Hindawi Publishing Corporation
Advances in Human-Computer Interaction
Volume 2009, Article ID 713516, 13 pages
doi:10.1155/2009/713516

Research Article

Supporting Collaborative Privacy-Observant Information Sharing Using RFID-Tagged Objects

Shin'ichi Konomi[1] and Chang S. Nam[2]

[1] *JST/CREST and School of Science and Technology for Future Life, Tokyo Denki University, Chiyoda-Ku, Tokyo 101-0054, Japan*
[2] *Department of Industrial Engineering, University of Arkansas, Fayetteville, AR 72701, USA*

Correspondence should be addressed to Shin'ichi Konomi, konomi@acm.org

Received 24 November 2008; Revised 1 July 2009; Accepted 29 September 2009

Recommended by Armando Barreto

RFID technology provides an economically feasible means to embed computing and communication capabilities in numerous physical objects around us, thereby allowing anyone to effortlessly announce and expose varieties of information anywhere at any time. As the technology is increasingly used in everyday environments, there is a heightening tension in the design and shaping of social boundaries in the digitally enhanced real world. Our experiments of RFID-triggered information sharing have identified usability, deployment, and privacy issues of physically based information systems. We discuss awareness issues and cognitive costs in regulating RFID-triggered information flows and propose a framework for privacy-observant RFID applications. The proposed framework supports users' in situ privacy boundary control by allowing users to (1) see how their information is socially disclosed and viewed by others, (2) dynamically negotiate their privacy boundaries, and (3) automate certain information disclosure processes.

1. Introduction

Our everyday world is increasingly populated with digital technologies. Mobile phones, for example, enable people to access information and communicate with friends online "anywhere at any time." They are being integrated into various facets of our lives, allowing for unique communication practices [1] to emerge. There are other forms of pervasive technologies from tiny microchips and sensors to large interactive surfaces, these new and pervasive technologies are finding their places in our society.

ID markers such as RFID tags and 2D barcodes are key components that tie physical objects to digital information [2]. Telecom operators, particularly, have keen interest in such services. For example, in 2002, Japanese mobile carrier J-Phone introduced one of the first mobile handsets (J-SH09) that can process a 2D barcode and display a corresponding website. Today, most of the mobile phone users in Japan own such barcode-enabled handsets [3], and 2D barcodes are printed on some product packages, ads, posters, magazines, web pages, business cards, and so on to guide users to relevant wireless web pages and services. Amazon Japan's Scan Search service [4], for example, allows consumers to scan ordinary barcodes using mobile phones and access Amazon's corresponding product information. In addition, an increasing number of mobile phones can read RFID tags and access relevant information. For example, Nokia has introduced NFC [5] devices that allow mobile phones to read RFID tags.

Not only is it economically feasible to attach individual RFID tags to high-value sales items, but supply chain and inventory management efficiency can be improved as well. In addition, numerous experiments are taking place to explore novel services using RFID-tagged "smart physical objects" [6]. For example, some retailers tested "smart shelves" that integrate RFID readers with store shelves so as to automatically monitor the presence of RFID-tagged sales items. The idea of combining "smart shelves" and surveillance cameras has keenly raised privacy concerns [7].

RFID technology [8–10] provides an economically feasible means to embed computing and communication capabilities in numerous physical objects around us. Large-scale RFID deployments are taking place not only to implement efficient supply-chain management systems but

also to provide various consumer-facing services [11, 12]. Most notably, such services facilitate information sharing and communication between consumers and retailers. For example, RFID technology could allow consumers to effortlessly announce and expose their information to retailers for personalized services and offers. However, there are questions about privacy implications of such information practices.

As pervasive computing technologies remove physical communication limits, there is a heightening tension in the design and shaping of social boundaries. There is a need for publicity and the ability to determine for ourselves when, how, and to what extent personal information is communicated to others. In supporting such a need, a key issue is raised in the availability of options, devices, and mechanisms that not only achieve desired interaction but prevent unwanted interaction. This view shares the same spirit with Irvin Altman's definition of privacy [13] as *selective control of access to the self or to one's group*. Such control is characterized by a dynamic and dialectic process in which different human behavioral mechanisms operate as a unified system to achieve privacy goals. Through such control, people can refine the boundary that distinguishes privacy and publicity according to circumstance [14]. Our approach to understanding this issue is in line with Dourish and Anderson's [15] argument for a move away from narrow views of privacy and security, as the focus of this study is on existing and emerging communication practices using RFID. Designing systems for the provision of appropriate information, with the right level of information disclosure/protection, requires an understanding of the practical uses of the information.

We propose a framework for collaborative privacy-observant information sharing using RFID-tagged objects. In our previous work [16–18], we implemented and tested *QueryLens*, a system that allows for information sharing using RFID-tagged physical objects and mobile devices. In particular, we tested the system in a controlled laboratory setting as well as in a university festival, and identified relevant usability, deployment, and privacy issues. Based on the data and anecdotal evidences from those trials, we discussed end user practices to connect with others, share information, and maintain social boundaries. Existing ID-triggered information sharing systems [16, 19, 20], including *QueryLens,* provide users with limited awareness about what happens to their personal information. Moreover, if users have any choices at all, existing systems often force users a binary choice in advance (e.g., specification of privacy preferences [21]), about whether or not to disclose their information.

In this paper, we frame privacy as a problem of boundary control between sender and receiver and discuss the challenges of providing appropriate feedback and control for in situ negotiation of privacy boundaries. It is difficult to support such interactive processes in situ as privacy requirements are influenced by complex contextual factors. This difficulty is exacerbated if arbitrary information flows and arbitrary contextual factors must be considered. To make the problem space tractable, we focus on three types of information flows that are triggered by RFID-tagged objects, and consider the roles of computational context-based representations in regulating these flows with or without user intervention. In order to facilitate the development of collaborative privacy-observant RFID information sharing, we propose a framework for visually representing contextual information and supporting mobile users to control what is in and out of their personal information spaces.

To enable fine-grain control over information flows, we formally define the structure of information that people disclose and access in RFID-based information sharing environments. We introduce a simple data model that considers users' interactions with RFID-tagged objects as well as the anonymity of the interactional records. These records are stored in a database along with the context of the corresponding interactions, and can be combined as well as aggregated with other information. To control information disclosure and access in such an environment, we consider ownership and use of privacy-sensitive information, and define input and output views of an end user based on a theoretical framework of privacy boundary regulation [13, 14].

This study demonstrates the usage of input/output views using a retail RFID example in order to enable visualization of information paths as well as malleable control over information flows, thereby facilitating reciprocal information disclosure as well as privacy boundary negotiations. This study also describes a user interface based on the proposed model. A user can access visual representations to understand what data is accessible, what data others are interested in, and how the user can actually present themselves to others.

2. Related Work

RFID tags and barcodes are used in various experimental systems that integrate digital information in the physical world. In general, existing systems provide limited support for collaboration and privacy protection. However, experiences in various application domains can be a valuable teaching tool. Researchers have proposed conceptual frameworks for protecting privacy in ubiquitous computing environments. Based on existing frameworks, we integrate user-friendly privacy-enhancing mechanisms in a collaborative information sharing model.

