Personal Information Privacy Protection in E-Commerce

NORJIHAN ABDUL GHANI[1], ZAILANI MOHAMED SIDEK[2]

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

[2]Centre 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. Electronic commerce or e-commerce is a potentially growing business for today's market. Basically, online shopping eliminates conventional purchase approach which is labor-intensive and time-consuming. Through cyber space, order can be placed electronically and the product will be produced and shipped with the middleman. 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 Internet is revolutionizing how we do our shopping. It has been developed into a dynamic virtual medium for selling and buying, either for information, services or products. The phenomenal growth and rising popularity of the Internet and the World Wide Web (WWW) today have attracted consumers and businesses to leverage the benefits and advantages brought on by this technology. Thousands of companies, large and small, are racing to set up online stores. Manufacturers that used to sell just to stores, now sell directly to you online. Brand-new online-only companies operate with no physical storefronts and little or no inventory and pass much of the savings on to you. And stores all over the world are just a click away. This new way of shopping provides you with and enormous choice of products, as well as a vast variety of detailed information to help you make the right decisions about everything from books to cars, from clothes to real estate--even money. The Internet exerts an increasingly strong influence on people's everyday life. The growth of interest in the Internet as a shopping and purchasing medium is fascinating for practitioners and researchers alike. Its rapid growth poses intriguing questions for academic research.

Online shopping is activities of buying and selling the products or services through Internet. Online shopping can be considered as easier, simple and the fastest way to do shopping. Users are able to do online shopping by browsing the online shopping web site. This web site will offered relevant information about the product offered by the company. Besides that buyers can make comparison between the products. The buyer then can selects items from the online catalogue and makes the

purchase. According to [20], "internet shopping is online versions of physical retails stores where all transactions and their relevant activities take place in online cyber spaces."

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.

This paper will differentiate between conventional and online shopping in Section 2. Section 3 highlights the importance of and the relationship between security and privacy. Section 4 discusses personal information and its basic flow. Section 5 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 6 will conclude the discussion.

2 Conventional Shopping vs. Online Shopping

2.1 Conventional Shopping

In conventional sales, the buyer or the salesman is the active party. If a buyer wants to purchase anything he either has to go to the store to buy or calling on the phone and making an order. In another situation, the salesman goes to the home or place of business to make the sale, or he calls customers on the phone to make the sale. Another method combines actions from both parties. The business sales department mails a product catalog or promotion advertisement, the customer then makes a purchase from the catalog. These methods all apply to business-to-person as well as business-to-business sales.

2.2 Online Shopping

E-commerce is a modern business methodology that addresses the needs of organizations, merchants and consumers to cut cost while improving the quality of goods and services and increasing the speed of service delivery. With e-commerce, consumers no longer need to travel to shops or stores to get our daily needs. All they have to do is browse through the Internet purchased the product they needed at anyway if they have a computer which connected to the internet with them. Furthermore, they also can safe their time and energy travel around to get the household they needed.

From a consumer point of view, two principal activities characterize e-commerce: online shopping and online purchasing. First, you can use the Internet to shop for products and services. That is, you can research a product, compare prices, and evaluate other factors such as return policies, security and privacy safeguards and as well as delivery options. Second, you can purchase a product from a Web site. The purchasing activity involves several steps: selecting the product, providing payment information such as a credit card number, providing a real-world address so that the credit card can be authorized and the product can be delivered, and providing an e-mail address so that the company supplying the product can immediately confirm your order. There are many differences between the conventional commerce and e-commerce. Table 1 shows the differences between conventional shopping and online shopping.

