IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12703

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Consideration of Privacy Protection for Ubiquitous Applications through an Interdisciplinary Approach

Kunihiko Kido, Hitachi, Ltd., Systems Development Laboratory, 292, Yosida-cho, Totsuka-ku, Yokohama, 244-0817, Japan, kido@sdl.hitachi.co.jp, Phone: +81-45-860-2427, Fax: +81-45-860-2425

Satoshi Yasiro, Hitachi, Ltd., Systems Development Laboratory, 292, Yosida-cho, Totsuka-ku, Yokohama, 244-0817, Japan, yasiro@sdl.hitachi.co.jp, Phone: +81-45-860-2428, Fax: +81-45-860-1675

ABSTRACT

Ubiquitous technologies will provide rich services to consumers and citizens. However, ubiquitous applications will raise serious privacy protection issues since ubiquitous devices will be embedded so pervasively everywhere and in countless objects and devices. Most notably there are some ubiquitous applications in which it is technically difficult to implement the self-information control required by law or privacy protection guidelines. Because there is no one perfect technological solution, it is necessary to investigate a full range of countermeasures in terms of legal remedies and security technologies through an interdisciplinary approach. In this paper, we investigate privacy protection issues for ubiquitous applications. We specifically try to clarify privacy protection issues surrounding RFID applications in terms of legal remedies and security technologies.

INTRODUCTION

Historically, the right to privacy was conceived as a passive right, the "right to be let alone." However, with the advent of the information age, it has become increasingly difficult to sufficiently protect the right to privacy based on such a passive right. Consequently, the privacy right has come to be understood more positively as "the right to self-information control," a concept that has now emerged as the most influential privacy right in the world [1].

In the field of ubiquitous computing, a number of studies have addressed the security functions required by "the right to self-information control" [2]. However, as we will show in Chapter 2, there are some ubiquitous applications where it is difficult to strictly implement the security functions required by "the right to self-information control."

This being the case, it is essential to investigate a full range of countermeasures to protect privacy in terms of legal remedies and security technologies. In this paper, we adopt an interdisciplinary approach to analyze issues of privacy protections in ubiquitous applications.

First, we propose an analytic framework for assessing privacy issues in terms of legal remedies and security technologies. Second, we clarify issues of privacy protections in RFID applications, based on the proposed framework and social cost analysis of security countermeasures. Finally, we clarify a number of issues relating to the Japanese Personal Information Protection Act.

ANALYTIC FRAMEWORK FOR ASSESSING PRIVACY ISSUES

In this chapter, we present an analytic framework for assessing privacy issues. Figure 1 shows the interdependence between privacy related entities. This framework can be used to identify weak points with respect to privacy protection for ubiquitous applications. More specifically, we will use the framework to identify situations in which a consumer's privacy cannot be adequately protected by current technological countermeasures and legal remedies.

LEGAL REMEDIES

In Japan, the Personal Information Protection Act was enacted in 2003 and went into effect in April 2005. As the name of the act suggests, this is a basic law dealing with the protection of personal information. Personal information is data pertaining to real people that can be used to identify specific person: names, numbers assigned to individuals, and so on [1].

When companies handle personal information, they are now obligated to implement the measures required by the Japanese Personal Information Protection Act. If the measures are not properly or sufficiently implemented, the authorities can insist that the measures are strengthened or improved.

Meanwhile, there are other kinds of information that, although they do not identify a specific individual, nevertheless reveal much about generic consumer behavior. For example, by tracing a unique ID code written into an RFID tag that is embedded in clothing or other commodities, companies can monitor a consumer's behavior in public spaces. The ID code or consumer behavior tracked by the ID code does not identify a specific individual, so it is not personal information per se. However, if RFID tags are embedded in consumers' clothing or books, companies can learn much about the consumer's clothing size and about his or her individual reading habits. This kind of information is classified as non-personal privacy information and does not come under the purview of the Japanese Personal Information Protection Act. In Japan, non-personal privacy information is protected by civil law. If someone felt their privacy was being invaded by this kind of non-specific information gathering, he would have to bring the case himself and claim compensation for damages as a civil lawsuit.