2.1. Sharing Digital Information in the Physical World. The idea of using ID markers for connecting physical objects and digital information is not new. ID-based information access has been studied in the WebStickers system [20] and in the CoolTown project [19]. In these efforts, Webpages were associated with physical entities using sensors and computing devices. There are projects that have explored social and dynamic aspects of physically-based information sharing. Burrell et al. [22] evaluated social aspects of a location-aware campus tour guide system, and Espinoza et al. [23] discussed the social filtering of information attached to geographic locations. Reno [24] is an application that allows

users to send their location to other people in their social network(s). Brush et al. [25] conducted a comprehensive field study of AURA, a system that provides users with relevant information using a wireless PDA and a barcode reader. AURA's privacy model is conservative in the sense that it explicitly asks a user if they want to publicly expose information about scanned objects rather than automatically uploading the information. The experience suggests that users may generally be in favor of such a conservative model.

Food and livestock industries are also exploring the use of RFID tags and 2D barcodes to implement food traceability systems. When such systems are fully implemented, in-store customers may use mobile phones to scan food packages' 2D barcodes (or use a kiosk terminal to scan packages' RFID tags) and easily access a website that shows corresponding historical information: how they were produced and transported, where they came from, who produced them, and so forth—some of which could be automatically captured using RFID and other sensors. Moreover, RFID tags could possibly be used to provide consumers with dietary guidance and food allergy alerts using third-party "overlay" databases [26]. However, some third-party databases, such as the ones providing price comparison information, could disrupt manufacturer/ retailer business models.

Researchers have explored application scenarios that consider the uses of RFID tags outside retail stores. Wan's [27] Magic Medical Cabinets, for example, utilize medicine bottles' RFID tags to reduce the cognitive burden to take the right medicine at the right time, and demonstrated a possibility of in-home assistive health technology [28]. In this type of application scenario, there seems to be a strong tension between benefits and privacy risks. RFID tags attached to personal objects tend to cause high privacy risks as they could be covertly scanned in public venues or in domestic environments. Indeed, EPC guidelines for Consumer Products [29] emphasize the consumer's choice to discard or remove RFID tags from acquired products.

2.2. Privacy Protection in Ubiquitous Computing. RFID is not the only technology that can cause privacy problems. In the past, inventions such as photography, polygraphs, database systems, and surveillance cameras triggered debates on privacy issues [30]. RFID technology may exacerbate privacy problems as it can allow for invisible capture and use of data about individuals without their knowledge. Once captured, "*sensitive private information might live indefinitely and appear anywhere at anytime*" [31]. In addition, RFID provides a means of unique identification, which would facilitate unambiguous detailed tracking of objects and people over time through accumulated records about their activities. Modern RFID systems face less expensive attacks than traditional high-budget military RFID systems as well [32]. Previously suggested approaches for preserving RFID users' privacy include

(i) destroying, removing, or permanently inactivating RFID tags (killing),

(ii) shielding tags by using a container made of materials that block radio signals (faraday cages),

(iii) shielding RFID tags by using a device that actively broadcast radio signals so as to block the operation of nearby RFID readers (active jamming),

(iv) locking, encrypting, manipulating RFID tags' data (e.g., [33]),

(v) blocking access to tags by using Blocker Tags, devices that announce themselves as all or a range of possible RFID tags [34],

(vi) processing data on personal devices as much as possible so as to avoid disclosing IDs to the infrastructure,

(vii) securely managing related database servers on the network, and

(viii) establishing guidelines and laws to regulate capture and use of sensitive privacy information.

These physical, digital, and social means of privacy protection can be combined to provide a useful solution. PAC (Physical Access Control) [35], for example, constrains data access so that the user can only access information about "nearby" events. Rastogi et al. [36] extend PAC to provide context-aware, rule-based access control. UCAL [37] is a relevant access control language that considers uncertainty in RFID data. This line of research emphasizes rule-based automatic privacy control and is complementary to our interactive approach that uses views to provide resources for interaction rather than automation.

Moreover, there have been extensive discussions on privacy-preserving data publishing methods in the database research community. Techniques to ensure anonymity, based on *k-anonymity* [38, 39] and *l-diversity* [40], are highly relevant because: even when disclosed RFID data does not explicitly contain personally identifiable information, the system could identify individuals by linking the data to other data or by looking at unique characteristics found in the data [38]. Some recent works extended and integrated *k-anonymity* into systems that handle RFID data [41] as well as moving objects [42].

One of the recurring themes in ubicomp privacy research is the tradeoffs between rewards and privacy risks. For instance, Acquisti [43] analyzes economic incentives of privacy preserving technologies and argues that individuals might be acting myopically when it comes to protecting their privacy. Hong and Landay [44] discuss information asymmetry among individuals involved in the exchange of private information makes it difficult to make informed decisions and assess privacy risks. Hong et al. [45] provide in-depth analysis of privacy risks in ubiquitous computing. Floerkemeier et al. [46] enhanced low-level RFID protocols in order to support *fair information practices*, a key notion that influenced privacy policies worldwide. Price et al. [47] extend Confab architecture [44] and propose a proxy-based system model for assisting users in balancing the tradeoffs between giving up privacy and receiving ubicomp services. Their models are designed to control the flows of privacy-sensitive information, however, without comprehensive support for RFID applications. Most existing systems utilize static privacy preferences and they rarely support the

social processes to dynamically negotiate preference settings. Privacy-enhancing user interfaces such as Faces [48] allow users to manage privacy preferences on stationary computers as well as handheld devices. Faces, in particular, employ the metaphor of *faces* to represent disclosure preferences. Faces could potentially facilitate users to manage privacy intuitively through their actions in situ if the user interface is appropriately integrated with users' practices to understand privacy implications and meaningfully act in the social world as well as system models and data structures. This study proposes a framework to explore a tighter integration of data structures and user interfaces as well as intuitive visualization of social information flows and individual privacy preferences.

Moving away from the narrow focus on the trade-offs and privacy preferences, broader social practices need to be considered. Dourish and Anderson's [15] view that *privacy is not simply a way that information is managed but how social relations are managed* is therefore relevant. In particular, one aspect to consider is the way people manage social relations in response to a privacy violation. Privacy violations occur in everyday life, and are often compensated by other actions. For example, one may interrupt another's private conversation because of some urgent need and act uncomfortably or appear apologetic—all because they had to invade another's privacy. In another example, reciprocity facilitates a successful negotiation of privacy boundaries among users of two-way video connections that force "if I see you, you see me" [49]. Another aspect is that privacy mechanisms define the boundaries of the self. Identity is a notion that is inseparable from privacy. Technology-mediated communication complicates regulation of the self/nonself boundary [14]. It changes the ways we perceive who is receiving information, what is received, and how it is received.

2.3. QueryLens: RFID Triggered Information Sharing. In order to understand the implications of RFID-triggered information services, a system that allows users to access and contribute queries, answers, and other types of information using PDAs and RFID-tagged physical objects, *QueryLens* [16–18], was implemented and tested. *QueryLens* was tested in a controlled laboratory setting as well as in a university festival. *The* test results suggest that details matter in facilitating collaboration among various users, and naive system design can lead to insufficient support for system usage awareness, in particular, the social context of RFID-triggered information exchange.

2.3.1. The QueryLens System. The *QueryLens* system supports dynamic and social information spaces by allowing users to easily share their personal and collective information needs. It features mechanisms for exchanging and reusing information needs using RFID, so as to facilitate collaborative construction of information spaces in relation to physical objects. *QueryLens* captures users' information needs as *query objects*, connects them with physical objects, allows users to share and modify them, and uses them to collect answers. The approach of *QueryLens* maintains that information contributions are equally as important as information access, while addressing some of the challenges of ubiquitous contributions by exploiting user profiles and shared persistent queries.

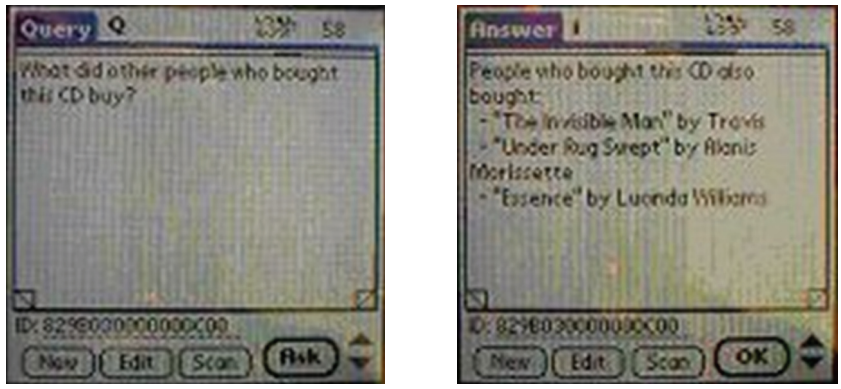
Figure 1: Using the *QueryLens* system.

The system was implemented by using a Palm OS(R) PDA, an RFID module (Inside Technologies Hand'IT), and a barcode module (Symbol(R) CSM 150) (see Figure 1).

A mobile database system was used to manage the information space. A PC database server (Sybase Adaptive Server Anywhere) and mobile PDA databases (Sybase UltraLite) synchronize with each other through a wired or wireless connection (For details, see [16]). A bi-directional synchronization mechanism was realized by using a database synchronization tool (Sybase MobiLink). The RFID tags (Inside Technologies PicoTag) operate at 13.56 MHz and their communication range is about several centimeters. Figure 2 shows a user interface for interacting with queries and answers. A user can browse queries by using a page-turn gesture on the touch screen, and obtain answers of a query by pressing the "ASK" button.

The same gesture can be used to browse answers. In addition, queries and answers can be displayed in a list view. The "NEW" button on each screen brings up a window to enter a new query (or a new answer), while the "EDIT" button allows users to modify the current query (or answer) and store it as a new query (or a new answer). The "Q" mark at the top of the screen (Figure 2(a)) indicates that there is an SQL query associated with this query. Selecting the "Q" mark brings up a window to view, modify, and execute the SQL query. The information generated by the query execution is added as an answer to this query. The "i" mark at the top of the screen (Figure 2(b)) indicates that there is some additional information related to this answer. Selecting the "i" mark brings up a window with a list of URLs, multimedia files, and so forth. When users want to simply view and attach annotations to a physical object, they can switch the software to the "info mode" in which users can use *QueryLens* as a sort of a digital version of PostIt Notes. The information space of the "info mode" is a subset of the information space of the regular "Q&A mode."

When a query is contributed, its answers may not exist in the information space yet. The *QueryLens* system collects answers using the following methods.



(a) Query (b) Answer

Figure 2: Graphical user interface of *QueryLens*.

(i) *Making queries accessible to other users*. The query is displayed when other users scan the same physical object.

(ii) *Active querying*. A user can specify recipients (individuals or groups) of her query using a pop-up selection list. When the recipients scan the corresponding physical object, the query is brought up in a pop-up window asking for an answer. In addition, users can subscribe to a physical object (Subscribing a physical object sends users the relevant queries by email.).

(iii) *Searching existing information resources*. The system can associate SQL database queries with corresponding natural language queries and use them to automatically fetch answers from existing databases. For example, using this feature, a query about a book's publication date can be retrieved from an existing bibliographic database.

User profiles are internally represented as SQL expressions, and can be configured using a Web interface. The current prototype provides a Web interface that allows users to select queries and answers according to languages, ratings, and contributors of information. The SQL expressions dynamically generate bitmaps, which specify queries and answers to deliver to the user.

2.3.2. Evaluation and Design Implications. We conducted an empirical user experiment to systematically evaluate the overall quality of the *QueryLens* system in order to obtain usability and performance data, as well as develop design guidelines for the development of RFID-based context-aware information sharing systems (for details, see [18]). In particular, this study employed two different user groups (i.e., 10 young participants whose mean age was 21.20 and 10 elderly participants, whose mean age was 57.30) to evaluate whether *QueryLens* effectively supported diverse user group interactions with information sharing system while minimizing distraction(s). The results of the study showed that the *QueryLens* system effectively supported social interactions for diverse user groups, showing no significant differences in task performance, user satisfaction, and perceived workload.

This usability study provided several practical implications for the design of RFID-triggered information sharing environments. First, we believe that user interfaces of such environments should be usable and accessible regardless of an individual's age, gender, experiences, physical and cognitive abilities, and so forth. Various types of media and interaction modalities should be supported to cater to diverse user populations, preferences, and settings. Second, RFID-triggered information should be presented in a manner that reduces distractions. Realizing Calm Technology [50] is not just about delivering accurate information: it is also about engaging both the center and the periphery of our attention. Some information should be "pushed" to the user while other information should be "pulled" by the user. Third, users' context needs to be carefully considered. For example, users may communicate in a succinct manner, depending on what the system seems to automatically capture. In such cases, difficulty can arise in communication when users do not share necessary context. For example, if a person on a train receives a question such as "where was this picture taken?" from a consumer in a music CD store, the query may not make sense without contextual information (e.g., the picture, the title of the CD, etc.) A user's privacy must be considered when systems automatically supplement contextual information. Also, different types of relationships between physical objects and digital information must be considered. For example, users may or may not expect that all music CDs of an artist bring up the same information.

A small field test of *QueryLens* was conducted in a university festival, in which groups of like-minded students organized various activities such as lectures, art exhibitions, concerts and food/shop tents at various (indoor and outdoor) locations on campus [16]. A mobile phone client of *QueryLens* was developed so that festival visitors could exchange queries and answers about these events using their mobile phones. Unique numbers were assigned to the events, which could be entered using phone keypads. Based on anecdotal evidences from a preliminary field observation, the following issues were identified.

(i) The *QueryLens* system has its own chicken-and-egg problem. The system becomes useful when its information contents are enriched by users' contributions. However, in order to motivate users to contribute information, the system must also be useful.

(ii) Deploying usable event codes can be socially and economically challenging. Due to limited human and financial resources, the festival's official event codes were designed by the administrative organization. Even though these codes were short, they were difficult to input on a mobile phone because the codes were mixtures of alphanumeric and Japanese characters.

(iii) In general, mobile phones are not good for text entry tasks. The system required users to enter small amount of text: a URL for connecting to the service, a user ID and a password for authenticating users (anonymous uses were permitted at a later point in time), and free text for queries and answers—somewhat burdensome tasks for many users.

(iv) Several people said that they wanted to use *QueryLens* for doing things besides sharing queries and answers. For example, some users wanted to use the system for displaying maps and showing directions to events of interest.