Table 1: Comparison between Conventional Shopping and Online Shopping

Conventional Shopping	Online Shopping
i. Real store at certain location	i. Virtual store on the web.
ii. Paper based transaction (cash, cherub, invoice and receipts.)	ii. Electronic records and communications (account number, credit card)
iii. Offline business.	iii. Online business.
iv. Use cash, credit card, cherub and other methods for payment.	iv. Usually use credit card for transaction.
v. Bounded by geographical factor.	v. Can do transaction at anywhere as long as have connection to internet.
vi. Can feel and touch the products.	vi. Cannot feel and touch the products

2.3 Consumer Trust towards Online Shopping

A survey has done in [27] shows the result as Table 2. The survey shown that most of the respondent knows the existence of online shopping, and for them, shopping online is better. Unfortunately, about 55% from the respondents said that they don't have positive experience with online shopping. This may result why they don't really trust online shopping. From the survey, there are two factors that can affect the trustworthiness of online shopping. The two factors are :

a. most of the respondents agree that security in payment is one of the trust factors to them towards online shopping
b. Most of the respondents agree privacy of the information is one of the trust factors to them towards online shopping.

Table 2: Level of Consumer's Trustworthiness towards Online Shopping

Questions	Yes	No
Do you know online shopping?	71	29
Using internet for purchasing online is a good idea	68	32
Do you have positive experience on online shopping?	45	55
Do you trust online shopping?	44	56
To build a trust towards online shopping is not difficult	67	31
Is it safe to do online shopping?	66	32
Do you trust the online shopping website?	54	46
Information privacy and confidentiality	73	27
Security in Payment	88	12
Provide consumer's Right	67	33
Are you willing to use online shopping?	62	38

Trust, as we know, is a prerequisite of many business interactions either for conventional shopping or online In essence, trust creates the social environment in which businesses can function [21].

Trust, in a broad sense, is the belief that other people will react in predictable ways [21]. This trust is crucial because people need to control, or at least feel that they understand, the social environment in which they live and interact. It is not easy for people to completely understand this social complexity or to know what to expect from others because other individuals are independent agents whose behavior and intentions cannot be controlled and may not be rational or predictable. Faced with such overpowering social uncertainty, on the one hand, and the need to comprehend the social environment in order to interact on a rational basis with other individuals, on the other hand, people are forced to trust in others. They must assume away many possible undesirable behaviors and intentions that others may indulge in. Trust is one of the most effective methods for reducing this social complexity, especially in the absence of rules and regulations [21].

Trust is especially important in an online environment when all consumers have to go by is a computer system embedded in web pages. Adapted to Anil work in [1], trust is very hard to develop in e-commerce situation because internet is known as open system architecture. It is important to understand the factors that might influence consumer's trust to use online shopping. From the survey done, we have identified two major factors to determine the successful of online shopping; security and privacy. The promotion and optimum use of security and privacy are important elements for supporting the growth of online shopping

3 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*.

3.1 Security

Security is a main issue in online shopping. Most of the consumers are concerned the security factors when dealing online. Security is one of the most challenging problems faced by customers who wish to do online shopping. It's not only for consumer but also for client. From [22], a security threat has been identified as a "circumstances, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse". Security that arises during the online shopping is derived from sending confidential information to clients and vendor over the internet. In some cases, parties involved should consider the threats such as stolen information and misuse of personal information. Most of the consumer are highly required the vendor to make sure all the information passes through the transaction were stored confidential and can't be viewed or used for any other transaction without their permission. They should feel that it's secure to do online shopping. Almost all online shopping provide online payment. In Malaysia itself there are two types of online payment that are widely used, such as credit card and auto debit from the account. Most of the consumers are afraid of giving the details of their account.

3.2 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. The ability to shop online – anytime, anywhere – is drastically changing the way consumers shop and has added more dimensions to privacy [23]. Privacy is the protection of the individual's right to nondisclosure [24]. Privacy refers to controlling the dissemination and use of data. In online shopping, vendors have to make sure that all the information gathered from consumer is protected and didn't spread to other parties. It is the willingness of consumers to share information over the internet that allows purchases to be concluded. Privacy issues over the internet include 'spam', usage tracking and data collection, choice, and the sharing of information with third parties [25]. Online shopping is successful if consumers are highly trust that their personal information is safe and secure. If consumer can't trust that their personal information is safe and secure; the internet will never reach its economic potential [26].

