J Bus Ethics (2015) 131:19–30
DOI 10.1007/s10551-014-2248-y

Information Relevance Model of Customized Privacy for IoT

Wei Zhou · Selwyn Piramuthu

Received: 27 July 2013 / Accepted: 7 June 2014 / Published online: 5 July 2014

Abstract Motivated by advances in mass customization in business practice, explosion in the number of internet of things devices, and the lack of published research on privacy differentiation and customization, we propose a contextual information relevance model of privacy. We acknowledge the existence of individual differences with respect to unique security and privacy protection needs. We observe and argue that it is unfair and socially inefficient to treat privacy in a uniform (or less differentiated) manner whereby a large proportion of the population remain unsatisfied by a common policy. Our research results provide quantifiable means to measure and evaluate the customized privacy. We show that with privacy differentiation, the social planner will observe increases in demand and overall social welfare. Our results also show that business practitioners could profit from privacy customization.

Keywords Value based privacy management · Customized privacy · Privacy differentiation · Internet of things · Privacy perception

W. Zhou
Information & Operations Management, ESCP Europe, Paris, France
e-mail: wzhou@escpeurope.eu

W. Zhou · S. Piramuthu
RFID European Lab, Paris, France

S. Piramuthu (✉)
Information Systems and Operations Management, University of Florida, Gainesville, Florida 32611-7169, USA
e-mail: selwyn@ufl.edu

Introduction

> It is apparent that the word "privacy" has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts. . . . Like the emotive word "freedom," "privacy" means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.[1]

Privacy issues play a very important role in traditional business ethics literature. Privacy is often considered as a double-edged sword. On one hand, people use privacy controls to protect their private information. On the other hand, privacy issues have become a huge barrier to new innovations, especially in the IT sector. In a majority of situations, the same level of privacy is uniformly enforced regardless of the needs and/or requirements of each individual (e.g., Kupfer 1987; Parent 1983; Parker 1974; Posner 1978). Even for an individual person, the privacy setting requirements could be disparate for different attributes. For example, with the widespread explosion of Internet of Things (IoT) applications and associated devices (e.g., RFID), it becomes readily apparent that the privacy settings for each such device owned by an individual could be different. Moreover, this difference is exacerbated even more since the privacy setting for a given device owned by an individual can vary drastically based on its different uses, use settings, and related context.

We argue that privacy is context-dependent and consumer-heterogeneous. Privacy exists in every corner of our social activities, but not all privacy-related situations pose the same level of threat (if any). In general, privacy

[1] J. Thomas McCarthy, The Rights of Publicity and Privacy, 5.59 (2nd ed. 2005).

protection mechanisms have been enforced in an "on/off" mode. For example, it has been hotly debated that RFID technology[2] poses privacy/security threats in health care systems despite its huge technological advantages and the existence of means to alleviate security/privacy concerns.

Constrained by financial resources and consumer preference, it becomes preferable for organizations to optimize social cost by addressing privacy issues through measurement and careful evaluation of each privacy concern. For example, in an online discussion forum, some forum users prefer to publicly display their actual names and photos while some others would rather use fake names and photos. In such an environment, it would be unwise to force everyone to use actual name and actual photo and vice versa (i.e., to force everyone to use fake names and photos). Privacy issue can be and probably should be differentiated and customized in similar situations. This is our motivation for this research study. We consider customized privacy/security using an appropriate model and develop relevant managerial insights.

We foresee a refined privacy protection regulation mechanism that would maximize the overall social privacy requests at the lowest social cost. Compared to the traditional flat security and privacy protection policy, a customized policy would treat customers based on their unique needs and preferences. In a retailing environment, for example, this signifies that customers who are not paranoid to share their personal identity and information with retailers could benefit from more personalized service and products. In near field communication systems, it signifies that consumers who can bear the small privacy risk associated with RFID use could leverage this technology for a wider spectrum of conveniences.

Security and privacy protection bears costs from multiple sources and facets. Privacy protection can prove to be expensive for an e-commerce provider when moving customer information to a dedicated and encrypted server compared to storing information on the cloud. There is a fixed cost and an operational cost in this case. Another cost of privacy protection is observed when it starts to hinder the diffusion of certain information technology. RFID, for example, is a technology that allows business practitioners to track/trace and to identify item-level components in real-time without direct line-of-sight (vs. bar code). This technology allows for effective management of related systems and saves cost for the firm while simultaneously providing much convenience to the customers. The widespread use and diffusion of this technology has been to some extent hindered by security and privacy concerns because of the potential for the leakage of their private information through the use of RFID (Zhou and Piramuthu 2012).

It is worth noting that there is inherently neither a 100 % safe nor a 100 % unsafe technology with respect to privacy and security. This can be observed with bar code and RFID as examples of technologies that are traditionally perceived as safe and risky, respectively. It is, therefore, preferable for industry and government policy makers to quantify context-specific privacy from a probabilistic perspective for applications in different domains to enable treatment of privacy in a scientific manner.

Inspired by recent advances in mass customization and (big) data business analytics, we propose a novel privacy differentiation/customization model. With this model, we argue that consumers with low demand for privacy protection should not be forced to bear the cost of the fraction of the population with demand for high privacy protection. On the other hand, the high demand consumers should be allowed the flexibility to enjoy their desired high level privacy protection, at a cost.

Our motivation for this research is to enrich existing privacy literature by introducing the contextual privacy perception framework and the information relevance model by identifying the different needs of privacy concerns from different consumers. The potential for widespread adoption of devices such as RFID, smart cards, and anything related to IoT and resulting privacy/security/contextual differentials across these devices is another motivation for this study. Although privacy/security issues have been studied by researchers in this area, we are not aware of any published research that addresses differentiated/customized privacy/security in the era of the Internet of Things.

Assuming that privacy protection comes with a certain social and monetary cost, we use (but not exclude) a nonlinear pricing scheme to optimize the overall social welfare and illustrate possible benefits. We conclude that differentiating privacy protection service in various business practices increases market share of the principal good, increases consumers' social welfare and improves firms' profit.

