Personal Information and Privacy in E-Commerce Application

NORJIHAN ABDUL GHANI¹, ZAILANI MOHAMED SIDEK²

¹Information Science Department
University of Malaya
50603 Kuala Lumpur
MALAYSIA
norjihan@um.edu.my

²Centre for Advanced Software Engineering (CASE),
Universiti Teknologi Malaysia,
City Campus, Jalan Semarak,
54100 Kuala Lumpur,
MALAYSIA
zailani@citycampus.utm.my

Abstract: - Today, the world are moving towards e-commerce application in completing their daily jobs. An e-commerce application becomes the preferred medium to complete the day’s tasks. The potential for wide-ranging surveillance of all cyber activities presents a serious threat to information privacy. It gives more bad results in personal information privacy. In any e-commerce activities, all personal information should be controlled including their disclosure in order to protect its privacy. This paper discusses how personal information is used in e-commerce application and how it should be controlled.

Key-Words: - personal information, information privacy, electronic commerce.

1 Introduction
Nowadays, the internet has become an integral part of millions of people in their daily lives. Individuals rely much on the Internet; e-commerce applications basically interact with others, businesses conduct their transactions online, and many other tasks have been done through the Internet. The more people rely on the Internet in their daily life, the more they reveal their personal information. People disclose their information such as their names, addresses, credit card numbers and many others; meanwhile organizations will store that information inside their databases. Increasingly, companies are holding more and more data about us every day. Unfortunately, there are many people that do not care about their own data. They do not know how valuable their information is. They do not know to what extent their information will be used. Besides that, many companies are unable to protect users' personal information.

Privacy International, from one of the articles published by the Centre for Independent Journalism, January 17th, 2008 [6], said that:

"On the one hand, individual information is not protected and can be used virtually by anyone for any purpose, ..."

The above statement notifies that the organization that collect the information do not protect the information they obtained from the owners. Because of that, the ability to protect that information and enforce privacy policies become more important. The increasing number of reports of privacy violations due to external break-ins as well as accidental and malicious misuse of personal information by individuals within an organization is only exacerbating the problem.

This paper will discuss the importance of and the relationship between security and privacy in Section 2. Section 3 discusses personal information and it’s basic flow. Section 4 discusses the importance of personal information in e-commerce applications, how they are being used, and the importance of controlling the personal information disclosure in such applications. Section 5 will conclude the discussion.

2 Security vs. Privacy
In general, security breaches are categorized as unauthorized data observation, incorrect data modification, and data unavailability. Unauthorized data
observation is whenever the disclosure of information to users which are not entitled to gain access to such information. Incorrect data modifications, either intentional or unintentional, may result in any incorrect database state. Data unavailability will cause the failure of transactions in any organizations; data is not readily available when needed. Thus in [1], a complete solution to data security must meet the following three requirements: 1) secrecy or confidentiality refers to the protection of data against unauthorized disclosure, 2) integrity refers to the prevention of unauthorized and improper data modification, and 3) availability refers to the prevention and recovery from hardware and software errors and from malicious data access denials making the database system unavailable.

In [2], confidentiality involves sharing of information while secrecy is a type of blocking that makes the information unavailable. "Confidential" information generally refers to any information that is kept in confidence such that its revelation requires the consent of its owner [11]. It implies protection of other people’s secret information through the control of access to information and its release according to certain agreements between the organizations and the owner. Credit card numbers, identity card numbers and telephone numbers should be considered as confidential information. Information ‘sensitivity’ is typically defined in terms of the necessary protection level required for that information [11].

Because of this, the promotion of security and privacy are important element for supporting the growth of online applications in the world today. It has summed this up by claiming that privacy is an articulation of the core value of security.

2.1 What is Privacy?

Privacy generally is central to our dignity and our basic human rights. The right to privacy was first defended by the American justices Samuel Warren and Louis Brandeis, in [12] who defined privacy as:

“the right to be let alone”

Besides that, there are a number of privacy definitions. From the information system views, privacy is a right of individual to determine for themselves when, how, and to what extent the information will be released [3]. Goldberg defines privacy as an ability to control collection, retention and distribution of themselves [4]. The definition of privacy according to Ross Anderson is “the ability and/or right to protect our personal secrets, the ability and/or right to prevent invading our personal space [5]”

Privacy is held to be valuable for many reasons. Most often, it is held to be important because it is believed to protect individuals from all kinds of external threats, such as defamation, ridicule, harassment, manipulation, blackmail, theft, subordination, and exclusion. It has also been argued that privacy is a necessary condition for autonomy. It is because without privacy, people could not experiment in life and develop their own personality and thoughts, because they would constantly be subjected to the judgment of others.

From the information system views, information privacy can protect individuals from misuse of data, or unauthorized access to, or modification of information could adversely affect, or be of risk to the owner of that information. An important principle used in privacy protection in Western nations is that of informed consent: it is often held that citizens should be informed about how organizations plan to store, use or exchange their personal data, and that they should be asked for their consent. People can then voluntarily give up their privacy if they choose [12]. It is the willingness of consumers to share information over the Internet that allows the transaction to be completed and successful. It is the ability that concerns with the protection of information about individuals that is stored in a database.