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.

Unlike data security, which focuses primarily on preventing unauthorized individuals from inappropriately obtaining information, the privacy problem focuses on providing individuals the ability to control how their data is managed and used by a particular organization. Violations of PI privacy also called data protection occurred when PI is improperly collected, used or disclosed. Westin, in [28] stated that there are three statements on how people agree or disagreed about PI privacy concerns:

1. Consumers have lost all control over how PI is collected and used by companies
2. Most businesses handle the PI they collect about consumers in a proper and confidential way
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

4 Personal Information

Data is important in any transaction; either off-line transaction or online transaction. The growth of web-based information system has 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.
iv) *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.

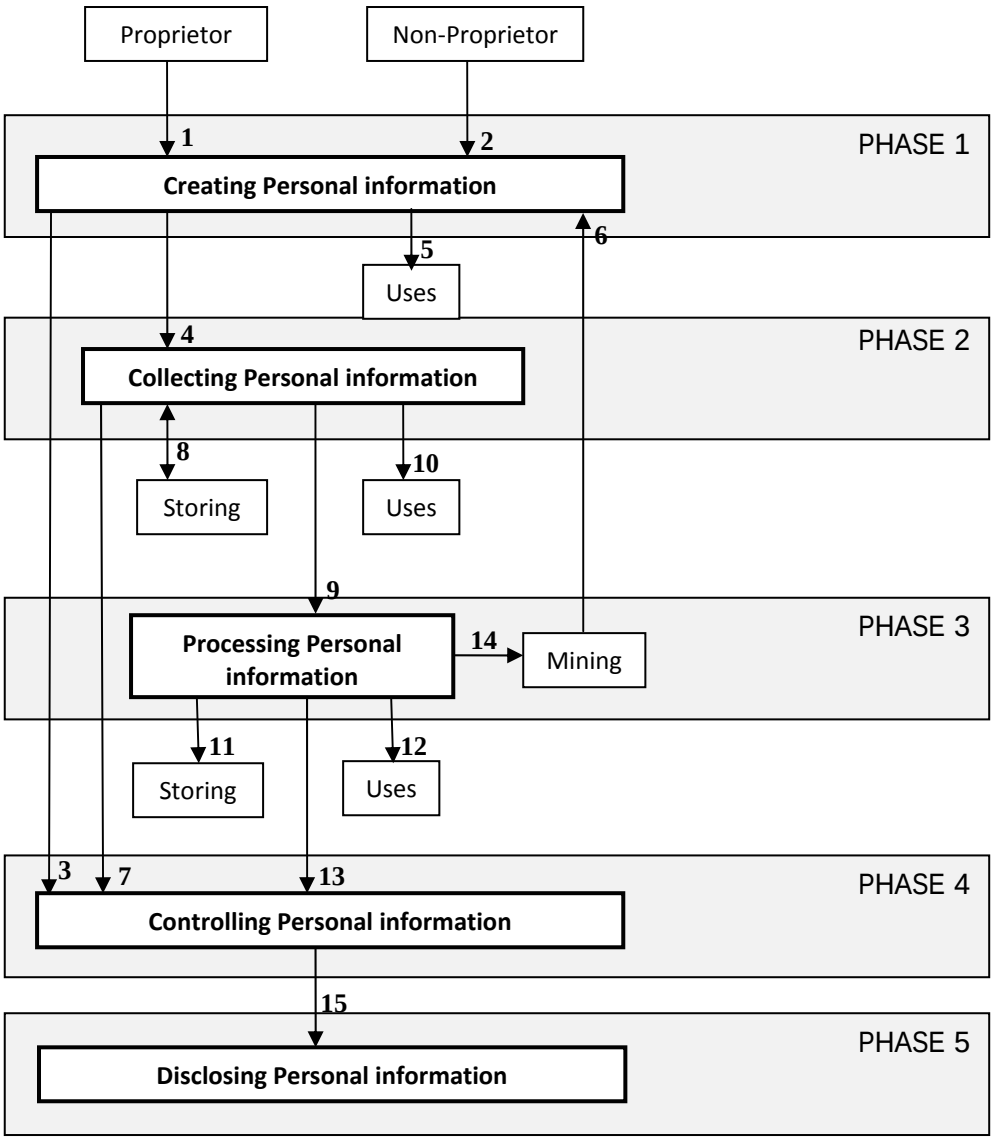

Figure 1: Enhancement of PIFM introduced by Al-Fedaghi, (2006b,2006c)

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 receives 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 authorize 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.

5 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 are 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 themselves. 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.

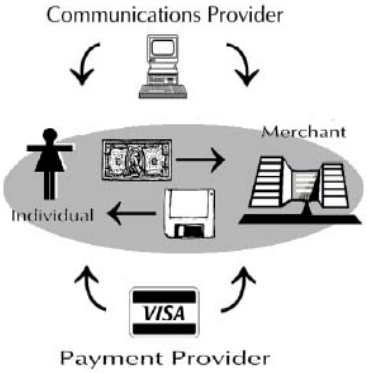

Figure 2 : An Elementary Electronic Commerce Transaction.

From the home, a user logs on into her requested Internet Service Provider through her computer and the Internet connection. After browsing various merchants, she made a decision to buy a book from an online book store. To complete the transaction, she needs to release her credit card number and her personal information such as name, contact number, billing address, etc. Besides this, the merchant's web site may require her interests, so that they can contact their customers to promote new books available.

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.

5.1 Personal Information and Its Privacy Issues in E-Commerce

Today, more people rely on online or web services in their daily life transactions such as buying groceries, renew driving license, even though checking their health. To make sure that human activities are successful, they need to release their important and PI such as identity card number, ATM pin number and also other secret information regarding occupation, health, and family. A first important class of techniques deals with privacy preservation when data are to be released to third parties. In this case, data once are released are no longer under the control of the organizations owning them. Therefore, the organizations that are owners of the data are not able to control the way data are used. Meaning that, once they released their information, anybody can access the information with or without their permission.

Central in privacy protection are the rights of an individual to know what data are maintained about him, challenge their veracity and relevance, limit their non routine use or dissemination, and to be assured that their quality, integrity and confidentiality are maintained. In the future, concerns for privacy and security must become integral in the planning and design of e-commerce application.

Privacy and security are the problems associated with computer systems and applications that were not foreseen until well into the second half of the present computer age (Turn, 1976). Privacy in information system is an issue that concerns the computer community in connection with maintaining personal information on individual citizens in information system or web based applications. Computer security includes procedures and technical measures required *1)* to prevent unauthorized access, modification, use and dissemination of data stored or processed in a computer system, 2) to prevent any deliberate denial of access, and *3)* to protect the system in it's entirely from physical harm. In the mid-1960's, privacy and security has emerged separately as problems an area in the computer field.

In the last few years, data and privacy protection have become critical issues in the development of information systems. This reflects the growing attention of customers to their personal information and the increasing number of laws, policies, and regulations that are intended to safeguard it. The US Privacy act of 1974 and the EU Directives on Privacy in 1995 define privacy as the right of data subjects to determine how their personal information is used. Several proposals (Agrawal, *et al.* 202) introduce the concept of *purpose* in order to capture this definition where purpose represents the intended usage of information. Current privacy legislation also defines the privacy principles that an information system has to meet in order to guarantee customer privacy. (Masaccio, *et al.* 2006) introduce two principles as *1)* transparency and 2) minimal disclosure. Principle of transparency said that enterprise should disclose to customers which data are collected and for what purposes, meanwhile minimal disclosure principle claimed that enterprises should maintain only such information about an individual as us necessary to fulfill the purpose for which it was collected. The transparency principles should aid customers to verify whether or not enterprise implements the minimal disclosure principle correctly. Enterprise should declare in their privacy policies the purpose for which data are collected, who can receive them, the length of time the data can be retained, and the authorized users who can access them.