The remainder of the paper is organized as follows: We provide background discussion on ambient intelligence, IoT and RFID in "Background on Ambient Intelligence, IoT, RFID" Section. We follow this in "Related Literature" Section with a brief review of relevant literature on privacy/security for IoT, with specific focus on RFID systems. We then present the privacy concept framework followed by the information relevance model in "Information Relevance Model of Privacy" Section. In "Customized Privacy" Section , we discuss the economic and managerial insights of both vertical and horizontal privacy differentiation and customization. In conclusion, we present our main findings and propose future avenues for research in "Concluding Remarks" Section.

[2] Radio Frequency IDentification technology that allows fully automatic and touchless tracking/tracing of merchandise, transportation, and even living beings.

Background on Ambient Intelligence, IoT, RFID

There is an increasing trend toward uniquely identifying items/objects/things so that each of these can be uniquely tracked/traced/attended-to/ as well as communicated with in a customized/personalized manner. This trend has also led to virtual representation of these items/objects/things as a part of the Internet. A 'thing' in the IoT is frequently associated with tagged items that can carry on a two-way conversation and often includes auto-identification technology such as RFID. The emergence of IoT essentially disrupts predictable pathways of information in most organizations such as databases and information from public sources, including the Internet, to reports. Sensors and actuators embedded in physical objects are readily connected to the Internet to communicate information about their immediate surrounding environment, for example, thus facilitating the ability to respond swiftly and appropriately as necessary.

The concept of *Ambient Intelligence* comprises seamless integration of ubiquitous information, communication and entertainment resources that are embedded in networks that connect disparate devices (e.g., IoT). With the explosion in the number of such devices that are integrated into our environment, ambient intelligence allows for the user interface to hide the complexities of underlying components and related technology. Components of Ambient Intelligence environment include RFID tags that have been successfully used in a wide variety of applications with positive outcomes. However, similar to other privacy-invasive technologies such as biometrics, covert filming, key logging, and monitoring of Internet use, RFID technology has the potential to violate an individual's privacy. While the item-level information generated and disseminated by RFID tags are generally beneficial for their intended purpose, there is a trade-off between the benefit of providing accurate item-level information and the drawbacks of risking personal privacy.

RFID tags are generally embedded in objects and facilitate tracking and tracing of the substrate object. Supply chains and retailers are beginning to implement item-level RFID tags. For example, American Express' (Barnes et al. 2005) U.S. Patent application (see for example, Sections 004, 194, 195, 212, 213) on the use of RFID readers as 'consumer trackers' to observe RFID-tagged items and therefore the identification, tracking and tracing of (potential or otherwise) customers with these items on their person. The information thus generated would then be used to target customers with appropriately customized promotions, incentives, and advertisements. Introduced by the International Civil Aviation Organization (ICAO), Supplemental Access Control (SAC) is a new optional and supplemental security mechanism for the next generation of ePassport. This standard will soon be integrated into documents in Europe in response to the EU mandate that all new residents permits and ePassports issued as of December 2014 are SAC-compliant. ICAO has mandated that all member states should issue machine readable ePassports by the deadline of November 2015. Biological entities (e.g., cattle, fish) have also been successfully RFID-tagged over the years. Although controversial, there have been several instances where RFID tags encased in glass have been implanted in humans (usually in their upper arm). For example, Mexico's attorney general and at least 160 people in his office were implanted with RFID tags to restrict access to secure areas of their headquarters (Weissert 2004). These tags were used to deter corruption by officials by tracking and tracing their access to sensitive data. A private video surveillance company in Ohio, CityWatcher.com, was testing RFID technology for controlling access to a room where it holds security video footage for government agencies and the police (Waters 2006). Two of their employees had glass-encased RFID tags implanted in their upper right arms.

Response from the general public to the incorporation of RFID tags (for example, in retail items, passports) has been rather strong. The governmental entities responsible for allowing such implementations have reacted, although sometimes at a rather slow pace, to outcry from the general public. In the UK, the new coalition government between the Conservatives and the Liberal Democrats has agreed to repeal identity cards, scrap the National Identity and Contact Point databases and the next generation biometric passport, delete DNA profiles of the innocent, outlaw fingerprinting of children without parental consent, regulate video surveillance, restrict communications surveillance that includes removal of stored Internet and email records (BBC 2010).

The US National Institute of Standards and Technology (NIST) Guidelines for Securing RFID Systems (Karygiannis et al. 2007, pp. 5.26–5.27) considers risks related to business process, business intelligence, privacy and externality risks and related management, operational and technical controls. Specifically, for privacy risks, they list several components that make up management (RFID usage policy, IT security policies, agreement with external organizations, and minimizing data stored on tags), operational (physical access control, secure disposal of tags, operator and administrator training, information labels/notice, separation of duties, non-revealing identifier formats), and technical (password authentication, HMAC, cover-coding, encryption of data in transit, electromagnetic shielding, adjustment of transmission characteristics, temporary deactivation of tags, tag press-to-activate switch, tag access controls, encryption of data at rest, kill feature) controls.

In addition to their immediate physical surroundings, the extent of influence of new technologies easily spans a much wider range. This is especially salient with ubiquitous technologies that are associated with the IoT where physical location is irrelevant. Moreover, it is not uncommon for such technologies to be introduced in applications without completely understanding their consequences. For example, the RFID tags used in biometric passports are all known, even before they were introduced, to be vulnerable to attacks with a very high potential to violate the privacy and security of the holder. This tension between the increasing power and ubiquitousness of technology and the concomitant need to understand and anticipate its consequences has been on the rise (e.g., EEA 2001, p. 185).

Related Literature

We now consider existing literature as they relate to the privacy of IoT systems, specifically RFID systems, and ICT.