CONSUMER RIGHTS

The Japanese Personal Information Protection Act is based on OECD guidelines. These guidelines adopt the concept of "The right to self-information control." Under the Japanese Personal Information Protection Act, consumers must be notified in advance based on Principle 1 "Collection Limitation" before their personal information can be used. Based on this same collection limitation principle, consumers must give their consent before sensitive personal information can be gathered and used. Note the distinction: *consumer notification* means that consumers should be notified that their personal information is being collected and used, while *consumer consent* means that personal information can only be collected with the consent of the information

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Figure 1. Analytic framework for assessing privacy issues

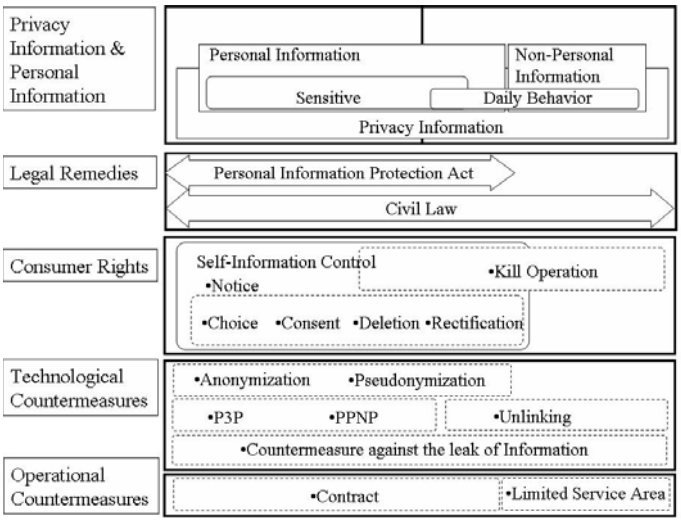
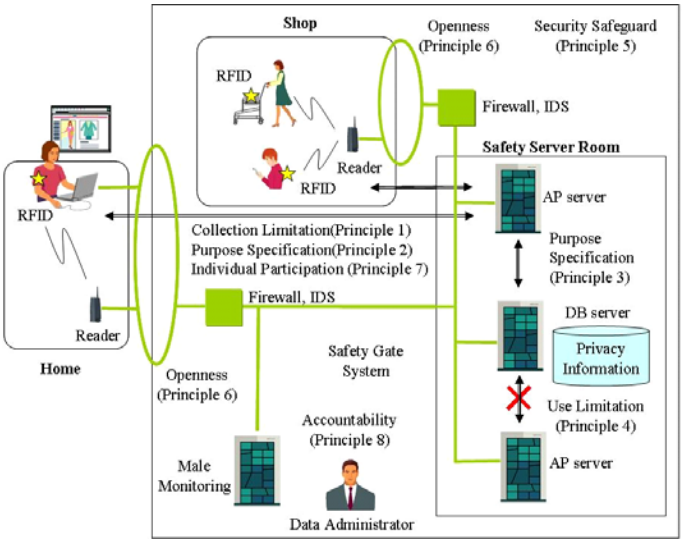


Figure 2. System model based on the OECD guidelines



subject. Once consumers are notified and provided with the address of the company collecting the information, they can request that the company erase or correct their personal information.

We will now turn our attention to RFID applications in which information pertaining to consumer behavior can be collected. When consumers use mobile devices, the mobile can be notified of the presence of RFID readers. However, in the case of passive RFID tags which respond automatically to censoring signals, it is difficult to obtain consumer's consent before the ID code is transmitted. Consumers must therefore be provided with some means that they can deactivate the RFID tag function by themselves [3][4].

