Research Article

Privacy Information Security Classification for Internet of Things Based on Internet Data

Xiaofeng Lu, Zhaowei Qu, Qi Li, and Pan Hui

1Beijing University of Posts and Telecommunications, Beijing 100876, China
2Hong Kong University of Science and Technology, Clear Water Bay, Hong Kong

Correspondence should be addressed to Xiaofeng Lu; luxf@bupt.edu.cn

Received 10 January 2015; Accepted 17 February 2015

Academic Editor: Xiuwen Cheng

Copyright © 2015 Xiaofeng Lu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A lot of privacy protection technologies have been proposed, but most of them are independent and aim at protecting some specific privacy. There is hardly enough deep study into the attributes of privacy. To minimize the damage and influence of the privacy disclosure, the important and sensitive privacy should be a priori preserved if all privacy pieces cannot be preserved. This paper focuses on studying the attributes of the privacy and proposes privacy information security classification (PISC) model. The privacy is classified into four security classifications by PISC, and each classification has its security goal, respectively. Google search engine is taken as the research platform to collect the related data for study. Based on the data from the search engine, we got the security classifications of 53 pieces of privacy.

1. Introduction

Cyber-physical systems (CPS) are engineered systems comprising interacting physical and computational components. Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of Internet of Things is the pervasive presence around us of a variety of things or objects, such as radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, which, through unique addressing schemes, build a network and are able to interact with each other and cooperate with their neighbors to reach common goals [1]. Since the key point of IoT is to make a variety of things to be a network, Internet of Things is a case of CPS.

Software design in CPS will have a very strong “systems engineering” flavor: the software implementation of various system functions (e.g., traction control in an automobile) becomes the primary method for realizing that function. This means that software cannot be designed independently of the system, and the system cannot be designed independently of the software [2]. So, when we build a CPS system, we must consider the information and information security in the software.

The ability of collecting personal private information is growing with the expansion of the IoT ability, so International Telecommunication Union (ITU) points out that user privacy is one of the important challenges of Internet of Things (IoT) [3]. In CPS, privacy security is an important challenge as well.

In order to provide integrated services, sensors will be integrated into buildings, vehicles, and common environments, carried by people and attached to animals to communicate among them locally and remotely [4]. Moreover, since IoT could include various cameras, GPS, and RFID equipment, the information of one's environment and behavior can be collected comprehensively and accurately, such as his/her location, movement speed, and physical signs (e.g., pulse, blood pressure, and disease) [5].

CPS and IoT can bring great commercial and political interests for hackers [6-8]. As CPS/IoT technologies are widely used in various industries, national defense, military, and other areas of the national interests, there are enormous commercial and political interests in it. Driven by those
interests, the hackers and Internet virus manufacturers will launch more targeted and harmful attacks.

The two points above bring great threat to the personal information security in the IoT. Unfortunately, the issue of privacy protection has not gotten enough attention. A lot of privacy protection technologies have been discussed recently [9–13], but most of them are independent and aim at protecting certain privacy, such as location. An IoT application includes different privacy classifications, and it is costly to protect all of them. Due to the economic cost of system implementation and running efficiency, it is impossible to employ all the privacy protection technologies in some cases [12]. Hence, it is necessary to divide the privacy into different classifications so that we can protect the important privacy with limited cost and technology.

Meanwhile, we found that the study of privacy attribute is not enough and there is not an objective method to classify privacy into different classifications. According to some privacy classification methods, the sensitive level of a piece of privacy is determined by the owner’s feeling [14]. However, to a certain piece of privacy, different people may have different feelings, so the piece of privacy will have many sensitive levels. This brings great difficulty to the CPS software development. For this reason, we propose an objective method to classify the privacy into different security levels.

The contributions of this paper include the following. (1) We focus on studying the attributes of the privacy and define two attributes of privacy. (2) We propose privacy information security classification (PISC) model. (3) We propose an objective method based on the big data from Google to classify the privacy information into different security levels.

2. Related Work

Facebook is the largest social network website, where people can share their photos and personal information. In Facebook, a photo can be set in different privacy levels [15]. There are five levels of privacy settings that a person can choose: everyone, friends of friends, friends, some friends, and only me. Different privacy levels mean the different viewers of the photo. Facebook privacy setting system is totally designed for the Facebook website. Although it gives users the right to determine the viewers, Facebook does not assign the privacy level of the information and photo.