Parks et al. (2010) consider RFID privacy issues from a health care perspective. They consider the relationship between technology and regulations in ensuring patient privacy through Fair Information Practice (FIP) principles. They examine the design of privacy enhancing technologies and conclude that these technologies fail to incorporate FIP principles, thereby rendering it difficult for health care organizations to comply with security standards and regulations.

Martin (2012) attempts to validate a social contract approach to privacy by considering how and whether privacy norms vary within, across, and outside of communities. Findings from this study indicate that although individuals at various reference points have similar expectations of privacy, they vary with respect to privacy norms and the factors they consider to be important in calculating privacy expectations. Moreover, the results also indicate that outsiders are less knowledgeable on the privacy norms that exist within communities and that privacy is contextual.

Gouvea et al. (2012) consider the potential for success of nanotechnology, an emerging technology, and associated related ethical sacrifices. They conclude that the ethical environment does not have an appreciable effect on research in such emerging technological areas; a positive ethical environment is associated with facilitating their invention and commercialization. They also observe that corruption has a negative effect on successful innovations in emerging technology. They note that knowledge and understanding of technical risks and societal implications of emerging technologies are critical and that threats and their solutions must be regulated and controlled with such knowledge and understanding, which when lacking will likely lead to failure. They suggest increased integration between research with simultaneous efforts to minimize associated risks to individuals, society and the environment in order to economically and socially benefit from emerging technologies.

Som et al. (2009) discuss technology development using the precautionary principle by considering new information and communication technologies (ICT) and their applications as sources of impact. They suggest that precautionary measures must be taken in guiding the development and application of ICT to avoid irreversible socio-economic developments. In doing so, they extend precautionary principle (PP), which has traditionally been used in environmental and public health related issues, to include social issues to account for technological developments with strong social implications.

Drake and Schlachter (2008) consider two types of inter-firm relationships in a supply chain—dictatorial and sustainable collaboration—through virtue ethics. Dictatorial collaboration occurs when a dominant supply chain entity assumes channel control and dictates other entities in the supply chain to satisfy its demands. Sustainable collaboration, on the other hand, is the scenario where the entities in a supply chain collaborate and share their resources and work toward improving the performance of the entire supply chain. After discussing several real-world case studies, they come to the conclusion that sustainable collaboration is preferable, both operationally and ethically, in the long run. They do not consider other issues related to revelation of inventory, competitive advantage, among others, which arise as a direct consequence of data/information sharing as well as collaboration among entities in a supply chain.

Martin and Johnson (2008) discuss ethical conformity in the general realm of marketing products to consumers. They ground their perspective in the strategic choice literature that casts departures from conformity as deliberate vehicles of differentiation. They argue that a firm's ethical conformity decisions are a blend of the firm's unique identity as well as institutional forces that exist at any given point in time. They discuss several facets that comprise a firm's identity and the need to maintain consistency among these facets such as marketing actions, organizational mission, and the firm's symbols and values that are conveyed through marketing communications. Ethical conformity, they claim, must be aligned with the firm's identity as well as stakeholder expectations and this process may take a long time to come to fruition with the dedication of necessary resources. They also discuss over- and under-conformity when faced with constraints and conclude that ethical firms stand their ground and unethical firms base their response on market response to their actions.

To our knowledge, very few published research consider privacy issues associated with the wide-spread introduction of RFID tags. For example, Jones et al. (2004) discuss privacy and policy issues associated with the introduction of RFID in the UK. They specifically consider the use of item-level RFID tags in a retail setting where (1) these tags could be read by anyone without the customer's consent, (2) RFID-generated information can be used to profile customers by linking purchase information with their personal information, (3) retailers physically track customers without their consent or knowledge Albrecht (2008), and (4) retailers distribute or sell information on customers to third parties.

Kelly and Erickson (2005) consider commercial applications of RFID tags from a consumer privacy perspective. Specifically, they evaluate the need for regulations to balance commercial economic interests with those of consumer privacy when these consumers are monitored by firms without their explicit or implicit consent. They discuss the ease with which information on individuals and the items they purchase/use can be used by firms (e.g., retailers) or others (e.g., burglars) based on the characteristics of the items (e.g., expensive stereo equipment). While the discussion in regard to implications may be true sometimes, there are several means to alleviate customer concerns. For example, while such scenarios are easy fodder for the yellow press, reading RFID tags (e.g., on expensive stereo equipment that is inside a house from "simply walking or driving by a house") is really not that straight-forward. For starters, the commonly used passive RFID tag located deep inside a house does not possess enough resources to communicate with a reader that is outside on the street. Moreover, the messages used in communication between tag and reader are encrypted and are not easy to decrypt for an adversary without necessary resources and skills (assuming that the authentication protocol used is not secure). Regardless, it is safer to err on the side of caution and take all necessary precautions to reduce the opportunity for adversaries to take advantage of to a minimum.

Peslak (2005) considers the fundamental issue of privacy and its implications from the perspective of RFID. He identifies four major areas that need further examination and careful consideration including the foundations and support for privacy rights, privacy issues associated with the collection, storage, and processing of vast amounts of private data from the Internet and through electronic commerce, RFID-specific ethical conflicts, and the use of Fair Information Practices (FIP) to deal with RFID privacy issues. Hossain (2009) claims that a majority of RFID privacy-related research has been from a retail customer's perspective. He considers citizen privacy when national ID cards are used by considering means to protect their privacy and by evaluating the diffusion factors including privacy of smart-ID (comprising explicit consent, detail privacy policy, legislative protection, data-owners' accessibility, data authenticity, and communication channels) as well as benefits and security of smart-ID.

Wasieleski and Gal-Or (2008) consider issues related to privacy as well as some of the benefits of RFID technology. They use Lessig's cyberspace framework to study some of the undesirable privacy-related side-effects and observe that this framework is insufficient at preventing individual privacy violations associated with RFID use. They then consider this from the perspective of the Fair Information Practices (FIP) principles and note that these deal only with procedural justice issues related to data collection and do not deal with the actual benefits and costs to individuals whose data are used. They suggest careful and fully disclosed collection and use of RFID-generated information to alleviate some of the concerns of the general public on the use of RFID tags. Zhou and Piramuthu (2012) consider RFID from the perspective of supply chain management. Specifically, they extend the general model of ethics with technology selection, social consequences, and practitioners' rationality and discuss vulnerabilities that arise from the introduction of RFID in supply chains. They also propose the use of technology regulation development matrix to facilitate policy makers with their policy design regulation process.