Privacy was an important issue that implicitly influenced the ways people used the system. During the field test, software updates were implemented to improve usability. Initially, the system required users to first create a user account and log in every time they use the service. The number of users increased after we modified the software to allow anonymous user log-in. This increase could be explained as a result of the reduction of perceived privacy risks as well as improvements in usability. Since this system upgrade resulted in both usability improvement and the introduction of anonymity, simplistic conclusions cannot be made about the impact of privacy on increased usage.

Users may desire anonymous usage in some cases; however they may not in other cases. In particular, anonymous usage eliminates users' capability to socially disclose information [24] to others in their social network(s). Users may, for example, want to disclose shopping cart items to their family members. Users' information sharing requirements are inseparably related to privacy requirements and can be contextually different. In order to design solutions for this fundamental issue along with the other issues discussed, a framework for transparently managing social boundaries and information flows in RFID-triggered information sharing environments will be introduced.

3. A Framework for Supporting Boundary Control

In RFID-triggered information systems, social disclosure and privacy preservation are key concerns. Although researchers acknowledge the importance of intuitive privacy management through users' actions in situ [48], it is still difficult to design interactive systems that can integrate privacy-management practices and underlying system/data models. To develop a framework for supporting intuitive privacy management in situ, a tighter integration of data models and user interfaces as well as effective visualization of information paths and flows were explored. Based on the discussion of context as a resource for actions [51], the role of contextual factors was considered, including the uses of views and other elements in a data model, as resources for privacy management. Unlike existing approaches that use views for automated control [36], this study proposes an approach that presents contextual views to support privacy management. In particular, a framework was introduced for visually representing contextual information on mobile devices, and thereby giving users the ability to adjust socially-defined boundaries and to control RFID-triggered information flows.

3.1. Designing for Feedback and Control. Some of what people take for granted in face-to-face interactions may be reduced or lost in interactions mediated by RFID. Bellotti and Sellen [49] proposed a design framework for counteracting problems related to privacy issues in ubiquitous computing environments. Their conceptual design framework was integrated to systematically support social negotiation processes for dynamically modifying RFID-triggered information flows. Designing appropriate feedback and control depend on context in which they are embedded [52, 53], including individual user preferences. Control parameters' default settings are particularly important for a new user. Technology-based privacy regulation mechanisms can be described in terms of different categories of feedback control processes [54]. One can create structures that prevent unwanted access *before* someone can access information. One can also allow anyone to access one's information; however, access to the information is monitored and recorded. One can subsequently revoke another's ability to access the information if needed. Alternatively, one can respond to each request and interactively deny or accept access.

RFID-triggered information media complicates the management of boundaries that separate and connect one's personal (information) spaces and the rest of the world. They are not merely defined by physical relationships such as geometric distances. They are also shaped by one's activities and social contexts. For example, information about things one touches can be public when one is at work in a warehouse. How much one considers RFID data can be private is also influenced by the cost of removal. For example, RFID train passes could be removed from the person more easily than RFID implants.

3.2. Information Flows. RFID information systems can be classified into three types according to the ownership of RFID readers and tags. In Figure 3(a), data about *scans* are disclosed from the environment (Type I information flow).

A user could directly control the information flows that are indicated with solid-line arrows by using "kill" kiosks, faraday cages, and so forth. In Figure 3(b), data pertaining

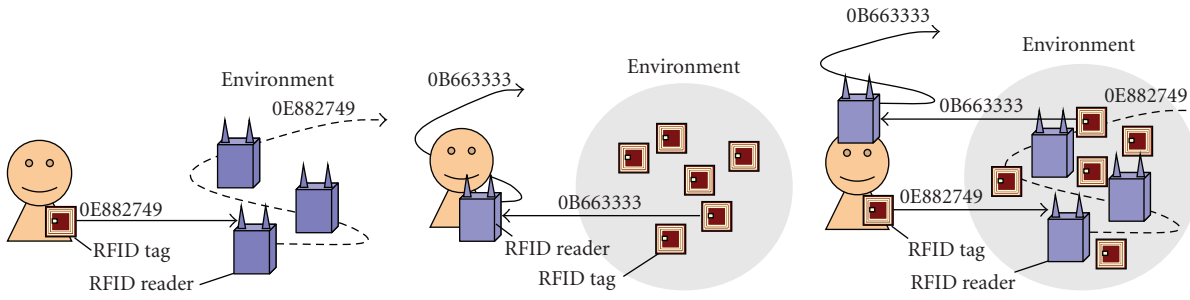


Figure 3: Information flow.

to *scans* are disclosed from the user (Type II information flow). Users could directly control the information flows that are indicated with solid-line arrows by turning on/off readers, controlling access to readers' data, and so forth. In Figure 3(c), Type I and II information flows coexist, and scan data are disclosed from the user and the environment. In this study, privacy-observant social information disclosure is related to these three types of information flows.

3.3. Disclosure Processes. This study assumes two distinct types of information disclosure processes, namely, *full disclosure process* and *expedited disclosure process*. In the full disclosure process, the system asks a user whether or not to disclose a scan. In this case, the user can have detailed interactive control over the disclosure of each *scan*. However, cognitive workload for the full process may be very high if users must deal with a large number of RFID tags individually. In contrast, the expedited process does not allow interactive control at all. Systems automatically disclose or conceal *scans* based on predefined default settings, thereby minimizing the users' cognitive workload for privacy regulation.

The transition between full and expedited processes needs to be carefully considered since users must come to trust the system in order for the automated process to work. For example, the detailed interactive control of the full process may need to fade away as the users' states change rather than disappear abruptly.

3.4. Modeling Contextual Information in RFID Systems. This study's approach is to develop a simple context model so that users can easily select appropriate information disclosure process. Since it is difficult to define what *context* is [55], the discussion is limited to *contextual information* in RFID-triggered information systems. Key components in the context model include *scan record s*:

$$s(id, data, rid, t); \tag{1}$$

is a unique serial number assigned to an RFID tag; *data* is any additional data stored in a tag; *rid* is a unique identifier of the RFID reader that scanned the tag; t is a timestamp. In a relational database, scan record s can be stored as a record in a relation. Collective units of *scans* were used to model context in relation to the user' *actions* and *activities*. A user's action generates a group g of scan records s_i $(1 < i < n)$ in the system. Then, the user's activity that involves m actions generates a group of groups $g_j (1 < j < m)$. These groups can be used to manage action or activity-relevant context.

Scan records are the kind of *microdata* [56] that have privacy implications when they are linkable to a person. For example, RFID tags embedded in cosmetic products, when used together with a surveillance camera, keenly raised privacy concerns [57]. In this case, scan records could potentially be linked to personally-identifiable images based on the time and location of data capture. In general, data without personally-identifiable information can be used to identify individuals by linking or matching the data to other data or by looking at unique characteristics found in the released scan records [38].

Scan records and their groups are *explicitly* owned by users or *implicitly* linkable to them. For example, if Bob purchased a kid's sweater, its RFID tag can be explicitly associated with Bob and implicitly with Bob's son. $f(x)$ denotes a function for obtaining a set of people who own or are linkable to data x. $f(s)$ and $f(g)$ obtain a set of people related to scan record s and scan group g, respectively. Techniques to achieve k-anonymity [38, 39] can be used to control the cardinalities of $f(s)$ and $f(g)$.