Information security and privacy classification (ISPC) is a classification schema to safeguard personal information and is mainly used in medical health. By ISPC, personal information is classified into 4 sensitivity classifications: high, medium, low, and unclassified [14]. Unclassified level is the information that is meant for the public to see. Unclassified information does not require any additional safeguards. Low level is the information that is generally available to employees and approved nonemployees only. Medium level is the information that is intended to be accessed by a specific group of employees only. High level is the information that is extremely confidential and intended for access by named individuals or positions only. However, ISPC does not assign the sensitivity level of each piece of personal information. By ISPC, the sensitivity classification level is determined by the individual.

Corby studied the producing of privacy and divided the privacy into static, dynamic, and derived types based on time concept and the source of privacy [16]. Static privacy describes who we are, significant property identifiers, and other tangible elements. Dynamic privacy is the data we create. Records of transactions we initiate constitute the bulk of dynamic data. Every charge card transaction, telephone call, and bank transaction are added to the collection of dynamic data. Derived privacy data is created by analyzing groups of dynamic transactions over time to build a profile of your behavior. Corby studied the source of privacy, but the privacy in the same state, such as static, has different confidentiality.

Goldberg focused on the anonymity of the private information. He classified the open state of the privacy information into: verinymity, persistent pseudonymity, linkable anonymity, and unlinkable anonymity [17]. A verinym is a true name. It could mean the name printed on the government-issued birth certificate, driver’s license, or passport, but not necessarily. The kind of persistent pseudonymity privacy means the information is related to someone, but this one is unable to be confirmed, such as an MSN account. The kind of linkable anonymity privacy means the information is generated by a possible object, such as a phone call record, by which we can identify the phone call from where but cannot verify who dials the phone. By unlinkable anonymous state privacy, it is completely impossible to verify the source of the information. However, anonymity of the privacy is not privacy confidentiality. According to Goldberg’s study, the anonymity degree of true name is the least, so true name should be strictly protected. However, most people use their true names every day, so obviously the confidentiality of the true name is very low.

Wu studied the privacy protection when a user requests a service in Internet of Things application [18]. He combined the studies of Corby and Goldberg and proposed a secrecy state classification method of the privacy. In Wu’s model, there are four types of privacy: anonymous, semianonymous, semipublic, and public privacy. Anonymous privacy is the personal information. Semianonymous and semipublic privacy include the static data, dynamic data, and derived data. And the norm of law is defined as public privacy. We think Wu’s model splits the relationship between the data and the person. In fact, personal information comprises static data, dynamic data, and derived data. And Wu mixed the concept of privacy and personal information. We think public privacy does not exist.

Corby, Goldberg, and Wu wanted to classify the privacy by its source or state. Wu wanted to classify the privacy into different secrecy levels according to the source of it, but the secrecy degree of the privacy does not depend on its source. All of them did not give an objective method to classify the privacy.

Lu et al. studied the privacy information security classification in IoT based on the data from Baidu search engine [19]. We improved the computational method of the paper and the classification result is different from that in [19]. Baidu is the biggest Chinese search engine. We found that
the classification results by Baidu are different from those by Google search engine. This shows the worry about the privacy and privacy disclosure of the Wester learnt from different technologies.

3. Privacy Attributes Definition

3.1. Definition of Privacy. About the meaning of “privacy,” psychologists believe that the privacy consciousness originates from the human sense of shame [20]. The personal information could be any of a large number of things, including personal name, age, shopping habits, nationality, email or IP address, physical address, and identity. The personal privacy is usually a very subjective concept, so the understanding of the privacy of different individuals is different. The private information that some people regard as private may be insignificant to others. For example, some women think the age is their privacy and will not tell it to others, but most men do not mind telling others their ages. In addition, the privacy is closely associated with the situation and environment. People would like to share their privacy with their friends in a private environment. The privacy may not be an entirely objective existence, but a cognitive process, and everyone has his or her own privacy boundary and threshold. However, the privacy is a kind of the general public psychology of the human society; hence it still needs to be studied in accordance with the standards of the general public. Thus it is necessary to research the privacy and privacy attributes with greater pertinence.

In order to protect privacy information, we must clarify the meaning of privacy at first. The Oxford English Dictionary explains the meaning of privacy as (1) freedom from interference or public attention and (2) state of being alone or undisturbed. The privacy shows a kind of general public psychology of the human society, which is that a person would not like to let others know his/her secret.

In this paper, “privacy information” refers to personal data or transactions that can be stored in IoT/CPS systems, not the personal thought or feeling that will not be stored usually.

3.2. Privacy Attribute: Confidentiality. A widely accepted meaning of privacy is the confidentiality. Privacy confidentiality refers to the degree of the secrecy of the information for a person. Privacy confidentiality reflects the severity degree of the consequences caused by privacy disclosure.

Some personal information such as the height is a kind of privacy, but the privacy is not undiscovered because others can guess someone’s height from his/her figure. Disclosure of this kind of information would not bring serious influence on the individuals. However, if some privacy items, such as personal property, physical defect, and specific disease, are leaked, it will bring serious economic loss or damage to owner’s reputation and social status. Therefore, the confidentiality of this kind of privacy is high. Sometimes the disclosure of them will even affect the whole society. In privacy information protection, more attention should be paid to the confidentiality than to the integrity.

3.3. Privacy Attribute: Universality. The privacy information is usually a subjective concept because different individuals have different understanding of the privacy, such as age. But some information, such as disease and physical defect, is the privacy for all people. The universality of the privacy means the proportion of people who believe this information to be their privacy among all the people. Since it is impossible to investigate in the whole society whether a certain piece of information is their privacy, our study is based on the survey on Internet.

4. Privacy Attributes Study Based on Search Engine

4.1. Study Data from Search Engine. The goal of the privacy information security classification is to ensure the safety of the important privacy under the constrained security technology and cost. The importance degree of a piece of privacy is the comparison result of the privacy with other pieces of privacy. With the development of Internet, people get used to get help from Internet by search engines, especially when people realize that their privacy is leaked. For example, a lot of people will search “What shall I do when my credit card information has been disclosed?” or “Is my home address privacy?” and so on. Therefore, the searching behavior on the search engine can reflect people’s worry about privacy disclosure [19]. Google is the largest search engine in the world. Based on Google search engine as our research platform, we can get the amount of the webpages of each piece of privacy on the search engine. The number of the webpages can be used to analyze the privacy attributes. In this study, we selected 53 pieces of privacy which are often used in IoT/CPS systems. The number of webpages is about $3 \times 10^{10}$.

4.2. Privacy Query Data. To collect the data of the webpages about a piece of privacy, we define two input templates as the input query question on the search engine. The first step is to study the degree of the privacy universality. The number of webpages related to a piece of privacy reflects the privacy universality of it. Input template 1 is designed to collect the number of webpages that contain the privacy.

Input Template 1: “The Name of a Piece of Privacy” “Privacy.” Let $Q_i(x)$ be the total number of query results of the privacy $x$ by input template 1. As $Q_i(x)$ is very large, we normalize $Q_i(x)$ by Min-Max normalization method. $U(x_i)$ is the privacy universality of $x_i$ and it is equal to the normalized $Q_i(x_i)$:

$$U(x_i) = \frac{Q_i(x_i) - \min(Q_i(X))}{\max(Q_i(X)) - \min(Q_i(X))},$$

where $X = \{x_1, x_2, \ldots, x_n\}$.

The second step is to get the number of webpages about the privacy confidentiality. The privacy confidentiality can be reflected by the queries which show users’ concerns about privacy disclosure. For some pieces of privacy, such as “criminal records,” the number of the webpages containing “criminal records” is not very large, but “criminal records” are
Table 1: $U(X)$ and $C(X)$.

| Privacy                  | $U(X)$  | $C(X)$  |
|-------------------------|---------|---------|
| Call records            | 0.0908  | 1.0000  |
| Disease                 | 0.1801  | 0.6534  |
| Identification          | 0.1735  | 0.6149  |
| Affiliation             | 0.0354  | 0.5966  |
| Birth                   | 0.1779  | 0.3771  |
| Online records          | 0.1942  | 0.3621  |
| Stock                   | 0.3308  | 0.3564  |
| Insurance               | 0.3291  | 0.3561  |
| Race                    | 0.2062  | 0.3475  |
| Nation                  | 0.2078  | 0.3349  |
| Criminal records        | 0.0000  | 0.3312  |
| Marriage                | 0.1072  | 0.2962  |
| Credit card records     | 0.0410  | 0.2880  |
| Religion                | 0.1507  | 0.2829  |
| Weight                  | 0.2628  | 0.2797  |
| Location                | 0.4151  | 0.2765  |
| Job                     | 0.4570  | 0.2719  |
| Bank account            | 0.1257  | 0.2342  |
| Party                   | 0.3370  | 0.2230  |
| Age                     | 0.5207  | 0.2222  |
| Children                | 0.5756  | 0.2185  |
| House                   | 0.6083  | 0.2133  |
| Home                    | 0.6463  | 0.1994  |
| Company address         | 0.5811  | 0.1939  |
| Blood type              | 0.0625  | 0.1726  |
| IP                      | 0.0384  | 0.1727  |

Table 1 is the number of $U(X)$ and $C(X)$ of each piece of privacy. Although the confidentialities of some pieces of privacy are high, such as call records, disease, and affiliation, the universalities of these pieces of privacy are low. It indicates that $U(X)$ and $C(X)$ are independent.

Figure 1 is the distribution of $U(X)$ and $C(X)$. Figure 1 shows the feature of the privacy. There are some pieces of privacy with high privacy universality and low privacy confidentiality. Also, there are some pieces of privacy with high privacy confidentiality and low privacy universality. Moreover, the number of the privacy pieces with both its privacy confidentiality and privacy universality being low or medium is the largest. However, the most important discovery is that there is no privacy with both its privacy confidentiality and privacy universality being high. Phone call records, which indicate who we contacted and where we were every day, have the most confidential privacy, but just small amount of people think it is their privacy. On the contrary, although most people think the photos are their privacy, they like to share their photos with their friends or even publish their photos on some websites, such as Facebook.

4.3. Determining the Security Levels of Privacy Attribute. According to ISPC [15], the sensitive level of a piece of privacy of a person is determined by the feeling of the person, so a piece of privacy may have different sensitive levels in ISPC.
employ privacy protection technologies to protect all pieces of privacy in some cases. Therefore, the privacy should be classified into different levels according to the importance of it. Thus, some pieces of important privacy are protected by complex technologies and some pieces of privacy are protected by simple technologies. The objective of classifying the privacy is to ensure the security of the important privacy; the classification is named as security classification.

5.2. Privacy Information Security Classification. The security protection level of an IT system does not depend on the scale of the IT system, the cost of building the system, and the service object, but rather depends on the damage of the information disclosure [21]. The damage refers to the infringement to the interests of all the parties involved in the information disclosure. We define the source of damage to be the threat source. The relationship among the threat source, the privacy information, and the interests of all the parties is shown in Figure 2.

The security level of the privacy information is not determined by the destruction to the privacy information itself but depends on the scope of person involved in the privacy disclosure and the degree of privacy confidentiality. This is the key to classify the privacy information. For instance, a RFID card is physically destroyed by the hostile and cannot be used again, but the privacy information in the card is not revealed in fact.

We propose a privacy information security classification (PISC) model for privacy in IoT and CPS, in which the security level of the privacy information is determined by the consequence of the privacy disclosure, which includes two factors: the scope of the parties involved in the privacy disclosure and the degree of the confidentiality of the privacy.

The privacy universality means the proportion of the people who regard a piece of information as their privacy among all the people. In other words, the privacy universality indicates how many people think they are infringed when the information is disclosed. Therefore, the privacy universality can represent the scope of the parties involved in the privacy infringement. The privacy confidentiality indicates the importance of the privacy to its owner and the degree of secrecy.

By PISC, privacy is classified into 4 security levels or classifications according to both the privacy confidentiality and privacy universality. The 4 security levels are high security, medium security, basic security, and low security. The security classification of a piece of privacy is determined based on its confidentiality level and universality level, which is shown in Table 3.

### Table 2: The referential boundary of each level.

| Level         | Boundary        |
|---------------|-----------------|
| Low           | [0, 0.19)       |
| Medium        | [0.19, 0.4)     |
| High          | [0.4, 0.75)     |
| Very high     | [0.75, 1]       |

![Figure 1: The distribution of the privacy universality and privacy confidentiality.](image)

![Figure 2: The relationship among the threat source, the privacy information, and the interests of all parties.](image)
Table 3: Security classification decision by the privacy universality and the privacy confidentiality.

| Universality | Low | Medium | High | Very high |
|--------------|-----|--------|------|-----------|
| Low          | Low | Basic  | Medium | High     |
| Medium       | Basic | Basic | Medium | High     |
| High         | Medium | Medium | High   |           |
| Very high    | High | High   |        |           |

Figure 3: The distribution of four classifications.