Information Relevance Model of Privacy

Privacy has been debated for centuries in the past. The relatively recent emergence of modern information and communication technologies (ICT), including IoT, has compelled business practitioners and researchers to re-examine associated privacy issues. For example, Lucas and Pouloudi (1999) utilizes stakeholder theory to understand privacy claims and associated risks among different stakeholders in the information age. Laurence and Free (2006) tries to understand consumers' online privacy concerns based on justice theories. Spinello (1998) reviews different personal privacy protection perspectives in the information economy and argues that modern information technology has made privacy more vulnerable to intruders because of the intrinsic value of privacy as collective good and even as property.

While the Internet has quickly become the largest market place in the world, it's been observed that consumers are increasingly concerned about their privacy in online shopping and other electronic commerce environments. Wang et al. (1998) studies consumers' privacy concern in Internet marketing by considering privacy issues related to the use of unauthorized collection,

disclosure, or other use of personal information as a direct result of electronic commerce transactions.

Privacy concerns are also encountered in various online activities such as junk emails, online marketing through cookies and security invasion (trojan, virus, etc). Private information may be collected through correct channels or from improper collections and transfers. However, despite all these concerns, Bowie and Jamal (2006) argues that sufficient evidence does not exist to prompt a search for a solution in the form of formal government mandated regulation for online environment.

We now consider the privacy concept framework based on existing literature in law and social philosophy domain to lay a theoretical foundation for subsequent discussions.

Contextual Privacy

In the history of literature in philosophy, law and business ethics, it has been lamented that there is a great difficulty in defining a satisfying concept of privacy. In the field of law, there still doesn't exist a universal concept of privacy. People even argue that privacy as one of the few values so fundamental to society is still in a state of "chaos" and "undefined" in social theory. In the law literature, Solove (2002) reviewed existing definitions of privacy and categorized them into six concepts: (1) the right to be left alone; (2) limited access to the self; (3) secrecy; (4) control over personal information; (5) personhood; (6) intimacy. In the business ethics literature, Spinello (1998) categorizes the general definition of privacy into three categories: secrecy, anonymity, and solitude, while also listing three broad types of privacy: psychological, communication, and information privacy.

Although any of the concepts of privacy mentioned above is self-sustained in its unique context and holds countless insights, the reasoning basis upon any of the concepts results in either overly broad or overly narrow comprehension of privacy Solove (2002). Because these complications lie in the different concepts of privacy, some privacy theorists (e.g., Judith Thomson, Danile Solove) claim that privacy should not be understood as a distinct concept, but rather as a set of "overlapped" rights. While it's been generally agreed that privacy can not be consolidated into a single concept, other privacy scholars categorize privacy according to its many conceptual facets. A well-recognized means is to define privacy according to three clusters: (1) physical space, (2) choice and (3) flow of personal information. Physical space indicates "the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals." Choice represents "an individual's ability to make certain significant decisions without interference." Flow of personal information means "an individual's control over the processing—i.e., the acquisition, disclosure, and use—of personal information"[3]

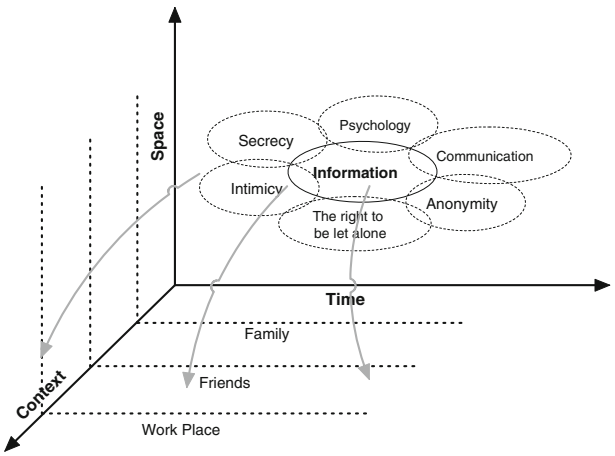

Fig. 1 Contextual Privacy Model

As there is a lack of general consensus on either the concept or an accurate definition of privacy, we proceed by introducing a contextual privacy model to incorporate several related concepts from existing literature in three key dimensions: context, space, and time (Fig. 1). Based on Solove (2002), Spinello (1998) and the privacy context, we contribute to existing literature by categorizing the seven common privacy perceptions in three dimensions: context, space and time. At the center is information privacy that overlaps with secrecy, intimacy, the right to be left alone, anonymity, communication and psychological privacy. Information (such as name, age, sex, address, telephone number, profession, financial information, etc.) comes across with the other perceptions of privacy. Among them, secrecy means to limit the knowledge about an individual. The right to be let alone follows Samuel Warren and Louis Brandeis's classic formulation for the right to privacy. Anonymity signifies the right of an individual to be shielded from undesired attention. Intimacy refers to the control over, or limited access to, one's intimate relationships or aspects of life. Communication privacy refers to an individual's right over the process of communication with others. Psychological privacy Jourard (1966) indicates the right to protect psychological activities and past experiences from unauthorized revelation.

These existing privacy concepts may take different forms and importance at different {context, time, space} manifestations or constellations as in Fig. 1. Context means the setup of a given activity. For example, medical consultancy is a context for patients to see doctors and receive treatments. Given context, an individual's privacy preference would have different dynamics according to space and time. Space includes both physical space and

[3] Kang, supra note 131, 1202–1203

Relevant Privacy Parameters	A	B	C	...
Name	Yes	No	No	...
Address	Yes	Yes	No	...
Bank Info	Yes	Yes	Yes	...
Age	Yes	No	Yes	...
Sex	Yes	No	No	...
Phone Number	No	Yes	Yes	...
Medical History	No	Yes	No	...