3 Personal Information

Data is important in any transaction; either off-line transaction or online transaction. The growth of web-based information system have made information privacy become a more critical issue to be considered. On one hand, users submit their personal data to obtain services, on the other side, organizations need personal data to carry out their business. There is a need for both sides to make an agreement on how the data will be collected, used, stored and manipulated. As a result, more and more personal information will be collected and processed electronically.

In any information systems, especially, web-based information systems, data are released from the owner, through the system to accomplish a task. Then, this data will be processed to become information; will be stored, reused and manipulated. This information will be kept in a database as a record or reused in the future. There are four types of data involved in processing [8]:

i) **Personal data**: any data that can be used to identify a person such as name, address, telephone number.

ii) **Sensitive data**: any data that disclose information about racial or ethnic origin, religious, philosophical or other belief, political opinions, membership of parties, as well as personal data disclosing health such as health history, race, etc.

iii) **Identification data**: personal data that permit the direct identification of the data subject such as DNA, identity card number, etc.
Anonymous data: any data that cannot be associated to any identified or identifiable data subject such as gender, type of disease, etc.

From the above classification, the first three types of data can be considered as sensitive information. Sensitive information is information that requires protection due to risks that could result from its disclosure, alteration, or destruction. This sensitive information should be protected to ensure their privacy. Based on [7], the conceptualization of privacy is built on two distinct categories of privacy:

i) personal information privacy, and
ii) non-personal information privacy.

IITF Principles defines information privacy as an “individual’s claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed and used. From the definition, we can make a conclusion that, the central component of information privacy is the term personal information. IITF Principles define personal information as information identifiable to the individual.

Al-Fedaghi identifies that personal information privacy involves acts on personal information. Typically, “personal information” is defined as information that is owned by a person, such as name, address, contacts and others. Heikkinen et. al. [9] defines personal information as any information that is related to the individual person.

From the above classification, a conclusion can be made that not all data need to be kept confidential. It depends on the data owner himself. For example, if Person A always receive e-mails form unknown organizations to sell their products. She does not like to receive any online catalog from unknown organizations. So, the best way is to keep her e-mail address as a confidential data. On the other hand, if Person B is a salesman, receiving an online catalog will make his sale much better. So, he does not mind to disclose his e-mail address.

Defining private or personal information is a problematic issue. “Privacy means different things to different people, including the scholars who study it, and raises different concerns at different levels” [10]. In a web-based environment, personal information is disclosed by the data owner and used by the organizations. The organization will collect, store, manipulate information to fulfill their organization’s needs. Figure 1 shows how information is collected, stored, used and disclosed.

This model stated that any personal information should be disclosed only to authorized users, with a specific purpose and for a limited time. Because of this reason, we add another phase named “Controlling the personal information” before “Disclosing the personal information” phase.

3 Personal Information in E-Commerce Application
The previous section covers the definition and explanation of private information and its privacy. This section will continue the discussion on the issues and challenges of the protection of personal information in a web-based environment. This is important in order to make sure the information released by the owner is secure and kept private.

As discussed in the first section, there are three requirements in data security; confidentiality, integrity and availability. The first and the most important issue that should be considered is to develop a system that can find a proper balance for confidentiality, integrity and availability of private information.

E-commerce is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world. The revolution in our communication infrastructure – in particular, the explosive growth of the internet – has fundamentally transformed how we create, acquire, disseminate and use information [14]. Now, shopping and entertainment can be accessed and done immediately through virtual and digital malls. But unfortunately, e-commerce application also raises new concerns. People are already concerned with their privacy,
especially regarding their personal information that have been collected, used and stored by e-commerce applications. For example, in e-commerce application, every interaction is done by either credit card or auto debit. In order to complete a transaction, users need to release their personal information. But this type of information should be considered as private information and its disclosure should be limited based on the intended purposes only.

Personal information should only be kept by the owner themself. But in web-based applications, this information should be disclosed in order to fulfill the transaction. Although the private information is being disclosed, normally for the security and privacy reasons, it cannot be accessed by unauthorized users. For this reason, there are three main issues that need to be considered:

i) personal information should not be accessed by unauthorized users,

ii) only required personal information will be posed,

iii) personal information cannot be passed to those who do not need the information.

From a privacy perspective, the crucial characteristic of cyber-activity is the rich of flow of personal information it triggers. Figure 2 adopted from [15] shows an elementary electronic commerce transaction.

There are three types of transaction parties involved in this transaction; the individual, the merchant and the payment provider. The individuals provide their required information to the merchant. As a result, the merchant has access to all data that appear on a user’s credit card and shipping order. But, in order to secure the privacy and protect the personal information, this information should only be accessed if it is required to fulfill the purpose and only for a limited time by authorize users. In this case, it should be accessed by person who is in-charge of the transaction and the information may be kept in two weeks only. The payment provider, in this case refers to the credit card company, will collect the subscription data such as transactional data so that, it will appear on the monthly billing statements; including merchant name, city and state, date of purchase, and the amount of purchase. This payment provider also needs to maintain the confidentiality of the card holder’s information regarding a consumer’s credit worthiness, credit standing, credit capability, that may be needed by other credit card companies, insurance and other legitimate business needs.

4 Conclusion
The emerging trend in the world today is the shifting from off-line system to on-line system. It is important to protect the personal information from any incidents. Data privacy can be used as a solution developed for data security. Both data security and data privacy are based on a balance of confidentiality, integrity and availability. Ensuring the privacy is not only protecting the personal information, but it is also to have a good system with this three requirements.

References:


