinking of infrastructure as stable, uniform, seamless, and universally available is clearly problematic" (pp. 28–29). The framework for the IoT already exists and features of it are already employed in limited ways. This is emphasized, as ubiquitous computing environments are often envisioned as occurring only in the future, while it is necessary to examine them as they emerge in order to design policies and systems that respect citizen concerns.

This paper outlines concerns about privacy and surveillance related to the IoT, addresses legal constraints related to the IoT, and introduces the framework of contextual integrity related to privacy developed by Nissenbaum (2010). The methodology used to explore normative conflicts related to the consumer in-store supermarket experience in the context of the IoT is then described, followed by a results and discussion section that outlines conflicts with novel practices related to the IoT.

Privacy, surveillance and legal constraints

The IoT generates many ethical questions related to privacy and surveillance. While privacy is often acknowledged a human right, there is no consensus about what privacy entails or how it can be adequately addressed in policy and law. Lyon (2006) highlights the complexity and ambiguity of surveillance in the Risk Society, noting that it is manifest in a variety of agendas and institutions. Modern society is characterized by risk, which is essentially a systematic method of handling the various threats introduced by the advance of ICTs and other technologies (Beck 1992). Risk Society theorists argue that we live in an era imbued by risks that are willfully initiated by humans in order to attain technological progress. Problems are not merely technological, but are institutional, embedded in

processes that place little value on public opinion or concern. Thus, specific contexts must be carefully observed to explore at what point surveillance activity represents an imbalance of power. Winseck (2003) calls the mandate of managing this risk "netscapes of power", which he describes as "mediascapes designed to buttress market power and to regulate behavior through network architecture" (p. 176). Media consolidation and a restructuring of network architecture and content have enabled large corporations to shape citizens' uses of the Internet and to manage uncertainty through surveillance and control of information.

Lyon (2006) emphasizes that "surveillance theory cannot ultimately be disengaged from the ethical and the political tasks" (p. 18). Because there will be marked changes in the types and amount of data collected, and the analyses used to exploit them, the IoT is certain to be a hotbed of ethical concerns. At national or regional levels, the IoT is becoming integral to ICT policy initiatives, and privacy concerns are being addressed in various ways. In 2010, China's Ministry of Industry and Information Technology (MIIT) announced plans to make the IoT a key component of IT policy and intends to strengthen relevant financial and taxation measures ("China working on unified national IoT strategic plan" 2010 July 5); however, there is as of yet no specific legal protection. In contrast, the European Union has long had a comprehensive data protection scheme and, in conjunction with its resolution to support IoT development, recently formally addressed privacy concerns about the IoT, adopting an agreement called the Privacy and Data Protection Impact Assessment Framework for RFID Applications as a means to safeguard citizen privacy (O'Connor 2011).

In the United States, there is no comprehensive law protecting consumer privacy. At the federal level, the *Electronic Communications Privacy Act* (1986) does not adequately address modern information technologies, data aggregation and exchange, and novel information practices. Instead, United States citizens must rely largely on corporate self-regulation and a number of sector-specific privacy laws (e.g., those governing health records). This has not been successful in allaying concern: In December of 2010 and March 2012, the Federal Trade Commission released reports proposing guidelines consumer privacy (Federal Trade Commission 2010, 2012), and growing concern about abuse of consumer records has recently led to proposals in Congress to reform the 1986 *Act*.

Weber and Weber (2010) note the legal challenges surrounding privacy and IoT development. A first question is whether there is a need for laws to govern these changes or if business self-regulation will suffice. Then, if legislation is the chosen path, are existing laws sufficient? Finally, if new laws are needed, "what kind of laws are required and what is the time frame for their implementation?" (p. 52). It is important to consider that blanket approaches that rely on a dichotomy between "public" and "private" data may fail to account for certain instances where citizens feel their privacy expectations have been violated. Many definitions of privacy and information protection focus on this dichotomy. For example, in the United States, the Fourth Amendment protects against unreasonable search and seizure. In the Supreme Court case *Kyllo v. United States*, law enforcement's use of then-novel heat scanners to detect illegal marijuana cultivation within the home was deemed unconstitutional. The Court stated, "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes" (Christakos and Mehta 2002, p. 473). The protection against intrusion of a private sphere, be it a specific physical location or an abstract domains, is highlighted in a number of laws in the United States, including the *Family Education Rights and Privacy Act* and the *Health Information Portability and Accountability Act* (Nissenbaum 2010). New ICTs are "disorienting as they reveal the inconstancy of boundaries and fuzziness of definitions" (p. 101). The pervasiveness of the IoT, which is anticipated to be thoroughly integrated into the home and daily environment, is certain to pose challenges for this dichotomy between public and private.

This paper addresses how we can better foster the development of new systems, practices, and policies that support citizens' rights to privacy. Following Kling (2000), it is argued that new technologies such as the IoT are not necessarily positive or negative but must be assessed in specific context. The framework of contextual integrity related to privacy developed by Nissenbaum (2010) is employed as a tool to understand citizen concerns about IoT-related technologies. Specifically, the purpose of the study is to identify and understand specific changes in information practices that will be brought about by the IoT and may be perceived as privacy violations by citizens and to reflect on the underlying norms that shape their perceptions. Understanding these perspectives is important to inform both context-sensitive design and policy, ensuring that these decisions have moral legitimacy.

The framework of contextual integrity

Nissenbaum (2010) describes the right to privacy not as a right to secrecy or control, but to "appropriate flow of personal information" or contextual integrity (p. 127). Addressing Facebook executive Mark Zuckerberg's claim that privacy is no longer a social norm (Barnett 11 Jan 2010), she proposes the framework in order to guide assessment of new practices arising from technical systems. 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 IoT and its related practices.

The framework of contextual integrity is intended to be employed as a descriptive and heuristic tool that helps account for people's reactions to novel, or changing, technical systems that affect flows of personal information. The framework also aids evaluation of these systems' moral and political values. Nissenbaum (2010) emphasizes that norms may vary substantially according to context. Depending on the goals embedded in the context, new systems may lead to conflicts among moral and political values, including various information harms, unjust discrimination, and threats to autonomy and liberty (Nissenbaum 2010).