Fig. 2 Privacy relevancy scheme

psychological (virtual) space. To our knowledge, this paper is the first to incorporate and expand on the spatial-temporal aspect of privacy. Time indeed plays a very important role in privacy because even for a unique event, the individual's privacy preference could be very different for different attributes/devices based on different contexts at various points in time. For example, someone's privacy concern with respect to the use of an IoT device might disappear when the physical location/context changes from *public* to *private*.

Based on contextual privacy perception framework, we introduce the information relevance model to describe the differences in privacy preferences among different members of the population.

Information Relevance Model

As discussed earlier, time, space and contextual differences form the privacy relevance components that can be extended to differentiate privacy needs at the individual or collective level. Another important perspective of privacy differentiation comes from individual customers themselves. About two decades ago, discussions in media (e.g., television, newspaper) as well as in economics journals alluded to customers' willingness to share private information with manufacturers and retailers, in exchange for the "right" products that fit their needs to be made available to them. It is not uncommon for some people to be open to the idea of sharing personal information in exchange for more personalized products. While others are more aware of their privacy, there is a conflict of interest not only between principals (firms) and agents (customers) but also among customers with different preferences in terms of their privacy level settings. As discussed earlier, these settings are different for different (personal) privacy attributes and different (IoT) devices based on context and across time.

We argue that the concept of privacy is misleading if not considered in context, space and time at both collective and individual levels. Each individual in a group with different privacy preferences could be represented on a information relevancy matrix based on their idiosyncratic privacy needs. Figure 2 illustrates differentiated privacy demand based on a set of private information {Name, Address, Bank Info, Age, Sex, Phone Number, Medical History} among a group of consumers. While privacy is characterized by {Yes, No} values in Fig. 2, it can be readily extended to any integer value from 1 to 10 or any real number in $[0, 1]$. To generalize the privacy relevancy scheme, we define a privacy relevancy matrix as:

$$X_{\forall \text{space,time,context}} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & & \ddots & \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix}$$

where n is the number of consumers with an exhaustive set of m different privacy concerns. Here, x_{ij} $(x_{ij} \in \{0, 1\})$ represents the jth individual's preference on the ith privacy concern. It can also be represented by a value in $x_{ij} \in [0, 100\%]$ as discussed above.

We acknowledge that the consideration of privacy from a utilitarian perspective is not completely new to privacy literature (e.g., Solove 2002; Spinello 1998). Privacy is often considered a "good" and assumes certain values. This viewpoint is also compatible with main-stream utilitarian business ethics literature.

Based on the individual privacy relevancy matrix X, we are now able to more accurately describe the privacy issue at the individual level and to derive characteristic parameters. First, we are able to define a consumer's privacy sensitivity as the summation of her privacy concerns

$$X_{.j} = \sum_{i=1}^{m} x_{ij} \tag{1}$$

The population privacy sensitivity is $Xpopulation = \sum_{j=1}^{n} X_{.j}/n$. Consequently, a consumer's relative privacy sensitivity can be derived from equation (1) by dividing the population privacy sensitivity as $\overline{X_{.j}} = X_{.j}/Xpopulation$.

Group collective characteristics of privacy issues can be determined by defining the privacy score of the ith parameter as

$$X_{i.} = \frac{\sum_{j=1}^{n} x_{ij}}{n} \tag{2}$$

From equations (1) and (2), a business practitioner can obtain exact indicators of a context-specific privacy issue, from both the overall consumer population and privacy concept perspectives. For instance, in the example

Table 1 Collective privacy indicators

	A	B	C	Privacy score
Name	Yes	No	No	0.33
Address	Yes	Yes	No	0.66
Bank info	Yes	Yes	Yes	1
Age	Yes	No	Yes	0.66
Sex	Yes	No	No	0.33
Phone number	No	Yes	Yes	0.66
Medical history	No	Yes	No	0.33
Individual concern	5	4	3	
Privacy sensitivity	1.25	1	0.75	

illustrated in Fig. 2, the privacy score for the parameter set can be calculated as in Table 1. From this example, we can immediately identify Bank Information as the most critical privacy concern from the privacy score list. The business practitioner can also distinguish the "privacy sensitive customer" (A) and "privacy tolerant customer" (C) based on the privacy sensitivity indicator.

We are now able to derive various privacy indicators of many different privacy issues in different {context, time, space} setups. In what follows, we investigate the economic realizations of this model to show how and by how much the social welfare can be increased along with a possible increase in a business practitioner's profit function.

Customized Privacy

There is an increasing demand for complete privacy protection. However, it is extremely difficult to provide complete privacy protection, especially in a large population. Privacy protection through law seems to have reached its limit. For example, Gavison (1980) points out that law has its constraints to protect different privacy demands, with each individual valuing privacy concerns in a complex manner with other personal needs such as liberty, mental health, and financial constraints. Based on the information relevance model of privacy described earlier, we argue that privacy as a demand really differs at the individual level. As a result, to protect privacy, efforts should be focused in the direction of product/service differentiation. Differentiated (even customized) privacy protection on products indeed has already existed for centuries. For example, a local supermarket stocks several different kinds of locks in different sizes and strengths to cater to different physical security and privacy needs of customers. The lock market is perfectly differentiated so that customers can choose the appropriate lock according to her unique needs and willingness to pay. In this market, a customer is not forced to pay more for a stronger lock that she doesn't need. On the other hand, she is not forced to buy a smaller lock if her security needs dictate a stronger lock—she can buy a stronger lock by paying a premium.