We first define basic *context object c* as follows:

$$c(id, value); \tag{2}$$

id is a unique identifier and *value* is a data item of a basic type such as a numerical or string value. Context objects can also be defined using a set of other context objects or a tuple of attribute-value pairs.

A context relationship then is represented as a relationship of subject *sub* and context object c:

$$r(sub, c). \tag{3}$$

Subject *sub* can be scan record s, scan group g, or any other piece of information. Note that any context that is not explicitly defined using relationship $r(sub, c)$ is *implicit*. Context object c is identical to c' if $c.id = c'.id$. c is equivalent to c' if their values (or query results) are the same. Context objects can be instantiated using the data retrieved from corresponding relations or *views* in a database. At this level

of modeling, any context object c can contextualize subject *sub*.

3.5. Boundaries as Two-Way Permeable Views in Context. *Views* are system components that are widely used in data management systems. They allow users to manage data presentation without affecting underlying data. *Views* are also used to enhance database security [58, 59]. We exploit and enhance *views* so as to provide users with lightweight methods for adjusting presentation of personal data and managing information flows.

Mobile users need the "right" data spaces at the "right" place and at the "right" time according to their changing needs. Traditionally *views* are *static* system components that are rarely changed once they are created. In order to support the dynamic aspects of mobile users, we introduce *view* object v:

$$v(id, q); \tag{4}$$

id is a unique identifier and q is a query that defines a view. Context can now be represented as $r(v, c)$. Below is a sample query q for defining a *view* that shows products linkable to John Smith:

```
SELECT product.name
FROM scan_rec, product
WHERE scan_rec.id = product.id
AND f(scan_rec.id) = 'John Smith';
```

View objects can be associated with context objects in order to limit linking of scan records with other information. For example, the system can impose a constraint that scan record s with context $r(s, c)$ can be accessed by or joined with view object v only if c is equivalent to c' such that $r(v, c')$. If v is defined by the above query and $c'.value$ = "FoodMart," v only retrieves information about scans that take place at FoodMart.

Based on Altman's model of privacy [13], privacy-observant social disclosure can be characterized by two kinds of information flows across a personal boundary: one coming into a person from others (inputs) and the other going out of a person to others (outputs). We denote *view* objects for inputs and outputs by $v_u \downarrow(id, q)$ and $v_u \uparrow(id, q)$, respectively. That is, *output view* $v_u \uparrow$ is a *view* accessed by someone other than u and $f(v)$ contains user u. *Input view* $v_u \downarrow$ is a *view* accessed by user u. We use $v \uparrow$ and $v \downarrow$ when user u is trivial. We now discuss boundary control that is performed through regulating $v_u \uparrow$ and $v_u \downarrow$.

3.6. Privacy-Sensitive Data. Our general idea is *to allow or disable uses of privacy-sensitive data based on context*. However, unlike security management, neither the system nor the users know in advance what the optimal state is. Therefore, we should rather provide users with a stage for exploring satisfying solutions through open-ended negotiations.

Privacy-sensitive data are characterized by *ownership* and *privacy concerns*, which can be represented by using partially-ordered privacy classes (e.g., "complete privacy," "limited time," "limited use," "accountable," "open," etc.). In a relational database, these classes could be assigned to individual records, attributes, or relations. In this paper, we only consider relation-wise privacy classes, that is, privacy concerns are assumed to be the same for all attributes and records in a relation. Usage of privacy sensitive data is characterized by their *functions* and *purposes*. Functions describe functional roles of a data item in the system. For example, a data item can be used as an identifier, a service handle, an input to predicate, or a source of a copy operation [60]. Purposes are represented as a context object in our model.

Although our *context* model can represent a wide range of contextual relationships, we initially focused on time, location, user groups, and purposes in our system development effort. A context object is associated with multiple *view* objects. Each *view* object has an owner and is assigned a privacy class.

For simplicity, we assume that the system authenticate users by using RFID tags (e.g., RFID consumer loyalty cards). A user is associated with a set of context objects $C = \{c_1, c_2, \ldots, c_n\}$ via a set of scans $S = \{s_1, s_2, \ldots, s_n\}$, which includes the scanning of the user's RFID card. Let $V = \{v_1, v_2, \ldots, v_m\}$ be a set of *view* objects associated with context objects C. The user can only access view objects in V. This context-based access constraint can support user authentication methods other than RFID cards with a minor modification.

3.7. Supporting Boundary Control. By explicitly representing context and views in the system, we can support the process of *allowing or disabling uses of privacy-sensitive data* using various mechanisms. This idea, which is influenced by the discussions of context as a resource for actions [51], guides the design of our framework and user interface. In our framework, context objects can be seen as "virtual places" where users present themselves to others and are watched by others. In face-to-face interactions, information disclosure is often reciprocal. If I see you, you see me; and how I look at you can be an important resource for your adjustment of self-presentation. *View* objects are used to facilitate similar reciprocal interactions in RFID applications.

Figure 4 illustrates how our framework can support privacy boundary control in an RFID-based mobile information service (We use the example of a retail store to demonstrate the use of our framework; however, the proposed framework can be used for RFID-triggered information sharing in other kinds of everyday spaces including museums and libraries). This service allows customers to scan RFID tags attached to individual sales items in a store using PDAs. The PDAs then show relevant information that could be useful for shopping. Using a wireless network, users may disclose their personal information to a family member, a sales agent or a store manager.

In Figure 4, there are three context objects c_1, c_2, and c_3 representing three different locations/times: "*Store A*," "*Aisle 5 of Store A*," and "*special discount time at Store A*." In *Store A*, the customer, the sales agent, and the store manager are

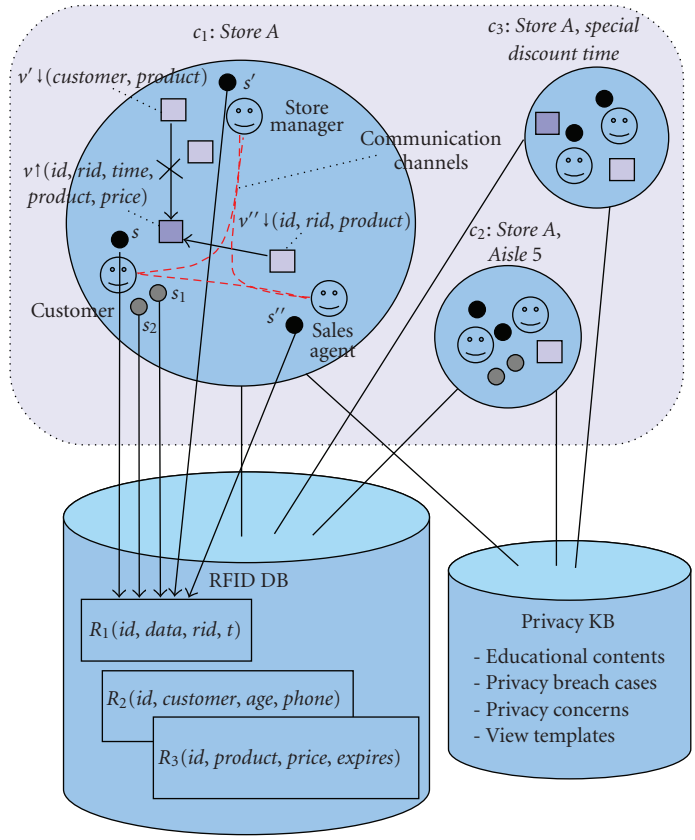


Figure 4: Applying our framework to a retail RFID application.

identified by using RFID identification cards (s, s', s'') and these scan records are stored in the database (*RFID DB*). The customer first set up a privacy preference, generating the output *view* $v\uparrow$(*id*, *rid*, *time*, *product*, *price*).

The customer then scanned a kitchen gadget (s_1) and a cough medicine (s_2) using a PDA while shopping. The sales agent's input view $v''\downarrow$ (*id*, *rid*, *product*) is subscribed to output view $v\uparrow$. This is an explicit representation of how the sales agent watches the customer and the store could promise to adhere to a "meta-level" policy of disclosing their *view* objects to relevant consumers. $v'\downarrow$ (*customer*, *product*) is also subscribed to $v\uparrow$; however, $v'\downarrow$ conflicts with $v\uparrow$ since $v\uparrow$ is defined to conceal attribute *customer* and $v'\downarrow$ accesses attribute *customer*. Communication channels among the customer, the sales agent, and the store manager include email and text annotations attached to view objects and subscriptions.

Finally, the privacy knowledge base (*Privacy KB*) provides resources for users to learn about privacy issues and access privacy breach cases and common privacy concerns that are pertinent to current context. It also manages view templates so that users can easily create *view* objects.

Without this study's framework, it is difficult to know who is monitoring one's captured/stored data and how they are monitoring data storage. It may be stated in the store's privacy policy; however, it can be a large burden for consumers to access, read, and understand the privacy policy. Also, consumers have very limited control: their options are accepting the store's proposed data or not utilizing the service. A privacy policy could easily be outdated or too general to be practically useful.

The proposed framework has the following advantages.

(i) Users can easily see how their information is being viewed by others. For example, the customer can access $v'\downarrow$ and $v''\downarrow$ to check how the sales agent and the store manager are monitoring (or are requesting to monitor) data collection. The system can automatically generate a summary of all subscribed *views* as well. The system can also compute the difference between *view* objects (e.g., the difference between $v\uparrow$ and $v'\downarrow$).

(ii) Users can socially negotiate privacy boundaries. The study's framework enables the situation where output view $v\uparrow$ and input view $v\downarrow$ are different. This means even though all attributes of $v\uparrow$ can potentially be viewed by anyone, others may be viewing less information. The difference between $v\uparrow$ and $v\downarrow$ enables "soft" privacy boundaries that are socially defined by mutual disclosure and communication among the customer and the sales agent.

(iii) Users' cognitive load for managing privacy boundary control can be reduced by a systematic support. According to the difference between $v\uparrow$ and $v'\downarrow$, the system can automatically select either full or expedited information disclosure process based on a predefined threshold value. In addition, *view* templates in the privacy knowledge database can be used to help users define view objects.

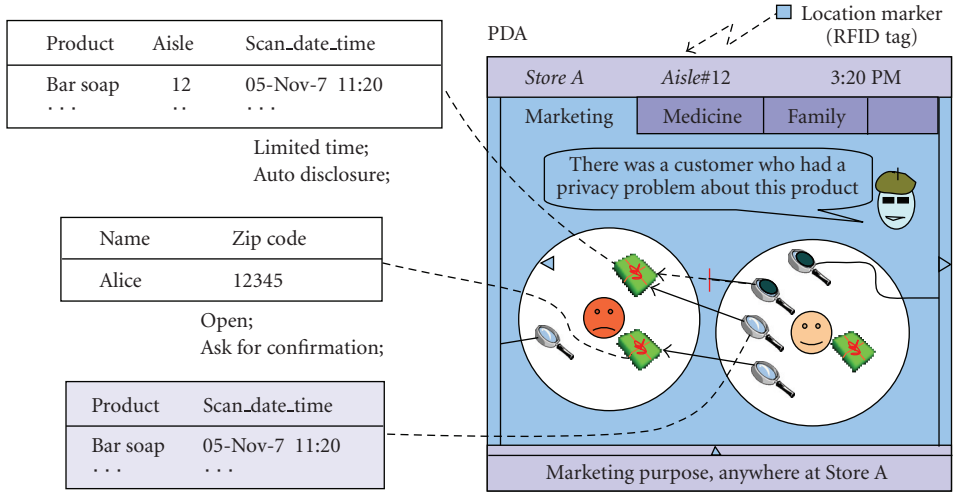


Figure 5: A user interface mock-up.

3.8. User Interface. A key challenge in designing the user interface for boundary control is the minimization of a user's cognitive burden. Boundary regulation for RFID tags can be a complex task if users must process a variety of feedback and control. Also, the task of managing boundaries may interfere with other important tasks that the user may need to attend to. However, a simplified user interface for a complex boundary management may remove details that some users consider important.

Using the proposed mechanisms, the proposed user interface design aims at allowing users to see how their information is being viewed by others and to socially negotiate privacy boundaries. Additionally, *critics* [61–63]—intelligent agents to reduce cognitive load required for boundary regulation—were incorporated.

Figure 5 shows a user interface mock-up that demonstrates the design features. Imagine a scenario where a customer uses a PDA that is equipped with an RFID reader to scan sales items and key locations in a store (i.e., aisle numbers). Such technology-rich "future store" environments are being deployed in the real world [64]. Note that other location technologies can be used for sensing the locations of customers. In Figure 5, the PDA shows the customer's location ("*Store A*" and "*Aisle#12*") and the current time ("*3:20 PM*"). Below the location information are three *context tabs*, each labeled "*Marketing*," "*Medicine*," and "*Family*." Each context tab corresponds to a group of equivalent context objects that are related to the current location and time. The area near the bottom of the PDA screen, showing text "*Marketing purpose, anywhere at Store A*," can be expanded to show detailed information about the currently selected context tab.

The left facial icon represents the customer and the right icon a sales agent. Another facial icon in the upper area of the screen is a *critic* agent that provides suggestions relevant to the current context objects. The customer can tap on the sales agent's icon to call the sales agent using a VoIP (Voice over Internet Protocol) application or send a short text message. The customer can select one of several emoticons that represent different emotional states. These emoticons are not representations of privacy preferences but a communication tool to convey subtle feelings about information disclosure.

Other icons look like magnifying lenses and gift boxes. Magnifying lenses represent *input views* and gift boxes *output views*. Tapping on a gift box icon brings up a window showing the definition and contents of a corresponding output view. The customer explicitly discloses product names, aisle numbers, and date/time of scans as well as a name and a zip code. End-users may create or modify *views* by simply selecting attribute names. Tapping a magnifying lens displays a window showing the definition and the contents of a corresponding *input view*. The customer can also be assured that only a portion of the disclosed information can be viewed by a sales agent. Black magnifying lenses indicate blocked *input views*: they are defined but not viewable by a sales agent. The customer can select multiple icons to review combined *views* or examine *view* differences. When the customer's icons are tapped by others, the icons will be highlighted on the customer's PDA. Corresponding *input/output views* are indicated by arrows. Arrows with dotted lines indicate conflicts between corresponding views. Also, users can attach personal and shared annotations to icons and arrows. The proposed user interface can automatically select a different privacy preference according to context, thereby making expedited processes feasible when users have different privacy needs in different contexts. It also facilitates dynamic control over information disclosure using abstract visual representations. Moreover, *critic* agents can alert users if they may have to manually adjust their privacy boundaries.

4. Discussion and Conclusion

We believe it is necessary to iteratively extend, improve and assess the *QueryLens* system based on the proposed framework. It is still challenging to evaluate the proposed framework in a naturalistic setting because of the lack of

inexpensive mobile RFID platforms that allows for large-scale field tests. Such a platform (e.g., NFC-enabled mobile phones) may be available in the near future. To cope with this challenge, different evaluation methods were combined using a PC-based mockup as well as a mobile phone-based prototype before possibly conducting a full-scale experiment using RFID-enabled phones. The proposed framework is not for ensuring a static goal that can be clearly defined in advance, but for creating an environment in which users continuously define and adjust the configuration to suit their dynamic needs. This orientation towards *design-in-use* is in line with end-user development (EUD) and Meta Design [65].

When a massive amount of RFID tags are used in the everyday world, it can be very difficult for users to control the information triggered by RFID tags. One of the challenges is to support users' simultaneous need for publicity and privacy in such environments. In order to provide such support, an RFID-triggered information sharing system was developed and tested. Then, a framework for supporting boundary control was developed based on initial testing experiences with the system.

The experiences involved with developing and evaluating the *QueryLens* system were revealing in terms of richness of design spaces as well as the challenges and promises of creating usable and useful services by exploiting inexpensive, ubiquitous RFID tags. Moreover, the *QueryLens* study maintained that (a) social contexts are important and (b) there are inescapable privacy issues that could seriously undermine usability and usefulness of RFID systems. In order to support users to control their information flows, this study proposed contextual information models and *views* for privacy-sensitive data, as well as described how the models can support users to control their boundaries that regulate information flows. The models were utilized to realize a user interface that integrates social networks and information flows using *input*/*output views*, context tabs, *critic* agents, and so on.

Although this study focused on RFID-triggered information sharing, implications exist for other related systems and applications. Context-aware information sharing systems that use barcodes, infrared beacons, or GPS share certain properties with the RFID-triggered information systems that we have investigated. The framework in this study is meant to serve as a starting point for further investigations on technological and social issues based around RFID-triggered information sharing. This study was conducted in effort to stimulate and facilitate the development of novel collaborative applications of "smart physical objects," which respect and balance people's various needs.

References

[1] L. Palen, M. Salzman, and E. Youngs, "Going wireless: behavior & practice of new mobile phone users," in *Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW '00)*, pp. 201–210, Philadelphia, Pa, USA, 2000.

[2] R. Want, K. P. Fishkin, A. Gujar, and B. L. Harrison, "Bridging physical and virtual worlds with electronic tags," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '99)*, pp. 370–377, 1999.

[3] Mobile Marketing Data Labo, "The 3rd Research on the Uses of Mobile Contents," 2007, http://mmd.up-date.ne.jp/news/detail.php?news_id=100.

[4] Amazon, Amazon ScanSearch, 2005, http://www.amazon.co.jp/exec/obidos/tg/feature/-/546374/ref=gw_lp_ct_4_1/250-0440035-9265812.

[5] NFC, "NFC Forum," 2006, http://www.nfc-forum.org/home.

[6] P. Kourouthanassis and G. Roussos, "Developing consumer-friendly pervasive retail systems," *IEEE Pervasive Computing*, vol. 2, no. 2, pp. 32–39, 2003.

[7] A. Gilbert, "Cutting-edge 'smart shelf' test ends," http://news.cnet.com/2100-1008_3-5067253.html.

[8] G. Borriello, "Introduction," *Communications of the ACM*, vol. 48, no. 9, pp. 34–37, 2005.

[9] S. Garfinkel and B. Rosenberg, *RFID: Applications, Security, and Privacy*, Addison-Wesley, New York, NY, USA, 2005.

[10] B. Nath, F. Reynolds, and R. Want, Eds., "Special issue on RFID technology and applications," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 22–24, 2006.

[11] S. Konomi and G. Roussos, "Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments," *Personal and Ubiquitous Computing*, vol. 11, no. 7, pp. 507–521, 2007.

[12] S. Sackmann, J. Strüker, and R. Accorsi, "Personalization in privacy-aware highly dynamic systems," *Communications of the ACM*, vol. 49, no. 9, pp. 32–38, 2006.

[13] I. Altman, *The Environment and Social Behavior*, Brooks/Cole, Monterey, Calif, USA, 1975.

[14] L. Palen and P. Dourish, "Unpacking "privacy" for a networked world," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI '03)*, pp. 129–136, ACM Press, 2003.

[15] P. Dourish and K. Anderson, "Collective information practice: exploring privacy and security as social and cultural phenomena," in *Human-Computer Interaction*, vol. 21, pp. 319–342, Lawrence Erlbaum Associates, Mahwah, NJ, USA, 2006.

[16] S. Konomi, "QueryLens: beyond ID-based information access," in *Proceedings of the 4th International Conference on Ubiquitous Computing (Ubicomp '02)*, pp. 210–218, Springer, 2002.

[17] S. Konomi, "Snap-on filter for mobile information appliances," in *Proceedings of the 5th Asia Pacific Conference on Computer-Human Interaction (APCHI '02)*, pp. 357–368, Science Press, 2002.

[18] C. S. Nam and S. Konomi, "Usability evaluation of *QueryLens*: implications for context-aware information sharing using RFID," in *Proceedings of the IASTED International Conference on Human-Computer Interaction (IASTED-HCI '05)*, pp. 90–95, Phoenix, Ariz, USA, 2005.

[19] T. Kindberg, J. Barton, J. Morgan, et al., "People, places, things: Web presence for the real world," in *Proceedings of the 3rd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*, ACM Press, 2002.

[20] P. Ljungstrand, J. Redstrom, and L. E. Holmquist, "Web-Stickers: using physical tokens to access, manage and share bookmarks to the Web," in *Proceedings of the Designing Augmented Reality Environments*, 2000.

[21] J. S. Olson, J. Grudin, and E. Horvitz, "A study of preferences for sharing and privacy," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI '05)*, pp. 1985–1988, ACM Press, 2005.

[22] J. Burrell, G. K. Gay, K. Kubo, and N. Farina, "Context-aware computing: a test case," in *Proceedings of the 4th International Conference on Ubiquitous Computing (Ubicomp '02)*, pp. 1–16, 2002.

[23] F. Espinoza, P. Persson, A. Sandin, H. Nyström, E. Cacciatore, and M. Bylund, "GeoNotes: social and navigational aspects of location-based information systems," in *Proceedings of the International Conference on Ubiquitous Computing (Ubicomp '01)*, pp. 2–17, Springer, 2001.

[24] I. Smith, S. Consolvo, A. Lamarca, et al., "Social disclosure of place: from location technology to communication practices," in *Proceedings of the 3rd International Conference on Pervasive Computing (Pervasive '05)*, pp. 134–151, Springer, Heidelberg, Germany, 2005.