TECHNOLOGICAL AND OPERATIONAL COUNTERMEASURES

In this section, we will survey the technological or operational countermeasures corresponding to legal remedies and consumer rights, based on the system model shown in Figure 2 corresponding to the

OECE Guidelines. To support Principle 5 "Security Safeguard," secure management over privacy information databases and other devices is required to prevent the leakage of information. On the other hand, implementing consumer notification and consent capabilities are needed to support Principle 1 "Collection Limitation," Principle 7 "Individual Participation," and Principle 6 "Openness." A number of self-information control technologies are available including P3P (Platform for Privacy Preferences) [5] and PPNP (Privacy Profile Negotiation Protocol) [6]. Essentially these technologies provide the functionality to control the level of personal consumer information that is disclosed based on relevant privacy protection policies.

"Anonymization" or "Pseudonymization" methods can be used to transform personal information into non-personal privacy information. While these methods are regarded as self-information control techniques, pseudonymized personal information should nevertheless be carefully managed since it does involve privacy information.

In the case of passive RFID tags, it is difficult for consumers to control the flow of ID codes. This calls for the implementation of operational countermeasures so that consumers can easily identify the presence of RFID readers. For instance, companies should publicly disclose places in which RFID readers are installed as part of their advertising in the areas where they market their products or on their web pages. If companies could enter into a contractual arrangement with consumers before providing their services, the consumers should be alerted to the presence of RFID readers such as with a map revealing the locations of RFID readers.

To prevent monitoring consumer behavior, "unlinking techniques" are available. One such method is the variable secret ID method [7] in which the ID code in an RFID tag is periodically replaced. Note however that the vulnerability to privacy violation increases as the ID code replacement interval lengthens.

PRIVACY ISSUES FOR UBIQUITOUS APPLICATIONS

In this chapter, we will attempt to identify events or situations that are not protected under current legal remedies and technical countermeasures by checking RFID applications against the analytic framework. Figure 3 illustrates the procedure.

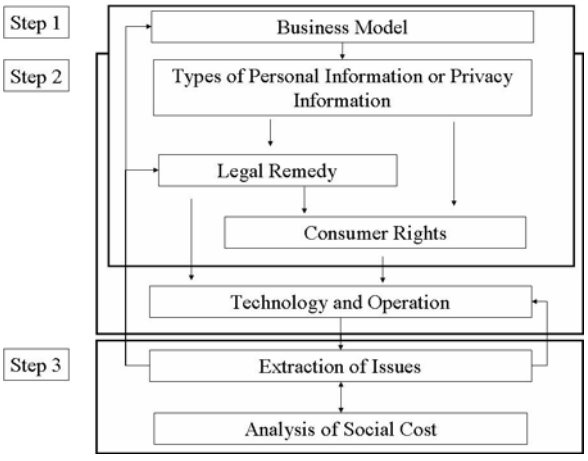
PRIVACY INFORMATION AND CONSUMER RIGHTS

Here we will consider three typical RFID applications. In Step 1 of Figure 3, we will specify the type of privacy information and consumer rights that are involved.

(1) Information Services

Companies can derive a wealth of information about commodities based on RFID tags embedded in the commodities. In this service, the ID codes transmitted from RFID tags are deleted immediately, so consumer notification and consent are not required.

Figure 3. Procedure of analysis based on analytic framework



Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

(2) Marketing Analysis
In this service, consumer information based on ID codes collected from RFID tags is stored in a personal information database, and the information is used to analyze consumer behavior and preferences. In this case, if specific individuals cannot be identified by the information, consumer notification and consent is not always required. Note that this assumes that the information is treated strictly as non-personal privacy information. To the extent possible, it is desirable that companies obtain the consent of consumers before collecting ID codes.

(3) Customer Relationship Management (CRM)
In this case, companies deliberately correlate ID codes in RFID tags to individuals' personal information for the purpose of conducting "one-to-one marketing." The ID code connected with personal information is regarded as personal information as defined by the Personal Information Protection Act, so consumers should be notified and if possible consent obtained before collecting the information.