We argue that the privacy protection market from an information economy perspective can be considered analogous to the lock market. Different people have different privacy protection needs and each such need can be satisfied at an appropriate cost, with some baseline protection for all regardless of their preferences. Researchers in this area have repeatedly shown that there is a huge difference between what people claim in terms of their privacy threshold and their actual behavior. For example, the same set of people who claim to care a lot about their privacy (e.g., in terms of name and telephone number) don't mind their private information to be collected at a McDonalds in exchange for a free big-mac a few moments later. In other words, privacy to some extent has its intrinsic value across individuals, but the valuation and preferences are different. In what follows, we consider a business scenario where privacy protection service bears a certain cost and consumers have individualized demand and preference on privacy. Consumers can also be characterized based on their price elasticities of consumption.

Centralized management philosophy such as government regulation doesn't make much sense in the modern information economy because of the complications associated with privacy management Bowie and Jamal (2006). However, decentralized privacy management is not commonly observed in current practice of most firms. Privacy is commonly protected through a uniform policy where everyone is covered by the same techniques and at the same price. We show possible managerial and economic incentives of privacy differentiation and customization based on an economic model.

There exists a huge amount of literature on nonlinear pricing and product differentiation of both traditional and information goods (e.g., Sundararajan 2004; Hoch et al. 1999; Jedidi et al. 2003; Lambrecht and Skiera 2006; Schmalensee 1981). We base our analysis on classical industrial organization literature Tirole (1988) by considering both horizontal and vertical differentiation. Differentiation based on higher and lower quality is vertical, whereas differentiation based on different functions is considered horizontal. An example of vertical privacy differentiation is found in the context of online information protection. A retailer can offer to protect personal identification and transactional information on the "cloud" (low quality) compared to another type of protection that is based on an encrypted and secured server (high quality). Although both these are privacy protection services, the degree (quality) of protection is different. As another example of horizontal differentiation, while some people might prefer to protect their personal identification, others

may be more concerned with their transactional information. Personal ID protection and transactional data protection serve as two functions (options) and are thus considered horizontal. Lastly, there are always some customers who may not necessarily care at all about privacy protection.

Vertical Differentiation

In a vertical privacy differentiation scheme, all consumers consume one principal good with a set of privacy protection levels. It's clear that in general, customers prefer higher privacy levels. For example, a stand-alone database server (high level) is generally preferable to a cloud (low level) data backup for high-security data. In a setup comprising vertical privacy differentiation, each consumer consumes one or zero units of the principal good at a selected level of privacy protection. We assume that a consumer has the following preferences $U(s,p)$

$$U = \begin{cases} S + \theta s - p & \text{if she buys a good with privacy} \\ & \text{level s at price } p \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

U represents the surplus derived from the consumption of the good/service. S is a positive real number that represents the surplus from consuming the main good/service. s indicates the level of security/privacy protection service. θ, a positive real number, indicates a privacy sensitivity parameter.

If we let $\tilde{p} = p - S$, the first term in equation (3) becomes $U = \theta s - \tilde{p}$. We assume that all consumers prefer a high level of privacy protection for a given price. However, the price increases with an increasing level of privacy protection. The privacy sensitivity parameter, θ, follows a density function $f(\theta)$ with cumulative distribution function $F(\theta)$ in the range $[\underline{\theta}, \overline{\theta}]$, where $F(\underline{\theta}) = 0$ and $F(\overline{\theta}) = 1$. The demand function for privacy preference s and price p for this utility function can thus be written as:

$$D(s,p) = N\left[1 - F\left(\frac{\tilde{p}}{s}\right)\right] \tag{4}$$

where N indicates the total number of consumers.

Theorem 5.1 The true demand with privacy issue is always lower than the demand without privacy issue.

Proof From equation (2), a proportion $NF(\tilde{p}/s)$ of consumers leave the market, concerned with privacy issues. Moreover, $F(\tilde{p}/s)$ is always greater than or equal to zero, resulting in $1 - F\left(\frac{\tilde{p}}{s}\right) \leq 1$. □

We now consider a scenario where two levels of security and privacy protection sL and sH are offered, and the consumers choose between the two levels as well as decide whether to purchase at all. We assume that $sL < sH$ and $pL < pH$,

Theorem 5.2 With privacy differentiation, more demand would be generated compared to the traditional uniform coverage plan.

Proof Without differentiation, the firm offers only one level of privacy protection and the demand follows $D(s,p) = N[1 - F\left(\frac{\tilde{p}}{s}\right)]$. Now the firm offers two levels of privacy service sL and sH such that $sL \leq s \leq sH$. The demand for high level service would become $D_2 = N[1 - F((p\tilde{H} - p\tilde{L})/(sH - sL))]$ and the demand for low level service is $D_1 = N[F((p\tilde{H} - p\tilde{L})/(sH - sL)) - F(p\tilde{L}/sL)]$. Combining the demand for both high and low level of privacy protection, the overall demand is $N[1 - F(pL\tilde{/}sL)]$, which is always greater or equal to the demand and follows a uniform coverage as described in Eq. (4). □

Theorem 5.3 More consumer social welfare would be generated with privacy differentiation compared to the traditional uniform coverage plan.

Proof The social welfare with a uniform privacy coverage is

$$W = \int_{\underline{\theta}}^{\overline{\theta}} U(\theta)F'(\theta)d\theta = \int_{\tilde{p}/s}^{\overline{\theta}} (S + s\theta - p)F'(\theta)d\theta$$

With vertical privacy differentiation, the total social welfare is the sum of both high level and low level privacy protection

$$\begin{aligned} Wdiff &= \int_{(p\tilde{H}-p\tilde{L})/(sH-sL)}^{\overline{\theta}} UH(\theta)F'(\theta)\mathrm{d}\theta \\ &\quad + \int_{p\tilde{L}/sL}^{(p\tilde{H}-p\tilde{L})/(sH-sL)} UL(\theta)F'(\theta)\mathrm{d}\theta \\ &= \int_{(p\tilde{H}-p\tilde{L})/(sH-sL)}^{\overline{\theta}} (sH\theta - p\tilde{H})F'(\theta)\mathrm{d}\theta \\ &\quad + \int_{p\tilde{L}/sL}^{(p\tilde{H}-p\tilde{L})/(sH-sL)} (sL\theta - p\tilde{L})(\theta)F'(\theta)\mathrm{d}\theta \\ &\geq \int_{\tilde{p}/s}^{\overline{\theta}} (s\theta - \tilde{p})F'(\theta)\mathrm{d}\theta \end{aligned}$$

□

Theorem 5.4 A firm with privacy differentiation generates more profit compared to one with traditional uniform coverage plan.