Nissenbaum argues that "privacy is worth taking seriously because it is among the rights, duties, or values of any morally legitimate social and political system" (p. 66). She claims special moral standing for entrenched norms as they are confronted with novel practices that conflict with them. What is important is not whether a technology is new, or accepted, overall, but how, in a particular context, it may come into conflict with underlying norms. In Nissenbaum's framework, the question becomes, do novel practices "violate context-relative informational norms?" (p. 148). Norms here are prescriptive, indicating how one ought to behave in a given context. Norms are embedded in systems; thus, they should be considered in context to avoid identification of those that are arbitrary or questionable. To address whether violations have occurred, a comparison must be made between the existing practice and the new practice. Then, "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). Contextual integrity is violated when informational norms are breached. However, detection of a violation does not necessarily mean that the development is unjust or lacks moral legitimacy; rather, it indicates that it should be assessed morally in order to determine whether the new practice is acceptable or should be challenged. It is important to highlight that there may be some instances where the violation, after assessment, is deemed a morally superior practice. Existing normative practices must be compared against novel alternatives to determine

> How effective each is in supporting, achieving, or promoting relevant contextual values. If the practices prescribed by entrenched informational norms are found to be less effective than the challengers, or, in the cases of particular interest here, less effective than novel practices resulting from newly deployed sociotechnical devices and systems, this constitutes a moral justification for replacing entrenched practices with novel challengers (Nissenbaum 2010, p. 166).

To measure whether a novel practice is morally or politically superior, we begin by considering general moral and political considerations relevant to privacy. These come from a wide range of perspectives addressing the value of privacy, including protection against informational harms, defense of personal autonomy, ensuring fairness, justice, and equality, and support of democratic institutions and publics. A second step is to consider values, ends, purposes, or goals relative to the specific context. Nissenbaum draws on Dworkin's (1986) concept of legal integrity as a source of moral legitimacy of a society's legal system to argue that, a practice has moral legitimacy if the flows of information adhere to context-sensitive informational norms: "there is a presumption in favor of entrenched rules rather than strict adherence to the letter that can be overridden if new practices are demonstrably more effective at achieving contextual values, ends, and purposes or the equivalent" (Nissenbaum 2010, p. 179)

The framework of contextual integrity is useful in understanding people's reactions to information technologies reshaping personal information flows and can be helpful in explaining resistance and fear in response to these changes. As such, it can be useful both in predicting when changing practices are likely to lead to concern or conflict, and it also assists in identifying the anxieties or concerns leading to objection, highlighting these new practices for ethical evaluation. The contextual integrity decision heuristic is the process of describing the new practice in context, along with changes in actors, attributes, and transmission principles; identifying entrenched norms and how the new practice may conflict with these; identifying whether informational norms have been breached (i.e., a violation of contextual integrity); evaluating based on moral and political factors (e.g., shifts in power structures, implications for justice or democracy); evaluating moral and political factors in according to contextual values; and recommending in favor of, or against, specific systems or practices under study (Nissenbaum 2010).

Methodology

The framework of contextual integrity was employed in this study to identify areas of concern related to emerging practices related to the IoT, highlighting them for ethical evaluation. This study addressed normative conflicts related to the consumer in-store supermarket experience in the context of the IoT. The supermarket was chosen for analysis because it is a site for a constellation of everyday tasks that are not typically associated with a great deal of

privacy concern. Supermarkets have long been a location to purchase food and sundry items and, with expanding corporate alliances, they have begun to offer more sensitive items such as alcohol, video rentals, and prescription drugs. While it is common to encounter other people, both shoppers and employees, there is also an expectation that other people will not be able to analyze the totality of your purchases over time. Furthermore, information exchanges in this context are not, at present, explicitly protected by United States federal privacy laws.

To explore citizens' perception about context-specific norms of privacy related to the in-store shopping experience, in-person, semi-structured interviews were administered. Interviews were employed so that the same sets of questions could be addressed in each interview, while allowing the flexibility to follow unanticipated paths as they emerged. Participants were elicited based on their status as citizens of the State of Hawaii, having visited a supermarket during the past month, and being self-described users of location-based services on a mobile device. Location-based services allow program-level software to identify a person or object's location, and many smartphones use this information to provide maps and navigation services or to share geospatial data for entertainment or work purposes. The IoT draws on geospatial data as embedded objects change location, so existing familiarity with these services was seen as advantageous (and indicated that the content under study would not likely be too abstract for participants to imagine). As this was an exploratory study, maximal variation sampling was used to select participants reflecting a diversity of perspectives based on age, ethnicity, gender and occupation. This study focused on the City & County of Honolulu, which includes Hawaii'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 range, and ethnicity) were saturated, participants in other categories were sought. Interviews were conducted in public locations, at the discretion of the interviewees, and lasted between 40 and 75 min.

The development of interview questions and analysis was guided by the analytic framework of contextual integrity (Nissenbaum 2010). In order to establish the prevailing conditions, participants were first asked to recall a specific, recent supermarket visit. Interview questions then sought to gain insight into their perception of *information attributes*, what types of data they thought might have been collected about them during this visit. This included their perception of (1) what data may have been collected when they arrived; (2) if they were there with any other individuals; (3) what they looked at or touched; and 4) what they bought. A second set of questions asked participants about the *actors* involved, who they thought had observed these behaviors (human or electronic), and who had access to it or 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 scenario describing a visit to the supermarket in the year 2021. A scenario is an imaginary environment or sequence of events, a story about the future (Schwartz 1996). Because the IoT is not fully implemented at this time, it was important to displace participants from a present-focused mindset and enable them to explore this future environment. Scenarios are used widely across disciplines and in corporate strategic planning because they allow one to focus on uncertainties and think creatively about different possibilities that might arise (Glenn 2009). This scenario was set approximately 10 years in the future and described a visit to the same supermarket participants answered questions about in the first section. The scenario described integration of a variety of short-range wireless technologies that enabled everyday objects to communicate over the Internet, more closely linking the real world to cyberspace. The content scenario was drawn from a variety of global IoT developments, including present research initiatives, government risk assessments, and corporate visions, and described the participant visiting the same store that they answered questions about in the first part. The scenario was not presented as a threat; rather, it described how participants might encounter IoT-related developments to make their visit more convenient and secure.

After they were immersed in the scenario, 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 eleven participants representing both genders, and a variety of age groups, occupations, and ethnicities

Table 1 Participants

Name	Gender	Age	Ethnicity	Profession
Anuhea	Female	Mid-twenties	Caucasian	Government IT specialist
Akoni	Male	Late twenties	Hawaiian/Chinese	Clothing company owner
Iolana	Female	Early forties	Chinese/Caucasian	Editor
Kaimi	Male	Early twenties	Japanese	Television board operator
Kainoa	Male	Early twenties	Caucasian	Full-time student
Kepano	Male	Late forties	Caucasian	Truck driver
Keoni	Male	Late fifties	Caucasian/Native American	Mechanic
Maile	Female	Early thirties	Japanese	Librarian
Maka	Male	Early thirties	Chinese/Caucasian	Aircraft pilot
Nahele	Male	Mid-thirties	African-American	Military communications supervisor
Nalani	Female	Early twenties	Caucasian	Full-time student

participated in the in-depth interview process. All participants resided on the island of Oahu and were therefore residents of the City & County of Honolulu. Table 1 provides a summary of participants. (Pseudonyms are used to protect their identities).

Existing practices and expectations

Although the intent of this study was not to understand informants' perception of current supermarket surveillance practices, it was important to identify their present expectations in order to understand how shifting information practices might be perceived as threats. Participants uniformly described their visit to the supermarket as a routine shopping experience where they examined and purchased a variety of items. However, interviewees expressed varied expectations of current information collection practices. All suggested that they felt store employees or other customers might be aware of their arrival or movement throughout the store, but would have limited interest in, or memory of, these encounters. In addition, five participants recalled surveillance cameras on site or related an expectation that they were present. For example, Maile suggested that "If they really wanted to they could go back and check the camera footage." Kepano and Kainoa indicated that they were aware of constant video surveillance from the moment they entered the store, as theft deterrent or to investigate security issues, as well as for possible review for marketing strategies. Kepano also hinted at the use of surveillance footage for other than security purposes: "I'm sure they keep those videotapes around for a while, and I'm sure they're using it for more than just saving my face in case I rob the place." Kainoa explained that he had previously worked in a supermarket and that he believes that surveillance footage may be combed for marketing purposes related to consumer behavior. Participants acknowledged that affiliates might have access to limited data. However, it was emphasized that this would be appropriate only if it were not linked to specific individuals and would be used to improve the consumer experience. There was the expectation that, even though they were in a public place where they might encounter people they knew, activities captured on surveillance footage would be managed discreetly.

All interviewees noted owning a rewards card linked to at least one market chain, and in all but three cases, such a card was used during the visit in question. Maka and Akoni explained that the market they patronized did not offer relevant discounts related to the card, while Nahele visited a commissary (military supermarket) that does not offer a rewards card due to data collection restriction on United States federal sites. With this exception, there was consensus that information about the items they bought was likely stored in some type of electronic database and would be explicitly linked to their identity over time. There was also consensus that use of the rewards card represented an agreement with the supermarket to share limited personal information in exchange for lower prices, special offers and coupons, and more customized suggestions, in part explaining Maka and Akoni's decision not to use their cards when they did not receive these perceived benefits. Informants agreed that the present intent of this gathering was to create a customized experience for the user and to make business operations more efficient in a way that benefitted the consumer—"an acceptable balance", as Nalani described it, or a "fair trade" in Kaimi's words.

Maka, Anuhea, and Kepano mentioned that it would be inappropriate for any of the information gathered about their activities in the store to be used outside the corporation with the exception of law enforcement in the case of criminal investigations. Kainoa indicated it would be inappropriate for any information to be shared outside the immediate site. Further, while all agreed that the store might employ some type of analytic technique to improve recommendations or product placement, participants felt that this should involve data stripped of unique identifiers.

Nahele raised an interesting point related to non-identifiable information used by the government:

> I do remember, and I don't know what this was for, where a kid was buying beer and cigarettes and [the cashier] asked for his ID and actually scanned [it]. They did that for about two months… I think they were recording for some type of DoD [Department of Defense] study… if they see trends – such as "on this post more soldiers purchase alcohol", they use it as an indicator… When a significant portion is deployed and then comes back, there are trends that the government follows.

Overall, participants showed various perceptions of what types of data were being collected, who had access to it, and how it was being stored and transmitted. In general, they expressed the idea that any data their supermarkets were collecting about them were being used for "acceptable" purposes of providing discounts and making the store more efficient, leading to lower prices. It is important to emphasize that these initial descriptions represent, in some cases, an idealized relationship, or what participants thought ought to occur with their data. Although in later parts of some interviews, there was acknowledgement of and concern about third-party data sharing and analysis, only Maile, Kaimi, and Nahele suggested that this was a present practice.

Conflicts with novel practices related to the IoT

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 location-based services, a lack of transparency, inferences about health-related and biometric information, threats to autonomy and identity, and questions about public spaces and the public good.

Location-based services

Location-based services were the component of the IoT that was most salient to participants, since they already had personal experience with these tools and an awareness of related current events, for example recent news stories about Apple and Google using location-based applications on smartphones (e.g., Albanesius 2011). Although all participants willingly used location-based services in some form on their present mobile device, there was a great deal of concern about who would have access to this data in the future. Proposed services that might announce who is in a store at a given time or seek to provide other social networking services during in-store visits were seen as extremely unwelcome. Kaimi emphasized a view shared by several participants, that this is

> not really important information. I would not receive any benefit from sharing this information. It seems like they're doing it so they can advertise themselves, and I don't appreciate that. I am just trying to get some grocery stuff. I don't want to be a walking billboard.

Concern about targeted communications arose as well, as several participants mentioned that they worried that unknown corporate affiliates might reach out to them based on location-based services linked to personal profiles and that these targeted advertisements might be unwanted or difficult to manage. Anuhea pointed out that she already deals with an unacceptable volume of unsolicited advertisements via phone, email, and SMS. Marx (2006) argues that location-based information is particularly sensitive because it can both identify an individual and monitor movement over time.

> The substantive information it provides can be compared to predictive models (or used to build them) that then serve to direct how the individual is responded to…. But it also offers a means of action – knowing where the person is may permit 'reaching' them, either literally, as with 911 responders, or through targeted communications (pp. 97–98).

In addition to corporate sharing of the data, there was also concern that others could access it through illegal means, increasing personal security risks. Keoni worried that unauthorized people might gain access to this information and be able to use it in real-time for burglaries: "they know you're not in your house so they could target you." Anuhea, Nahele, Keoni, and Maka mentioned that, even with laws requiring protection of data, there is a substantial potential for data theft or hacking. Nahele channeled the fears of several participants when he noted "the possibility of a very dangerous stalker with the ability to hack into that system… or someone abusing that information for whatever purpose."

Maile noted that people might be willing to share location-based data with others initially, but that this could have unintended consequences:

> And I hope it's just not a negative view to take but I do specifically remember that a friend told me that it's the greatest thing ever that he could find his friends walking down the street and I thought "don't you think that's crazy? I wouldn't want someone to know that about me." I mean, he hadn't thought about it… and realizing that a lot of people do walk right into that, thinking, "oh, it's not so bad…"

Several participants raised the fear of stalking, particularly by those who might be acquaintances. Perhaps relationships would change over time, or there would be subtleties in the information one would share willingly. In his categorization of moral wrong-doings related to panoptic technologies, van den Hoven (1997) describes these as "information based harms" (p. 34). Here, the framework of contextual integrity highlights violations that pose a threat of financial or physical harm to individuals. Thus lacking moral legitimacy, we are justified limiting the freedom of persons who cause, or are likely to cause informational harms to others.

On a related note, all but two interviewees shared concerns about deception in communication. Kainoa emphasized that one's location is personal and he admitted to lying on occasion when people call to ask where he is. Similarly, Kainoa, Iolana, Maka, and Nahele described incidents where they saw an acquaintance while shopping and quickly moved to avoid being seen. Akoni imagined a scenario where a "white lie" about hosting a small party might be revealed and cause irreparable harm to a relationship. Deception, including altruistic lying, is a part of everyday communication (DePaulo and Kashy 1998); and as Dourish and Bell (2011) point out, this will become increasingly difficult in a ubiquitous communication environment. This shift could endanger many social relationships, and participants did not identify any benefit to themselves or society. One need not have malicious intent or be involved in illegal practices to desire some secrecy about everyday behaviors. Here, privacy is a necessary context for a variety of social relationships (Nissenbaum 2010).

Lack of transparency

Transparency was a key issue, both as it relates to what data is being collected and who has access to it. Kaimi demonstrated awareness of third-party data aggregators: "There are companies out there that just data mine. You've never heard of them, you've never met these people, but they know a lot more about you than they should." Kainoa explained that,

> it's not really clear what [supermarkets] say about their corporate affiliates. That can be anybody. I wouldn't want information going to the government. I wouldn't want it going anywhere, to be honest… My biggest discomfort is knowing that my data is stored somewhere and it's not going to go away. I can't get it off. I might not know where it is.

Due to the invisibility and pervasiveness of the IoT, laws restricting the sharing of consumer data may be difficult to enforce. Similarly, Keoni pointed out that while the data collected would not necessarily have negative consequences, the uncertainty about what was actually occurring troubled him: "I don't see that that's necessarily a bad thing, but they are gathering it and I just don't know who has it… it's like you just don't know to what use this information is to be put." In Turow's (2006) analysis of customer relationship media, he observed that marketers and advertisers are trying to find ways to "insert themselves unfiltered into their desired customers' domestic lives in ways that encourage consumers to accept surveillance and relationships tailored to their personal characteristics" (p. 295). Direct marketing, product placement, customized media, and loyalty programs are all converging to enhance marketers' and advertisers' surveillance power. At the same time, these "seemingly benign relationships in the new digital environment can quickly lead to feelings of discrimination, anger, and suspicion of institutions" (p. 303). Haggerty and Ericson (2006) note that surveillance enables monitoring pre-constituted social groupings, with the logic of a particular system subjecting individuals to varying levels of scrutiny. Lyon (2002) describes this surveillance behavior as "social sorting":

> Codes, usually processed by computers, sort out transactions, interaction, visits, calls and other activities; they are invisible doors that permit access to or exclude from participation in a multitude of events, experiences, and processes. The resulting classifications 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 (Lyon 2002, p. 13).

Information systems have biases, intentional or otherwise, and these shape and constrain individuals' lives. Friedman and Nissenbaum (1996) note that these may be intentional or unintentional. Preexisting biases may be rooted in social institutions and practices. Technical biases can also arise due to system constraints. Emergent biases arise in the context of use, particularly as new groups (with different values or knowledge) encounter the system. In all cases, biased systems "systematically and unfairly discriminate against certain individuals or groups of individuals in favor of others" (p. 332). Although there are ways to minimize these risks during the design process, it is often financially advantageous for those in control of information systems to foster these inequalities, both as a form of social control and to maximize profit. For example, Winseck's (2003) "netscapes of power" constitute a deliberate reshaping of information infrastructures to reinforce systematic biases. van den Hoven (1997) describes this type of moral wrong-doing as "information inequality". Social sorting privileges some members of

society and disadvantages others. Using the decision heuristic of contextual integrity, this aggregation and mining of personal data stands out as violating norms related to the collection of shopping and location data in the supermarket. These novel practices do little enhance the goals of citizens during a shopping experience. Further, because these practices can lead to political and economic discrimination and can provide an unfair advantage to corporations who could use this data for financial gain, to subtly influence citizens' behaviors, or to deny them access to particular resources or activities, they lack moral legitimacy, and should be challenged.

Health-related and biometric information

Concern about health-related and biometric information was among the most sensitive issues described. There was recognition that a great deal of personal information, related to both one's health and identity (including sexual, religious, or cultural practices) might be inferred from one's aggregate data. Although going to the supermarket is an "ordinary" and public occurrence, according to Anuhea, electronic monitoring, storing, and analysis of data gathered during routine excursions can be highly personal. She noted,

> I can't see myself buying anything unusual, but if I do, I don't want to have that be a judgment later on. I see a trend for women, maybe you're buying certain feminine products and then you stop buying them, so maybe they know you're hitting a certain age. I mean, that's personal information that maybe you don't want to share.

While store employees or other patrons might witness a consumer making a sensitive purchase, the aggregation and mining of the data allows for historical patterns to be identified and stored. Kaimi reflected on sophisticated data mining techniques, having recently read a news story (Hill 2012) that describes a large retail company's current practice of data mining to identify potential customers in the early stages of pregnancy:

> I am not sure what they do with the information but I know that they use it… for example, I know that Target tries to target pregnant women and they can do that by looking at the things they are buying, I think it was like unscented lotion and other indicators. And when you're pregnant you're changing up all your routines so that's a time when you might develop new habits, so that's why they try to target certain people. So they definitely make use of information based on what you buy. That's probably why they have the rewards system.

Duhigg (2012) elaborates these marketing analytics techniques, noting that shoppers at stores like Target are assigned a unique identification number and any use of credit cards, coupons, surveys, phone or email contacts with the store, as well as website visits are all recorded and combined into personal profiles. In addition, stores can purchase additional demographic information about customers from data aggregators, including information such as:

> your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit… your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own (para. 7)

Interviewees also expressed concern about this purchase information being transmitted to other parties. While, in the United States, the *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) prevents specific actors, such as personal physicians, from sharing health information about an individual, other actors not explicitly covered (e.g., supermarkets or third-party data aggregators) could amass and analyze data:

> If I've got a health issue and I'm buying donuts, you know… my rates may go up, they may drop me. I don't drink but I may buy a bottle of wine or buy cigarettes… I do that all the time for a friend. If that started getting linked to my health organizations, to my insurance… well, my rates are going to go up (Kepano).

This introduces yet another category of moral wrong-doing related to personal data, informational injustice (van den Hoven 1997; Nissenbaum 2010). Here, data that has already been identified as a protected class under the law due to the potential for economic discrimination (e.g., employment, insurance availability) might be more easily access or inferred with the IoT, so certain data must be protected against free travel across different spheres. In addition to sensitive personal information being inferred or shared, this raises the concern that erroneous personal data could be linked to an individual. For example, Keoni noted that he often buys things for his grandmother, who has a number of health conditions. Haggerty and Ericson (2006) highlight the likelihood of error in personal profiles of

aggregated databases, something that is likely to increase as more and more data is collected and analyzed. Solove (2011) also points out that data mining is prone to inaccuracies, and that it might also enable targeting based on First Amendment-protected activities. These may also lead to informational inequalities (van den Hoven 1997; Nissenbaum 2010), as information about race, ethnicity, religion, or political views can be inferred and used to discriminate.

Further, because ubiquitous gathering and sharing of data via omnipresent, near-invisible devices would make transparency difficult, if not impossible, to achieve, one would not be aware of what information is being stored about them, be able to correct factual errors, or delete information deemed invasive. Recent news stories have demonstrated the commercial value of such information. For example, the Nielsen Corporation, a global advertising and marketing company, was caught harvesting private medical postings from behind a password-protected forum dedicated to discussion of patients' medical conditions (Angwin and Stecklow 2010). There is also evidence that data aggregators have developed technology that "matches people's real names to the pseudonyms they use on blogs, Twitter and other social networks" (para. 20). Furthermore, even data that has been stripped of identifying information in order to meet legal requirements can be "re-personalized" using data analytics to exploit the massive amounts of aggregated data (Schwartz and Solove 2011). This surveillance represents a major shift in power, in which corporations are increasingly provided with a view-all of consumer behavior and an ability to sort individuals and engage in targeted marketing without a corresponding increase in benefits to citizens. This has the potential to lead to discriminatory behavior on the part of corporations, who might offer different products, or prices, to individuals based on advertiser-generated profiles (Turow 2006).

The entry of new actors, supermarkets and their nebulous affiliates, was of concern to several participants. Kaimi noted that, "I kinda don't like them having your medical information. I mean, it's put to good use here [in the scenario], but I still feel like that's inappropriate. Because they're not my doctor, physician, health provider."

In addition to the potential for networked sensors to be placed in or on the body in order to monitor specific medical conditions such as diabetes, participants expressed concern about monitoring shoppers' facial expressions or eye movement. Anxiety about the analysis of facial expressions and affect identification was raised in seven interviews. Maka described his concern that cameras linked to facial recognition systems capable of analyzing both identity and microexpressions could be repositioned to examine his behavior based on what products he looked at or touched:

> Reading your microexpressions, your expressions, and understanding how you really feel about this product even thought you might not know it yourself… that's a little spooky, plus they know your feelings, your personal feelings rather than just what you're purchasing… that's creepy. And just the pervasiveness of all of it… It's like mining your thoughts more than just your buying habits.

In the supermarket context, there have already been technical developments and marketing experiments seeking to accomplish this very thing. Emotion-recognition software has been developed and tested to examine consumers' reactions to advertisements and products on billions of devices (e.g., nViso 2011). The Microsoft Kinect, a motion-sensing device made for use with the Xbox 360 game system that was released in 2010, employs face-recognition and expression-reading technologies and heart-rate monitors. Microsoft has released statements to quell public concern about the use of this data (Microsoft 2013). In 2003, a Wal-Mart store in Oklahoma used RFID in cosmetic packages to trigger video cameras in-store to observe and record consumers, an act met with outrage by privacy advocates (Hildner 2006). Iolana also noted that even if she were somehow able to avoid sharing or use false information about her identity to make purchases, facial recognition technologies could still link all of her behaviors to an actual identity profile. Of particular note is the emergence of cloud-based facial recognition (Keller 2011) enabling Internet-enabled mobile devices to near-instantaneously match subject images to online identity profiles. Acquisti et al. (2011) describe experiments where they were able to match unidentified, pseudonymous profile photos of subjects from an online dating site with their Facebook photos, as well as matching students walking around college campuses with their online records using online an Internet-enabled mobile device. The sophistication and reach of these technologies will certainly continue to grow as we move towards next-generation standards for the World Wide Web. Importantly, there may be no way to truly opt-out of sharing this information, as it is linked to numerous public records and online profiles. Further, whether one actively uses the Internet or not, this information is being collected and stored about them online. Facial recognition technologies are currently under study by the Federal Trade Commission due to consumer privacy concern (Federal Trade Commission 2011), but these technologies are rapidly entering the marketplace with little oversight. This aggregation and mining of personal health data links the consumer shopping

experience to the previously-distinct realm of medical information and violates norms related to the collection and transmission of medical data. While context-specific laws such as HIPAA protect existing medical information practices, the IoT will link this to the larger, and less restrictive, domain of search and purchasing behaviors linked to the World Wide Web.

Autonomy and identity

Surveillance networks challenge citizens' autonomy and identity in a number of ways. Although all of the participants described certain aspects of IoT developments as welcome conveniences, they also expressed concern that they could lead to invasive targeted marketing. A primary concern was that advertisers with access to stores of personal data, browsing and purchasing trends, and one's location might seek to influence consumer behaviors in an unwelcome manner. Keoni said that, "it seems somewhat intrusive… driven by companies looking for information about you, and once you've even thought about their product, that there's a push for you to purchase it." This was echoed by Maile, who observed that,

> I think underneath it all that the concern would be that there is too much information about your identity going out and how is it really linking you to other people and other places because I don't necessarily want people to know my habits… and I can live without the store telling me that I need to come back.

Furthermore, consumers' constant awareness of, and interaction with, these profiles could limit individual choices. Haggerty and Ericson (2006) note that surveillance can foster the establishment of new forms of identity, with new identity categories being created by advertisers. One's position in this "new constellation of market segments" determines the commercial offers and communication one receives (p. 16). Increasingly, consumers could be influenced by these messages in ways that limit their own abilities to shape their identities or to resist those assigned them. A related area that is currently underexamined in policy lenses is the growth of machine-to machine communications. The IoT relies explicitly on billions of interlinked computing devices, and the World Wide Web is evolving into a sociotechnical system designed for automated data gathering and intelligence. As intelligent systems increasingly take actions on behalf of citizens or corporations, these types of interactions may influence citizens' moral rights and obligations (Stahl 2004). The IoT relies on sophisticated technical standards that involve computers making sense of data, as well as entering relationships with humans as advisors or assistants. This vision of data that can be readily interpreted by machines may alter the nature of machine-to-machine and machine-to-human communication. Essentially, there is a possibility that computers might move from mere data processing to understanding the meaning of the information in rich social settings.

For Kainoa, Nahele, Maka, and Kaimi, another aspect dealt with dependence on the technology and information networks. Kainoa was somewhat reluctant, noting, "It's like people are rats on wheels being directed what to do by their phone." Maka added that, "I think for myself I'd like it to know as little as possible about me. I can make my own decisions." Nahele was concerned that it would make humans lazy and also lead to an undesirable dependence on corporations.

> We seem to be getting more dependent on companies than we are on ourselves. For example, my mom when she was a kid almost never went to a grocery store because my grandfather had a garden. It's making you dependent on that machine rather than using your own judgment. That is my biggest problem … it seems to presume to know you better than you know yourself. This makes you a *drone*.

Daly (2010) argues that modern ICTs have created a global surveillance network, or "travel panopticon" that corrodes personal autonomy. IoT-enabled supermarket surveillance will evolve from technologies intended to aid the tracking of products for supply-chain management, and the informational practices are on track to create a marketing surveillance system that will challenge personal freedom and autonomy. The design heuristic of contextual integrity reveals these practices restrict one's ability to shape one's personal information identity. As Floridi (2005) observes, "We never stop becoming ourselves, so protecting a person's informational privacy also means allowing that person the freedom to change, ontologically" (p. 197). This relates to a fourth category of informational wrong-doings, moral autonomy (van den Hoven 1997). Using the framework of contextual integrity, we see that the IoT may present grave challenges to moral autonomy that should be addressed by data protections.

Public spaces and the public good

Although the supermarket is considered a public space, it is also a bridge to one's home life, which is presumably not intended to be open to the public gaze. Because the IoT is expected to link a variety of household objects, including refrigerators and other appliances, to global networks, the home itself may become a site of surveillance linked to the supermarket. This melding of spheres due to ICT will further enhance the likelihood of information related to sensitive issues such as medicine, religion, political views,

and so forth being captured and exchanged. Through the IoT, the supermarket is transformed from a mundane place, where one has an expectation of privacy, to a site of surveillance. Here, the shifts revealed by employing the framework of contextual integrity highlight the blurring boundary between public and private space. Anuhea elaborated this idea with an example from the recent Asia–Pacific Economic Cooperation (APEC) conference in Honolulu. She described reading a news release about a company interested in embedding the pavement in Waikiki with sensors, in order to detect the presence of individuals and move surveillance cameras accordingly.

> It's putting a new spin on public life. And public space… You think you're just going around doing your average chores in daily life… Because if I go to a public space there's an awareness that [I'm] going to be filmed perhaps, but if I am just going to the grocery store doing my daily chores I have an expectation that it's more private. So I guess if you're looking at saying it's for the public good for events like that, it's interesting… I don't know if it makes me feel comfortable but it probably does make the job easier for emergency management teams or the police… but just for going to the grocery store, I am not too comfortable with every move being followed. I just think that because it's a routine activity that it's different and that because it's items that I am purchasing it's different, because these are items I am using and maybe I don't want people to know what I am using. I'm not saying that Waikiki [site of APEC] is different, but if there's a large event or a lot of potential crimes that can occur there, maybe it's a public safety issue, whereas I don't really think that the grocery store is a public safety issue. I think [security surveillance at APEC] was about the public benefit or public good… whereas the grocery [surveillance] is for corporate good.

Anuhea's claim that neither she nor society at large is benefitting from access to this information again highlights an imbalance in power that emerges from this particular act of surveillance. The question becomes: How much information is actually needed to optimize the shopping experience or to protect the public, and what is actually being collected (for monetary value) that is not of use to the consumer or public safety? Here, the flagged practice lacks moral legitimacy due to an undemocratic shift in power, erosion of personal autonomy, and threat of unjust discrimination, and this argues for it to be rejected. Likewise, Kaimi and Nahele expressed skepticism that certain aspects were for their benefit or a larger public good, despite corporate marketing indicating otherwise. Through programs like rewards cards, emphasis is placed on potential financial or convenience benefits, with little discussion of the benefits to corporations themselves. Similarly, in the United States, the major policy discourse frames privacy as something one must be willing to give up in order gain security (Solove 2011). However, as Solove notes, it is possible to have both privacy and security, and we must carefully evaluate security measures to ensure not only that they do not unnecessarily hinder privacy but that they also are effective. Where existing norms are transgressed, new practices must be demonstrated to be superior, and the onus of proof is on the advocates of the novel practice. Arguments in favor of surveillance based on the rationale of public safety need to demonstrate that democratic principles such as the freedom to express political views, vote in confidence, and engage in information seeking necessary to engage in informed decision making will not be diminished through these new practices.

Conclusions

This study examined concerns about privacy and the emerging IoT by using Nissenbaum's framework of contextual integrity to explore citizens' perceptions about changes in the key actors involved, information attributes, and principles of transmission. This analysis revealed a number of points where existing norms about the collection and use of personal information will potentially be violated in everyday consumer transactions employing the IoT. Among these were the introduction of many new actors, including nebulous corporate affiliates who might have access to one's personal information related to activities in the supermarket or home (as the IoT will link the two). Other concerns dealt with new types of data collected, including biometric data, affect monitoring and cloud-based facial recognition. The transmission and storage of these data also raised concerns, as automated data gathering and intelligence leading to increased aggregation and transfer of personal information was not seen as relevant or necessary in the context of the supermarket. These changes have the potential to produce a variety of informational harms, inequalities, and injustices, and they threaten moral autonomy. Examples discussed above included the erosion of social relationships, political and economic discrimination, harming citizens' personal autonomy, or limiting freedom of access to information or discussion of issues relevant to democratic decision-making. Thus, these new practices lack moral legitimacy.