[25] A. J. B. Brush, T. C. Turner, M. A. Smith, and N. Gupta, "Scanning objects in the wild: assessing an object triggered information system," in *Proceedings of the 7th International Conference on Ubiquitous Computing (Ubicomp '05)*, pp. 305–322, 2005.

[26] A. Fletcher, "Two sides of RFID," 2004, European Edition, http://www.foodproductiondaily.com/.

[27] D. Wan, "Magic medicine cabinet: a situated portal for consumer healthcare," in *Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing (HUC '99)*, pp. 27–29, 1999.

[28] L. Palan and S. Aaløkke, "Of pill boxes and piano benches: "home-made" methods for managing medication," in *Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work (CSCW '06)*, pp. 79–88, 2006.

[29] EPCglobal, "Guidelines on EPC for Consumer Products," 2005, http://www.epcglobalinc.org/public/ppsc_guide.

[30] A. F. Westin, *Privacy and Freedom*, Atheneum, New York, NY, USA, 1967.

[31] X. Jiang and J. A. Landay, "Modeling privacy control in context-aware systems," *IEEE Pervasive Computing*, vol. 1, no. 3, pp. 59–63, 2002.

[32] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "The evolution of RFID security," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 62–69, 2006.

[33] S. Inoue, S. Konomi, and H. Yasuura, "Privacy in digitally named world with RFID tags," in *Proceedings of the International Workshop on Social-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing*, 2002.

[34] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS '03)*, pp. 103–111, ACM Press, 2003.

[35] T. Kriplean, E. Welbourne, N. Khoussainova, et al., "Physical access control for captured RFID data," *IEEE Pervasive Computing*, vol. 6, no. 4, pp. 48–55, 2007.

[36] V. Rastogi, E. Welbourne, N. Khoussainova, et al., "Expressing privacy policies using authorization views," in *Proceedings of the International Workshop on Privacy in UbiComp (UbiPriv '07)*, pp. 531–542, 2007.

[37] V. Rastogi, D. Suciu, and E. Welbourne, "Access control over uncertain data," in *Proceedings of the 34th International Conference on Very Large Data Bases (VLDB '08)*, pp. 821–832, 2008.

[38] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[39] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and supression," *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems*, vol. 10, no. 5, pp. 571–588, 2002.

[40] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: privacy beyond k-anonymity," in *Proceedings of the 22nd International Conference on Data Engineering (ICDE '06)*, p. 24, 2006.

[41] B. C. M. Fung, M. Cao, B. C. Desai, and H. Xu, "Privacy protection for RFID data," in *Proceedings of the 24th ACM Symposium on Applied Computing (SAC '09)*, pp. 1528–1535, Honolulu, Hawaii, USA, 2009.

[42] O. Abul, F. Bonchi, and M. Nanni, "Never walk alone: uncertainty for anonymity in moving objects databases," in *Proceedings of the 24th International Conference on Data Engineering (ICDE '08)*, pp. 376–385, 2008.

[43] A. Acquisti, "Protecting privacy with economics: economic incentives for preventive technologies in ubiquitous computing environments," in *Proceedings of the International Workshop on Socially-Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing*, 2002.

[44] J. I. Hong and J. A. Landay, "An architecture for privacy-sensitive ubiquitous computing," in *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services (MobiSys '04)*, pp. 177–189, ACM Press, Boston, Mass, USA, 2004.

[45] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS '04)*, pp. 91–100, ACM Press, Cambridge, Mass, USA, 2004.

[46] C. Floerkemeier, R. Schneider, and M. Langheinrich, "Scanning with a purpose—supporting the fair information principles in RFID protocols," in *Proceedings of the 2nd International Symposium on Ubiquitous Computing Systems (UCS '04)*, pp. 214–231, 2004.

[47] B. A. Price, K. Adam, and B. Nuseibeh, "Keeping ubiquitous computing to yourself: a practical model for user control of privacy," *International Journal of Human Computer Studies*, vol. 63, no. 1-2, pp. 228–253, 2005.

[48] S. Lederer, J. I. Hong, A. K. Dey, and J. A. Landay, "Personal privacy through understanding and action: five pitfalls for designers," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 440–454, 2004.

[49] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *Proceedings of the 3rd European Conference on Computer-Supported Cooperative Work (ECSCW '93)*, pp. 77–92, Kluwer Academic Publishers, 1993.

[50] M. Weiser and J. S. Brown, "Designing calm technology," *PowerGrid Journal*, vol. 1, no. 1, 1996.

[51] P. Dourish, "What we talk about when we talk about context," *Personal and Ubiquitous Computing*, vol. 8, no. 1, pp. 19–30, 2006.

[52] S. Konomi and C. S. Nam, "Using context for privacy boundary control in RFID applications," in *Proceedings of the IASTED International Conference on Human-Computer Interaction (IASTED-HCI '05)*, pp. 252–257, Acta Press, Phoenix, Ariz, USA, 2005.

[53] S. Konomi, "Personal privacy assistants for RFID users," in *Proceedings of the International Workshop Series on RFID—Information Sharing and Privacy*, Tokyo, Japan, November-December 2004.

[54] J. Grudin and E. Horvitz, "Presenting choices in context: approaches to information sharing," in *Proceedings of the*

International Workshop on Ubicomp Communities: Privacy as Boundary Negotiation, 2003.

[55] T. P. Moran and P. Dourish, "Introduction to this special issue on context-aware computing," *Human-Computer Interaction*, vol. 16, no. 2, pp. 87–95, 2001.

[56] P. Samarati, "Protecting respondents' identities in microdata release," *IEEE Transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010–1027, 2001.

[57] Spychip.com, "Scandal: Walmart, P&G, Involved in Secret RFID Testing," 2003, http://www.spychips.com/press-releases/broken-arrow.html.

[58] B. G. Claybrook, "Using views in a multilevel secure database management system," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 4–17, IEEE Computer Society, 1983.

[59] D. E. Denning, S. G. Akl, M. Heckman, et al., "Views for multilevel database security," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 129–140, 1987.

[60] G. Aggarwal, M. Bawa, P. Ganesan, et al., "Vision paper: enabling privacy for the paranoids," in *Proceedings of the 13th International Conference on Very Large Data Bases*, pp. 708–719, Morgan Kaufmann, 2004.

[61] G. Fischer, A. C. Lemke, and T. Mastaglio, "Using critics to empower users," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '90)*, pp. 337–347, ACM Press, 1990.

[62] G. Fischer, K. Nakakoji, J. Ostwald, G. Stahl, and T. Sumner, "Embedding computer-based critics in the contexts of design," in *Proceedings of the Conference on Human Factors in Computing Systems (INTERCHI '93)*, pp. 157–164, ACM Press, 1993.

[63] M. S. Ackerman and L. Cranor, "Privacy critics: UI components to safeguard users' privacy," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '99)*, pp. 258–259, ACM Press, Pittsburgh, Pa, USA, 1999.

[64] MetroGroup, "Metro Group Future Store Initiative," July 2006, http://www.future-store.org/fsi-internet/html/de/375/index.html.

[65] G. Fischer, E. Giaccardi, Y. Ye, A. G. Sutcliffe, and N. Mehandjiev, "Meta-design: a manifesto for end-user development," *Communications of the ACM*, vol. 47, no. 9, pp. 33–37, 2004.