Proof In general, the firm's profit with uniform privacy coverage is

$$P = \int_{\underline{\theta}}^{\overline{\theta}} (p - c_1 - c_2)F'(\theta)\mathrm{d}\theta$$
$$= \int_{\tilde{p}/s}^{\overline{\theta}} (p - \tilde{c})F'(\theta)\mathrm{d}\theta$$

assuming that the marginal cost of the principal product component is c_1, the marginal cost of the privacy service is c_2, and $\tilde{c} = c_1 + c_2$. The overall profit of the firm with privacy differentiation is

$$Pdiff = \int_{(p\tilde{H}-p\tilde{L})/(sH-sL)}^{\overline{\theta}} (pH - \tilde{c})F'(\theta)\mathrm{d}\theta + \int_{p\tilde{L}/sL}^{(p\tilde{H}-p\tilde{L})/(sH-sL)} (pL - \tilde{c})F'(\theta)\mathrm{d}\theta \geq \int_{\tilde{p}/s}^{\overline{\theta}} (p - \tilde{c})F'(\theta)\mathrm{d}\theta$$

□

Theorems (5.1–5.4) show that because of privacy issues, some consumers leave the market without consuming the principal product. A basic uniform privacy commitment helps the firm only to some extent and a differentiated privacy policy could help the firm to enlarge the market and help customers enjoy more social welfare. A first degree differentiation regarding privacy preference is to offer a mass customization of privacy protection options such that all the original customers of the principal product are retained.

Horizontal Differentiation

Privacy tastes vary in the population. While a large proportion of personal information may evoke privacy concerns, the answer to the question "who cares what" is really heterogeneous. A patient who is ill is more likely to prefer medical information to be privacy protected while a healthy person may not mind the same type of information to be revealed. An illegal resident would do whatever he/she can to hide his personal identity information (to an extreme, even to fake or change it) while people with legal residential status are relatively likely to share their identity, for example, in order to obtain a fidelity card at a local grocery store. Consumers have their preference among a set of privacy components, and the firm provides horizontal privacy differentiations. In this case, there is no degree difference in terms of high or low level of privacy protection as was previously discussed for vertical differentiation.

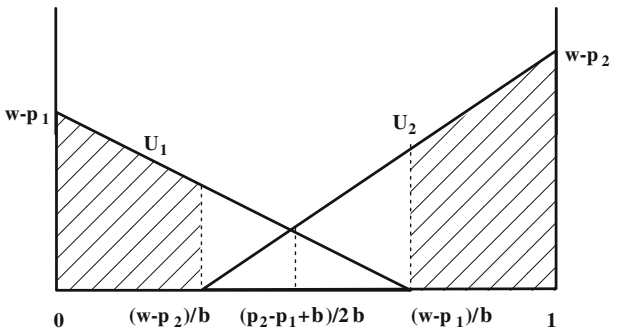

Fig. 3 Consumer surplus in horizontal privacy differentiation

We base our following discussion on a classical linear Hotelling model. Assume that there are two privacy concerns and there exists a virtual line, of length normalized to one, between these two concerns. Each customer is located on this line such that the distance from her to one concern is x and that to the other is $1 - x$. Let p_1 and p_2 denote the prices charged for these two concerns. The generalized price of the first concern is $p_1 + \beta x$ and the price of the second one is $p_2 + \beta(1 - x)$, where β indicates the trip cost that each consumer has to bear for the gap between her true needs and firm's offerings. Let w denote the surplus for each consumer when she consumes the good. The utility for both type 1 and type 2 consumers are

$$U_1 = w - p_1 - \beta x \quad (5)$$

$$U_2 = w - p_2 - \beta(1 - x) \quad (6)$$

As a result, the demand for the principal product with type 1 and type 2 privacy protections are

$$D_1 = N[(p_2 - p_1 + \beta)/2\beta] \quad (7)$$

$$D_2 = N[(p_1 - p_2 + \beta)/2\beta] \quad (8)$$

where $(p_2 - p_1 + \beta)/2\beta$ indicates the indifference point between type 1 and type 2 and can be derived by setting $U_1 = U_2$.

Theorems (5.1–5.4) derived for the vertical privacy differentiation case also apply to the horizontal case. It signifies that as in the vertical differentiation case, horizontal privacy differentiation would enlarge the market of the principal good, generate more consumer social welfare and more firm profit. Figure 3 shows that with only one

privacy choice, it would lose $[(w - p_1)/\beta, 1]$ market share with type 1 privacy service and $[0, (w - p_2)/\beta]$ market share with only type 2 service.

Concluding Remarks

With the increase in popularity of IoT devices (e.g., wearable fitness devices) and their ubiquitous presence on the Web (e.g., social media), it is necessary and urgent to address related privacy/security issues. We observe that tolerance or requirements with respect to privacy/security issues may not necessarily be the same across individuals and their associated IoT devices across different points in time. Technologically, it is feasible to customize or to differentiate privacy policy to fit each individual's privacy need by customizing the configuration of each device. However, while some of these technologies support the idea of customization of privacy, clearly there are instances where a uniform policy is followed. We contribute to existing literature on privacy by offering a novel angle of privacy differentiation and customization, with a specific focus on IoT.

We base our investigation and model development on existing privacy literature in the domain of business ethics, law and industrial organization. We first introduce a new paradigm of contextual concept by extending the classical privacy concept model to the set of {context, time, space} perspectives. Based on this, we develop the privacy relevance model to incorporate a measurement system to differentiate privacy demand from different individuals/groups in the population. Lastly, we study the social welfare of possible privacy differentiation schemes, such as horizontal and vertical differentiation. We show that privacy differentiation and ultimate privacy customization would lead to increased social welfare and possible firm's profit improvement. We conclude that the proposed privacy protection scheme could lead to a win-win situation for both business and consumers, by eliminating the inefficiency that exists in traditional uniform one-size-fits-all privacy policy.