PRIVACY ISSUES IN TERMS OF SECURITY TECHNOLOGIES
In Step 2 of Figure 3, we consider the ability of current technological and operational countermeasures to protect consumer rights. First we would observe that in all cases, robust security to safeguard privacy information databases must be in place to prevent the leakage of personal information.

In the case of (3) Customer Relationship Management, since personal information is involved, consumer notification and consent is required by the Personal Information Protection Act. If the service is based on a contract, the company can explain the purpose of the data collection to consumers in the contract document. If the service is not based on a contract, the company should provide the functions of consumer notification and consent on their mobile terminals. But as we observed earlier, it is technically difficult in the case of RFID tags to control the flow of the ID codes. In this case, information should only be collected in limited service areas, and consumers in those areas should be clearly informed about the purpose of the data collection through advertising in the service areas.

Turning to (2) Marketing Analysis, since non-personal privacy information is involved, consumer notification and consent is not always required. And again, in the case of passive RFID tags, it is difficult for consumers to control the flow of ID codes in RFID tags which have not been deactivated. Given this business model, consumer privacy could be readily and frequently violated under current technological countermeasures and legal remedies.

In the next chapter, we will address some of the issues involved in protecting non-personal privacy information, as highlighted in (2) Marketing Analysis. Considering that non-personal privacy information is protected by civil law, in Step 3 of Figure 2 we conduct the social cost analysis to investigate the relationship between compensation for information leakage and the level of security countermeasures.

ANALYSIS OF PRIVACY PROTECTION THROUGH SOCIAL COST ANALYSIS

Economics of Law
We have underscored the difficulty of fully implementing self-information control where passive RFID tags are involved. This means that companies must take responsibility for protecting individuals' information in their personal information databases. Currently there are no standard guidelines for safeguarding personal information databases, so companies must determine the level of security countermeasures needed to protect personal information databases by themselves. In this section, we will consider the approximate costs of different security measures provided by companies based on social cost analysis.

Let us first briefly consider how social cost calculations are done in case of Internet services such as shown in Figure 2.

Let D(x) be the expected loss resulting from the leakage of information. Here, x represents the cost of preventing the leakage. Let t be the countermeasures implemented by a company. Then, x is expressed as follows:

$$x = x(t) \tag{1}$$

Let P(t) be the probability of information leakage under security countermeasures t. The probability P(t) of information leakage decreases as countermeasures t is enhanced.

Now let C be the compensation for damages, M the temporal damages, cc the cost to the consumer to bring a lawsuit, ce the cost to the company resulting from the lawsuit, and m the number of service members. The expected loss is expressed as follows:

$$D(x(t))=P(t)\ [n(C+\ cc)+mM+ce] \tag{2}$$

Assuming an economic rationalistic response, a company selects x that minimizes the social cost of the following equation [8]:

$$\min_x [x + D(x)\ ] \tag{3}$$

Let x* be the cost that satisfies Equation (3). According to prevailing the tort liability laws [8], more than cost x* is required to implement security countermeasures to prevent information leakage.

SOCIAL COSTS OF RFID APPLICATIONS
In the case of Internet services, the flow of personal information can be controlled using technologies such as P3P and PPNP. But because consumers cannot control the functions of passive RFID tags, ID codes are transmitted automatically. Here, let k be the number of non-members whose ID codes are collected. Then, the socially optimal level t of security countermeasures satisfies the following equation:

$$\min_x [x + P(t)\ [(n+n')(C+ c_c)+(m+k)M+c_e]\ ] \tag{4}$$

But if the ID codes are not connected with personal information, companies cannot identify the consumers behind the ID codes. Thus, k in Equation (4) is nearly equal to 0. Note too that in the event information leakage does occurs, consumers are generally unaware that they have been victimized because they don't know that their ID codes are being collected. Thus, the number n' of consumers actually bringing a lawsuit is nearly equal to 0. Thus, although an additional cost corresponding to $n'(C+ c_c)+kM$ should be required, companies typically adopt the security countermeasure t which satisfies the Equations (2) and (3).

N EXAMPLE OF SOCIAL COST CALCULATION
In this section, we will consider an example of social cost calculation. Let us assume a small company with five retail stores. Here we assume a total workforce for the five stores of 500 employees, 50 of whom security clearance access secure customer information. We further assume 50 external attacks are made on the company's computer system in an effort to illegally acquire personal information every year. The probability P(t) of information leakage was calculated from the fault tree shown in Figure 4 [9].

$$P(t)=50\times PT1(t)+450\times PT2(t)+50\times PT3(t) \tag{5}$$

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Table 1. Various countermeasures

Countermeasure	Cost (Yen/year)
1) e-Mail Monitoring	2 million
2) Firewall	1 million
3) Intrusion Detection System	5 million
4) Countermeasures against Server Vulnerability	1 million
5) Copy Restriction of Data within Safety Areas	0.5 million
6) Safety Gate System	3 million
7) Body Search	5 million
8) Security Education	2 million

$$PT1(t)\bullet\ P1(1-X8\,\Delta X18)(P2(1-X7(1-P3))(1-X5(1-P4)) +P5(1-X1(1-P6))+P7(1-X2(1-P8))) \quad (6)$$

$$PT2(t)\bullet\ (1-X8\,\Delta X28)P9P21(P10(1-X5(1-P11))(1-X7(1-P12))+P13(1-X1(1-P14)) +P15(1-X2(1-P16)))+(1-X8\Delta X28)P17(1-X3(1-P18))(1-X2(1-P19))(1-X4(1-P20)) \quad (7)$$

$$PT3(t)\bullet\ P22(1-X6(1-P23))P24(1-X5(1-P25))(1-X7(1-P26)) +P27(1-X4(1-P28))(1-X3(1-P29))(1-X2(1-P30)) \quad (8)$$

Here, when Xj is equal to 1, the countermeasure j shown in Table 1 is implemented. When Xj is equal to 0, the countermeasure j shown in Table 1 is not implemented.

The probability P1~P30 of events or incidents shown in Figure 4 were set as follows:

P1=0.05, P2=0.01, P3=0.2, P4=0.2, P5=0.01, P6=0.2, P7=0.04 P8=0.2, CP9=0.01, CP10=0.01, CP11=0.2, CP12=0.2, CP13=0.05, P14=0.2, P15=0.04, P16=0.2, P17=0.0001, P18=0.3, P19=0.2, P20=0.2, P21=0.2, P22=0.04, CP23=0.1, CP24=0.01, CP25=0.1, CP26=0.2, CP27=0.0004, CP28=0.1, P29=0.3, P30=0.2

Moreover, the effects $\Delta X18$ and $\Delta X28$ of security education were set to 0.3. Actually, the probability of events or incidents and the effect of security education will vary depending the expertise of the company's security expert. However, since the purpose of this analysis is to investigate the relationship between compensation for information leakage and the level of security countermeasures through a rough assessment of social costs, we have arbitrarily set the probability and the effect of security education at 0.3.

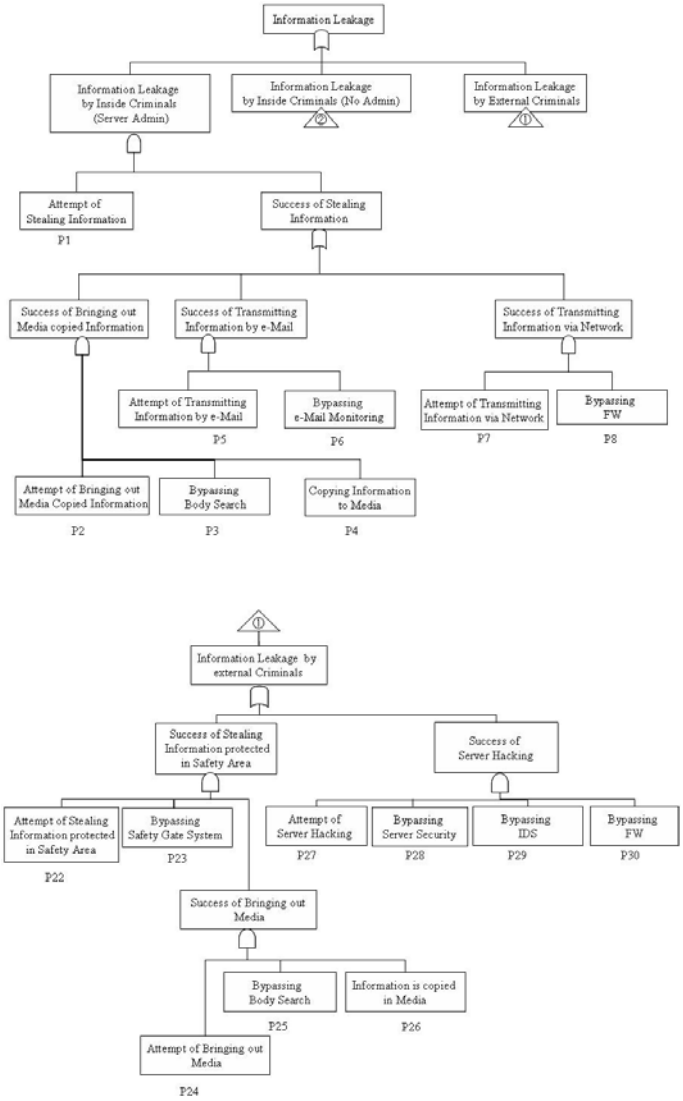
RESULTS

Parameters for the social cost calculation were set as follows [10]:

- Compensation for damages: C = \10,000
- Number of members: m=10,000
- Number of plaintiffs: n+n'=0.0001×m
- Temporal damages: M=\500
- Company's cost of lawsuit: ce=\50,000,000
- Consumer's cost of lawsuit: cc=\100,000

The number k of non-members in the database is from 0 to 150,000. For each k, the combination t = [Xj] of countermeasures that satisfies Equation (4) was searched.

Figure 4. Fault Tree analysis



(1) k = 0 (No RFID services)

P(t) = 0.1123, Optimal countermeasure t = [11001001], Cost of the Countermeasure=4.5 million

(2) k =20,000 person

P(t) = 0.0583, Optimal countermeasure t = [11001101], Cost of the Countermeasure =7.5 million

(3) k =140,000 person

P(t) = 0.04966, Optimal countermeasure t = [11011101], Cost of the Countermeasure =8.5 million

The socially optimal level of security countermeasures against information leakage increased at k=20,000 and k=140,000. The optimal level did not change for the range from k=20,000 to k=130,000.

This is because, for k=20,000^ÿ130,000, the additional cost of additional countermeasures surpasses the reduction in D(x). The results reveal that companies with a large number of members have already achieved the socially optimal level of security countermeasures against information leakage.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

IMPLICATIONS

Our findings reveal that for companies with a large number of members, the companies have already implemented security countermeasures at the level of Equation (4). But companies with a small number of members should enhance the level of countermeasures against information leakage corresponding to the amount of non-personal information they have stored on their personal information databases.

Companies that are unable or unwilling to implement additional countermeasures should adopt the following measures:

Measure 1: ID codes collected from RFID tags and related data should be deleted after a certain period.

As observed earlier in Section 2, the protection of non-personal privacy information is not covered by the Japanese Privacy Information Protection Act. We also noted that if companies do not voluntarily disclose where RFID readers are installed, customers really have no way of knowing that RFID readers even exist. As noted in Section 4, his situation can cause companies to underinvest in security countermeasures to protect non-personal privacy information. And once consumer behavioral data associated with a unique ID code is leaked from personal information database, there is the potential danger for that data to be acquired and abused by criminals. This suggests that the Japanese government should modify the Personal Information Protection Act to encourage a second measure:

Measure 2: The location of RFID readers and why data is being collected should be clearly and publicly displayed on company web sites.

If this additional Measure 2 was implemented, then consumers would at least be able to figure out the likely source of the leak.

CONCLUSIONS

In this study we adopted an interdisciplinary approach to investigate privacy protection for ubiquitous applications. We surveyed the range of countermeasures for RFID applications in terms of legal remedies and security technologies. This same approach could be used to examine other ubiquitous applications such as sensor networks based on the analytic framework for assessing privacy issues shown in Figure 1.

NOTE

This research was supported as a leading research project with special coordination funds for promoting science and technology by the Ministry of Education, Culture, Sports, Science and Technology.

REFERENCES

[1] M. Horibe (Editor), Masaasa Suzuki: Personal Information Protection Act and Compliance Programs, Shouji Houmu (2004) (in Japanese).
[2] M. Langheinrich, “A Privacy Awareness Systems for Ubiquitous Computing Environments”, UbiComp 2002, (2002).
[3] CASPIAN, Position Statement on the Use of RFID on Consumer Products (Nov.14 2003) .
[4] EPCGlobal, Guideline on EPC for Consumer Products. http://www.epcglobaleinc.org/public_policy/public_policy_guideline.html
[5] http://www.w3.org/P3P/
[6] S. Tamaru, J. Nakazawa, K. Takashio, and H. Tokuda: PPNP: A Privacy Profile Negotiation Protocol for Services in Public Spaces, Fifth International Conference on Ubiquitous Computing(UbiComp2003), First International Workshop on Ubiquitous Systems for Supporting Social Interaction and Face-to-Face Communication in Public Spaces, (2003).
[7] S. Kinosita, F. Hosino, T. Komuro, A. Fujimura, and M. Okubo: Low-cost RFID Privacy Protection Scheme, IPSJ Journal, Vol.45, No8, pp.2007-2021 (2004) (in Japanese).
[8] T.J. Miceli: Economics of the Law Oxford University Press (1997).
[9] Y. Hidaka, M. Isii, and R. Sasaki: Multi-Risk Communicator and Trail Test, SCIS2005 (2005) (in Japanese).
[10] NPO Japan Security Network Association: Research Report on Information Security Incidents (Part II) in 2003 fiscal year, http://www.jnsa.rog/active2003_la.html (2003) (in Japanese).

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/proceeding-paper/consideration-privacy-protection-ubiquitous-applications/32729

Related Content

Application of Improved Sparrow Search Algorithm in Electric Battery Swapping Station Switching Dispatching
Qingsheng Shiand Feifan Zhao (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-21).*
www.irma-international.org/article/application-of-improved-sparrow-search-algorithm-in-electric-battery-swapping-station-switching-dispatching/330421

Human-Agent-Robot Teamwork (HART) Over FiWi-Based Tactile Internet Infrastructures
Mahfuzulhoq Chowdhuryand Martin Maier (2021). *Encyclopedia of Information Science and Technology, Fifth Edition (pp. 27-41).*
www.irma-international.org/chapter/human-agent-robot-teamwork-hart-over-fiwi-based-tactile-internet-infrastructures/260173

Qualitative Research in Information Systems: An Exploration of Methods
M. Gordon Hunter (2004). *The Handbook of Information Systems Research (pp. 291-304).*
www.irma-international.org/chapter/qualitative-research-information-systems/30354

Towards Higher Software Quality in Very Small Entities: ISO/IEC 29110 Software Basic Profile Mapping to Testing Standards
Alena Buchalcevova (2021). *International Journal of Information Technologies and Systems Approach (pp. 79-96).*
www.irma-international.org/article/towards-higher-software-quality-in-very-small-entities/272760

Gendering Information and Communication Technologies in Climate Change
Sam Wong (2021). *Encyclopedia of Information Science and Technology, Fifth Edition (pp. 1408-1422).*
www.irma-international.org/chapter/gendering-information-and-communication-technologies-in-climate-change/260275