None of the participants in this study objected to the entire vision; in fact, all also mentioned specific contexts or applications that were desirable. Nalani describes this "tradeoff":

> I mean it all seems awkward because it is letting go of so much but it also makes it so much easier. I feel it would just be taking getting used to and as long as I felt I still had control that I would come to accept it… Like you would get more control of your life by knowing all these things, but you'd kind of have to give up control, private information. You've got to give a little control to get a little control, I guess.

Others also described these changes in terms of a tradeoff that did not meet expectations. Kaimi argued that collecting even more fine-grained data about one's shopping habits goes too far; "it is not respectful of your privacy. It just strikes me as a little [pause] *beyond*, a little much." Many of the concerns identified above—mining of medical data, invasive target advertising, loss of autonomy through marketing profiles or affect monitoring—appeared to tip the balance between consumer benefit and corporate gain: "Certain things are just not a good tradeoff—what small benefit can come of them could never outweigh the risk" (Anuhea). The risk noted by Anuhea relates to increasing ability to aggregate and mine data from a number of novel sources. This led to concerns that information related to both one's health and identity could be gathered and used to discriminate economically and politically. This new surveillance power creates an imbalance between the consumer and the corporation that may also impact individual autonomy. In particular, automated systems pushing recommendations or personal affect monitoring were seen as invasive.

Several implications for policy and system design arise from these findings. First, there are clearly some aspects of the IoT in an everyday shopping context that will be problematic for some consumers. Thus, some resistance is to be expected. Bennett (2008) notes, for example, the privacy advocacy organization CASPIAN, which focuses explicitly on supermarket consumers and stresses protests and boycotts in the United States. He also explores the possibility of this type of privacy advocacy becoming a global social movement. Recalling Weber and Weber's (2010) questions about laws in the context of the IoT, the time to create legal protections is before major problems arise. Moor (2008) makes a powerful argument for the need to be more proactive, engaging ethical issues related to emerging technologies as early as they are detectable, using multidisciplinary teams to address issues, and developing more sophisticated ethical analyses. Similarly, Winter (2008) argues the need for participatory foresight activities to involve a wide variety of stakeholders in "broad public discussion, education, and insight into these emerging issues, ensuring that technological developments more closely reflect broad community values and goals" (p. 202). Neumann and Weinstein (2006) also emphasize the importance of fostering a society-wide discussion about the contexts and conditions within which RFID systems are acceptable.

> This is an especially difficult task, because many of the would-be applications are emotionally charged, and RFID capabilities and ostensible benefits are in some cases being hyped far beyond what is realistic. Yet it is such critical deliberations that will likely influence whether RFID will be deployed primarily in useful tools, or rather as identity shackles (p. 136).

This is particularly important to consider in light of Maile's argument that the norm for privacy is still there but that citizens are not fully aware of the many changes that are happening, and don't think through the implications of their engagement with technology. Considering the possibility of resistance, an informed citizenry is critical not only from an ethical, human rights perspective, but for all parties. Acquisti (2010) observes that many companies have been punished for data collection that was perceived as invasive of consumer privacy, and that customers may be less likely to engage in business transaction due to concern about future privacy costs. He argues for finding a balance that is in the best interest of citizens and society at large. This will also involve extending the burden of proof to companies holding consumer data, requiring demonstration of "why they cannot efficiently keep providing the same products and services in manners that are more protective of individual privacy" (p. 20). In addition to identifying new practices that may violate contextual integrity, the heuristic tools of the framework lead us to consider related moral and political factors. In the case of data aggregation and mining,

> the moral legitimacy of such practices… rests not upon finding that nothing important has changed but that novel patterns of information flow initiated by those who amass personal information, those who give or sell information, or those who buy or otherwise gain access to it, are promoting social goals, ends, and values more effectively than traditional patterns of flows regulated by entrenched norms (Nissenbaum 2010, p. 204).

As noted earlier, there may be some violations of contextual integrity that will, after ethical analysis, be revealed to be superior practices. However, in the case of the consumer shopping experience, the onus is currently on the stores themselves to provide substantial evidence showing that technologies such as eye tracking or emotion recognition are beneficial to consumers.

This study has identified several novel practices related to use of the IoT in supermarkets that lack moral legitimacy and require data protection. However, the policy and design response will require multiple domains—sociological,

technical, and regulatory—to be addressed in tandem when seeking privacy solutions (International Telecommunication Union 2005). Public education and discourse about what is desired and acceptable is a key part of the sociological solution. From the technological side, the development of privacy enhancing technologies (PETS) and designing new systems with public input is emphasized. One promising approach is Involving users in design through elicitation of situated values (e.g., Friedman 2008; Denning et al. 2010). This Value Sensitive Design (VSD) approach has been furthered by Pommeranz et al. (2011), who found that many existing engineering methods fail to elicit situated values and create authentic dialog between stakeholders and designers. To address this need, they have designed a mobile tool to actively elicit situated values (those relevant to a specific real life context, e.g., privacy, autonomy, and trust) from stakeholders and enhance communication with designers. This is a promising and necessary approach.

The regulatory domain is likewise complex. Will omnibus privacy protection laws like those employed by the European Union be sufficient in this emerging environment, or would domain-specific laws prove more effective? It is clear that the present standard of industry self-regulation in the United States is not sufficient to constrain the threat to privacy. As Hildner (2006) observes, "Experience demonstrates that legally unenforceable self-regulation will not be a sufficient limitation on RFID's threat to privacy" (p. 159). Without significant and enforceable legal recourse, it is unlikely that retailers will handle citizens' data in a conscientious manner. However, an omnibus privacy law may be unenforceable or lack the ability to target specific technologies or practices. Since a great deal of participant concern appears to be related to data storage, sharing, and analytics, one possibility is a general law for consumer data sharing coupled with sector-specific laws related to RFID (or other relevant technologies, as they arise).

Acknowledgments The author wishes to thank the reviewers of this article. The author also wishes to thank the participants who took part in this study and the National Science Foundation Team for Research in Ubiquitous Secure Technology (TRUST) Women's Institute for Summer Enrichment. Preliminary findings of this study were published by the author in the Proceedings of the Pacific Telecommunications Council Annual Conference. Honolulu, Hawai'i. January, 2012. "Privacy and the emerging Internet of Things: Using the framework of contextual integrity to inform policy."

References

Acquisti, A. (2010 December 1). The economics of personal data and the economics of privacy. Joint Working Party for Information Security and Privacy (WPISP) and Working Party on the Information Economy (WPIE) Roundtable, background paper 3. Paris: Organisation for Economic Co-operation and Development (OECD).

Acquisti, A., Gross, R., & Stutzman, F. (2011). Faces of Facebook: Privacy in the age of augmented reality. *Black Hat 2011*. Retrieved on December 11, 2011 from http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

Albanesius, C. (2011 May 10). Senator has 'serious doubts' about privacy of Google, Apple location apps. *PC Magazine*. Retrieved on June 8, 2011 from http://www.pcmag.com/article2/0,2817,2385150,00.asp.

Angwin, J., & Stecklow, S. (2010 October 12). 'Scrapers' did deep for data on Web. *The Wall Street Journal*. Retrieved on October 20, 2010 from http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html.

Ashton, K. (22 June 2009). That 'Internet of Things' thing. *RFID Journal*. Accessed from http://www.rfidjournal.com/article/view/4986 on May 11, 2010.

Barnett, E. (11 Jan 2010). Facebook's Mark Zuckerberg says privacy is no longer a 'social norm'. *The Telegraph*. Retrieved on March 10, 2010 from http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html.

Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage.

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: The MIT Press.

"China working on unified national Internet of Things strategic plan." (2010 July 5). TMCnews. Retrieved on August 10, 2010 from http://www.tmcnet.com/usubmit/2010/07/05/4884535.htm.

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

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498–512.

Daly, E. (2010). Personal autonomy in the travel panopticon. *Ethics and Information Technology, 12*, 97–108.

Denning, T., Borning, A. Friedman, B. Gill, B. Kohno, T., & Maisel, W. (2010). Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of CHI 2010 conference on human factors in computing systems* (pp. 917–926). New York: Association for Computing Machinery.

DePaulo, B. M., & Kashy, D. A. (1998). Everyday lies in close and casual relationships. *Journal of Personality and Social Psychology, 74*(1), 63–79.

Dourish, P., & Bell, G. (2011). *Divining a digital future: Mess and mythology in ubiquitous computing*. Cambridge, MA: The MIT Press.

Duhigg, C. (2012 February 16). How companies learn your secrets. *The New York Times Magazine*. Retrieved February 17, 2012 from: http://www.nytimes.com/2012/02/19/magazine/shopping habits.html?_r=2&pagewanted=1&hp.

Dworkin, R. (1986). *Law's empire*. Cambridge, MA: Harvard University Press.

European Commission & Information Society and Media. (2008). *Internet of Things in 2020: Roadmap for the future. European technology platform on smart systems integration.* Version 1.1 (27 May, 2008).

European Parliament. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0207+0+DOC+XML+V0.

Federal Trade Commission. (2010 December 1). FTC staff issues privacy report, offers framework for consumers, businesses, and policymakers. Retrieved on November 24, 2011 from http://www.ftc.gov/opa/2010/12/privacyreport.shtm.

Federal Trade Commission. (2011 November 21). FTC announces agenda, panelists for facial recognition workshop. Retrieved on November 24, 2011 from http://www.ftc.gov/opa/2011/11/facefacts.shtm.

Federal Trade Commission. (2012 March 26). *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers*. Washington, DC: Federal Trade Commission. Retrieved on March 27, 2012, from http://ftc.gov/os/2012/03/120326privacyreport.pdf.

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

Friedman, B. (2008). Value Sensitive Design. In D. Schular (Ed.), *Liberating voices: A pattern language for communication revolution* (pp. 366–368). Cambridge, MA: The MIT Press.

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems, 14*(3), 330–347.

Glenn, J. (2009). Scenarios. In J. C. Glenn & T. J. Gordon (Eds.), *Futures research methodology—Version 3.0*. AC/UNU Millennium Project. Washington: American Council for the UN University.

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

Hildner, L. (2006). Defusing the threat of RFID: Protecting consumer privacy through technology-specific legislation at the state level. *Harvard Civil Rights-Civil Liberties Law Review, 41*, 133–176.

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

International Telecommunication Union. (2005). Privacy and Ubiquitous Network Societies: Background paper. In *ITU Workshop on Ubiquitous Network Societies*, April 6–8, 2005. Geneva: International Telecommunication Union.

Internet of Things Conference Organizing Committee. (2010). Internet of Things. Retrieved on March 17, 2010, from http://www.iot2010.org/outline/.

Keller, J. (2011 September 29). Cloud-powered facial recognition is terrifying. *The Atlantic Monthly*. Retrieved on October 1, 2011, from http://www.theatlantic.com/technology/archive/2011/09/cloud-powered-facial-recognition-is-terrifying/245867/.

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

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.

Marx, G. T. (2006). Varieties of personal information as influences on attitudes towards surveillance. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 79–110). Toronto: University of Toronto Press.

Microsoft. (2013, June 6). Privacy by design: How Xbox One and the new Kinect sensor put you in control. Retrieved on June 6, 2013 from: http://news.xbox.com/2013/06/privacy.

Moor, J. H. (2008). Why we need better ethics for emerging technologies. In J. van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 26–39)., Cambridge studies in philosophy and public policy Cambridge: Cambridge University Press.

Neumann, P. G., & Weinstein, L. (2006). Risks of RFID. *Communications of the ACM, 49*(5), 136.

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

nViso. (2011). Technology. Retrieved on October 11, 2011 from http://www.nviso.ch/.

O'Connor, M. C. (2011 April 6). European Commission issues framework for measuring and mitigating RFID's privacy impact. *RFID Journal*. Retrieved on April 6, 2011 from http://www.rfidjournal.com/article/view/8345.

Pommeranz, A., Detweiler, C., Wiggers, P., & Jonker, C. (2011). Elicitation of situated values: Need for tools to help stakeholders and designers to reflect and communicate. *Ethics and Information Technology,*. doi:10.1007/s10676-011-9282-6.

Schwartz, P. (1996). *The art of the long view: Planning for the future in an uncertain world*. New York: Currency Doubleday.

Schwartz, P. M., & Solove, D. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review, 86*, 1814–1894.

Solove, D. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven, CT: Yale University Press.

Stahl, B. C. (2004). Information, ethics, and computers: The problem of autonomous moral agents. *Minds and Machines, 14*(1), 67–83.

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

van den Hoven, M. J. (1997). Privacy and the varieties of moral wrong-doing in an information age. *Computers and Society, 27*(3), 33–37.

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

Winseck, D. (2003). Netscapes of power: Convergence, network design, walled gardens, and other strategies of control in the information age. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 176–198). New York: Routledge.

Winter, J. S. (2008). Emerging policy problems related to ubiquitous computing: Negotiating stakeholders' visions of the future. *Knowledge, Technology & Policy, 21*, 191–203.