Extensions of this research can be guided toward finding the optimal privacy protection package such as those that are widely used in product/service bundling literature. Some parts of the current work also need further empirical testing, such as the degree of possible privacy differentiation, the links in privacy concepts between any two social contexts, and the privacy preference differences that root from spatial and temporal differences. Specific extensions to this work may also involve restrictions to specific domains to narrow privacy relevant issues only to those domains (e.g., online market place).

We also want to acknowledge the difficulty in implementation of complete privacy differentiation/customization in real business situations because of technological and possible budgetary constraints. However, a small scale privacy differentiation/customization in a controlled environment could prove to be feasible. With fast advances in information and communication technology (ICT), we foresee the realization possibility of privacy differentiation/customization in the not so distant future.

References

Albrecht, K. (2008). How RFID tags could be used to track unsuspecting people. *Scientific American*, *299*(3), 72–77.

Barnes, B., Bonalle, D.S., Saunders, P.D. (2005). Method and system for facilitating a shopping experience. United States Patent Application, 20050038718, February 17.

BBC. (2010). Conservative liberal democrats deal. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/politics/election_2010/8677933.stm. Accessed 10 May 2014.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the internet: Self-regulation or government regulation? *Business Ethics Quarterly*, *16*, 323–342.

Drake, M. J., & Schlachter, J. T. (2008). A virtue-ethics analysis of supply chain collaboration. *Journal of Business Ethics*, *82*, 851–864.

EEA. (2001). Late lessons from early warnings: The precautionary principle 1896–2000. European Environmental Agency.

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal*, *89*(3), 421–471.

Gouvea, R., Linton, J. D., Montoya, M., & Walsh, S. T. (2012). Emerging technologies and ethics: A race-to-the-bottom or the top? *Journal of Business Ethics*, *109*, 553–567.

Hoch, Stephen J., Bradlow, Eric T., & Wansink, Brian. (1999). The variety of an assortment. *Marketing Science*, *18*(4), 527–546.

Hossain, M. A. (2009). RFID in National ID Cards: A privacy concern. Proceedings of the Fifth Asia-Pacific Computing and Philosophy Conference (AP-CAP).

Jedidi, Kamel, Jagpal, Sharan, & Manchanda, Puneet. (2003). Measuring heterogenous reservation prices for product bundles. *Marketing Science*, *22*, 107–130.

Jones, P., Clarke-Hill, C., Hillier, D., Shears, P., & Comfort, D. (2004). Radio frequency identification in retailing and privacy and public policy issues. *Management Research News*, *27*(8/9), 46–56.

Jourard, S. M. (1966). Some psychological aspects of privacy. *Law and Contemporary Problems*, *31*(2), 307–318.

Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). Guidelines for Securing RFID Systems. Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800–898.

Kelly, E. P., & Erickson, G. S. (2005). RFID tags: Commercial applications vs. privacy rights. *Industrial Management & Data Systems*, *105*(6), 703–713.

Kupfer, J. (1987). Privacy autonomy, and self concept. *American Philosophical Quarterly*, *24*(1), 81–82.

Lambrecht, A., & Skiera, B. (2006). Paying too much and being happy about it: Existence, causes and consequences of tarif choice biases. *Journal of Marketing Research*, *43*, 212–223.

Laurence, A., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*(2), 107–123.

Lucas, D. I., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders interests and values. *Journal of Business Ethics*, *22*(1), 27–38.

Martin, K. D., & Johnson, J. L. (2008). A framework for ethical conformity in marketing. *Journal of Business Ethics*, *80*, 103–109.

Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics*, *111*, 519–539.

Parent, W. A. (1983). Recent work on the concept of privacy. *American Philosophical Quarterly*, *20*(4), 341–355.

Parker, R. B. (1974). A definition of privacy. *Rutgers Law Review*, *27*(1), 275–296.

Parks, R., CHU, C.-H., & Xu, H. (2010). RFID information privacy issues in healthcare: Exploring the roles of technologies and regulations. *Journal of Information Privacy and Security*, *6*(3), 3–28.

Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, *59*(4), 327–345.

Posner, R. (1978). The right to privacy. *Georgia Law Review*, *12*, 393–422.

Schmalensee, R. (1981). Monopolistic two-part pricing arrangements. *Bell Journal of Economics*, *12*(2), 445–466.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1156.

Som, C., Hilty, L. M., & Köhler, A. R. (2009). The precautionary principle as a framework for a sustainable information society. *Journal of Business Ethics*, *85*, 493–505.

Spinello, R. A. (1998). Privacy rights in the information economy. *Business Ethics Quarterly*, *8*(4), 723–742.

Sundararajan, A. (2004). Nonlinear pricing of information goods. *Management Science*, *50*(12), 1660–1673.

Tirole, J. (1988). *The theory of industrial organization: Jean Tirole*. Cambridge: MIT Press.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), 63–70.

Wasieleski, D. M., & Gal-Or, M. (2008). An enquiry into the ethical efficacy of the use of radio frequency identification technology. *Journal of Business Ethics*, *10*, 27–40.

Waters, R. (2006). US Group Implants Electronic Tags in Workers. Financial Times.Retreived February 12, from http://www.ft.com/intl/cms/s/2/ec414700-9bf4-11da-8baa-0000779e2340.html.

Weissert, W. (2004). Chip Implanted in Mexican Judicial Workers. Associated Press. Retreived July 14, from http://www.infowars.com/print/bb/judicial_employees_implanted.htm.

Zhou, W., & Piramuthu, S. (2012). Technology regulation policy for business ethics: An example of RFID in supply chain management. *Journal of Business Ethics*, *116*, 327–340.