High Security Privacy. High security privacy is (1) the privacy that its confidentiality or universality is very high and (2) the privacy that both its confidentiality and universality are high.

Medium Security Privacy. Medium security privacy is (1) the privacy that its confidentiality is high and universality is medium or low and (2) the privacy that its universality is high and confidentiality is medium or low. The security requirement of this classification is lower than the high security privacy.

Basic Security Privacy. Basic security privacy is (1) the privacy that one of its confidentiality and universality is medium and another is low and (2) the privacy with both its confidentiality and universality being medium.

Low Security Privacy. Low security privacy is the privacy with both its confidentiality and universality being low. The security requirement of this classification is the lowest.

5.3. PISC Classification Results. Figure 3 shows the distribution of the four security classifications. The distribution of the four security classifications is roughly symmetrical. The privacy in the bottom right is more than the privacy in the top left, which shows that the privacy universality was stronger than the privacy confidentiality to affect the classification result.

Table 4 is the PISC classification result and the privacy source. It shows that the security classification of a piece of privacy does not depend on the source of the privacy. We found that most people agree that family and photo are our private information or privacy. Call records, personal photo, and family information are the high security privacy that needs to be protected firstly. 62.5% static privacy is basic security or low security privacy. Because people often provide their static personal information to their companies or some institutions, such as banks, static privacy actually is known in many places. 50% dynamic privacy is medium security or high security privacy. It shows that the privacy which we create should be protected. For most people, the privacy in the high security level is more personal or steady than that in the lower security level. For example, both house and salary are a person’s property, but house can show a person’s wealth more than the salary. Another example, a person changes his or her mobile phone number more frequently than changing the line telephone number. Derived privacy is created by analyzing groups of dynamic transactions over time, so it is not created by the owner of the privacy. The security level of the derived privacy is the highest security level among the dynamic transactions privacy that it analyzes.

5.4. Discussion. The data we used to classify the privacy were not collected from IoT or CPS systems, but from Google. However, the data on search engine are generated by the people all over the world, so the data can reflect most people’s feelings and judgments. Thus, the data are impartial and objective and the classification results are objective. By classifying and organizing the privacy/data in IoT system, the system efficiency can be increased.

6. Security Goals

According to the harmful consequence caused by the illegal access to the privacy information or the privacy leak, the privacy in Internet of Things is divided into four classifications according to the security level. We should take into account different privacy protection technologies to achieve specific security goals for different security classifications privacy. The following are the four security goals of the above four privacy security levels:

(1) the security goal for the low security privacy: the privacy in this classification is allowed to be unencrypt, but the privacy cannot be accessed without authorization;
(2) the security goal for the basic security privacy: to encrypt the privacy in the storage medium and during the transmission and ensure that the privacy cannot be accessed without authorization;
(3) the security goal for the high security privacy: consisting in the protection abilities in goal 2 and the encryption keys of different people being different;
(4) the security goal for the medium security privacy: consisting in the protection abilities in goal 3 and ensuring the access authorization is valid just for one time reading or writing.
Table 4: PISC classification result.

| Privacy source (Corby [16]) | High security privacy | Medium security privacy | Basic security privacy | Low security privacy |
|-----------------------------|-----------------------|-------------------------|-----------------------|---------------------|
| (I) Static                  |                       |                         |                       |                     |
| (A) Who we are              |                       |                         |                       |                     |
| (1) Bio identity            | Age                   | Weight, height, Race, birth | Blood type, fingerprint |
| (2) Financial identity      | Identification        | Bank account, credit card | Passport, driver’s license |
| (3) Legal identity          | Identification        | Religion, nation, marriage, and position |                       |
| (4) Social identity         | Affiliation, job, and party | Email address, mobile phone |                       |
| (5) Virtual identity        | Phone number, password | Msn, IP                 |                       |
| (B) What we have            |                       |                         |                       |                     |
| (1) Property                | House, car, and property | Investment, stock | Salary |
| (2) Nonreal property        | Insurance             | Phone book, address book | Spouse |
| (3) Relation                | Family                | Children                |                       |
| (C) Where we are            | Home, company address |                         |                       |
| (II) Dynamic                |                       |                         |                       |                     |
| (A) Transactions            | Call records          | Shopping                | Credit card records   | Booking hotel, credit score |
| (B) How we live             | My photo              | Travel, disease         | Online records, criminal records, and chat | Hobby, drug use |
| (C) Where we are            | Location              |                         |                       |                     |

7. Conclusions

The IoT/CPS application cannot work without the users’ participation, so their personal information and behavior are stored, transmitted, and processed in the application. To minimize the damage and influence of the privacy disclosure, we must pay more attention to the important and sensitive privacy. The importance degree of a piece of privacy is the comparison result of the privacy with other privacy. For this reason, we studied the attributes of the privacy information and defined two privacy attributes: privacy universality and privacy confidentiality. We proposed privacy information security classification model which classifies the privacy into four security classifications. The security goals for the four classifications are different, and then people should take different security protection technologies to achieve corresponding security goals. Moreover, if an IoT application has some other pieces of privacy that are not included in this classification results, the system designer can employ the method in this paper to determine the security classification of the additional privacy.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grants nos. 61472046 and 61372109).

References

[1] D. Giusto, A. Iera, G. Morabito, and L. Atzori, Eds., The Internet of Things, Springer, Berlin, Germany, 2010.
[2] Software Engineering Institute, “Cyber-Physical Systems,” http://www.sei.cmu.edu/cyber-physical/.
[3] International Telecommunication Union, “The internet of things,” ITU Report, 2005.
[4] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: a survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[5] G. Mulligan, “The internet of things: here now and coming soon,” IEEE Internet Computing, vol. 14, no. 1, pp. 35–36, 2010.
[6] R. H. Weber, “Internet of Things—new security and privacy challenges,” Computer Law and Security Review, vol. 26, no. 1, pp. 23–30, 2010.
[7] C. M. Medaglia and A. Serbanati, “An overview of privacy and security issues in the Internet of things,” in The Internet of Things: Proceedings of the 20th Tyrrhenian Workshop on Digital Communications, pp. 389–395, Springer, New York, NY, USA, 2010.
[8] C. P. Mayer, “Security and privacy challenges in the internet of things,” Electronic Communications of the EASST, vol. 17, 2009.
[9] C. M. Medaglia and A. Serbanati, “An overview of privacy and security issues in the Internet of things,” in Proceedings of the 20th Tyrrenian Workshop on Digital Communications, pp. 389–395, Ponza, Italy, 2010.

[10] P. De Leusse, P. Periorellis, T. Dimitrakos, and S. K. Nair, “Self managed security cell, a security model for the internet of things and services,” in Proceedings of the 1st International Conference on Advances in Future Internet (AFIN ’09), pp. 47–52, Athens, Greece, June 2009.

[11] B. Shen and Y. Liu, “Privacy and security in the exploitation of internet of things,” Journal of Dialectics of Nature, vol. 33, no. 6, pp. 77–83, 2011.

[12] K. Aquilina, “Public security versus privacy in technology law: a balancing act?” Computer Law & Security Review, vol. 26, no. 2, pp. 130–143, 2010.

[13] T. Zhang, J. He, and H. Yu, “Secure localization in wireless sensor networks with mobile beacons,” International Journal of Distributed Sensor Networks, vol. 2012, Article ID 732381, 11 pages, 2012.

[14] Office of the Chief Information & Privacy Officer, “Information security & privacy classification(ISPC),” in Proceedings of the Sharing New Perspective: Access & Privacy Workshop, October 2008.

[15] S. Grauschopf, “Facebook Privacy Levels—Understanding Facebook’s Levels of Privacy,” http://contests.about.com/od/facebookcontests/tp/Facebook-Privacy-Levels.htm.

[16] J. M. Corby, “The case for privacy,” Information Systems Security, vol. 11, no. 2, pp. 9–14, 2002.

[17] I. Goldberg, A pseudonymous communications infrastructure for the internet [Ph.D. thesis], University of California at Berkeley, 2000.

[18] L. Wu, Research on technology service acception and personal privacy information affection of internet of things [Ph.D. thesis], University of Electronic Science and Technology of China, 2011.

[19] X. F. Lu, Q. Li, Z. Qu, and P. Hui, “Privacy information security classification study in internet of things,” in Proceedings of the International Conference on Identification, Information and Knowledge in the Internet of Things, 2014.

[20] Z. Li, The law protection for the privacy right [Ph.D. thesis], China University of Political Science and Law, Changping, China, 2006.

[21] Chinese Standard, “Information security technology—classification guide for classified protection of information systems security,” Tech. Rep. GB/T 22240–20, 2008, http://www.cspec.gov.cn/web/Upload/2011-04/file/zhengcefangui/201104140229198906937.pdf.