Personal information only should be kept by the owner itself or control the disclosure in order to ensure its privacy. But, in web-based application, this information should be disclosed in order to fulfill the transaction. Although the private information is being disclosed, normally, for the security and privacy reason, it can't be accessed by unauthorized users. For this reason, there are three main issues that need to be considered :

1. Personal information shouldn't be access by unauthorized users.
2. only required PI will be posed
3. personal information can't be passes for those do not need the information

6 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.
Factors, security and privacy should be considered when designing a website for online shopping. People trust is very important factors to make sure the successfulness of online shopping.

References:

[1] Elisa Bertino, and Ravi Sandhu, "Database Security—Concepts, Approaches, and Challenges", *IEEE Transactions on Dependable and Secure Computing*, Vol. 2, No. 1, January-March 2005, pp 2 – 19.

[2] Sabah S. Al-Fedaghi, "Privacy as a base for Confidentiality". Presented in the Fourth Workshop on the Economics of Information Security, Harvard University, Cambridge, MA, 2005.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic databases. In *The 28th International Conference on Very Large Databases (VLDB)*, 2002.

[4] Goldberg, I., Wagner, D., Brewer, E., Privacy-Enhancing Technologies for the Internet. Proceedings, IEEE COMPCON ' 97, 1997, 103-109.

[5] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed System. Wiley Computer Publishing. New York, 2001 612 pp.

[6] Gayathry Venkiteswaran. 2007. Poor privacy protection in Malaysia, says Privacy International. Centre for Independent Journalism (CIJ) . Available at http://www.bangkit.net/2008/01/17/poor-privacy-protection-in-malaysia-says-privacy-international

[7] Al-Fedaghi, S. S. 2007. Anatomy of personal information processing: application to the EU privacy directive. Int. J. Liability and Scientific Enquiry, Vol 2. No's ½, pp129 – 138.

[8] P. Guarda, N. Zannone, Towards the development of privacy-aware systems. Information Software Technology (2008).

[9] Heikinen, K., Juha E., Pekka J., and Jari, P. Personalized View of personal information. WSEAS Transactions on Information Science and Applications, vol. 2, No. 4, 2004.

[10] Alessandro, 2004. Security of Personal Information and Privacy: Technological Solutions and Economic Incentives. In J. Camp and R. Lewis (eds), The Economics Information Security, Kluwer.

[11] Sabah S. Al-Fedaghi, "Privacy as a base for Confidentiality". Presented in the Fourth Workshop on the Economics of Information Security, Harvard University, Cambridge, MA, 2005.

[12] S. Warren, L. Brandeis, The Right to Privacy, Harvard Law Review 4, pp. 193-220, 1890.

[13] Martin S Olivier, Database Privacy Balancing Confidentiality, Integrity and Availability SIGKDD Explorations. Volume 4, Issue 2 - page 26.

[14] NETWORK WIZARDS, Internet Domain Survey, January 1997 (visited October 11, 2008) http://www.nw.com/zone/WWW/report.html

[15] Kang, Jerry,Information Privacy in Cyberspace Transactions. Stanford Law Review, Vol. 50, p. 1193, 1998.

[16] Skinner, G., Han, S. & Chang, E. (2006). A conceptual framework for Information Security and Privacy. *Proceedings of the 5th WSEAS International Conference on Applied Computer Science*, Hangzhou, China. April 16-18, 2006. pp410-415.

[17] Skinner, G., Han, S. & Chang, E. (2006). A conceptual framework for Information Security and Privacy. *Proceedings of the 5th WSEAS International Conference on Applied Computer Science*, Hangzhou, China, April 16-18, 2006. pp981-986.

[18] Papathanassiou, A. E., Mamakou, X. E. & Kardaras, D. K. (2006). Privacy Online: Research and Recommendations. *Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics*, Istanbul, Turkey, May 27-29, 2006 (pp309-314).

[19] Ali, H. (2005). Security & Trust in Agent-enabled E-commerce : Survey. *Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers*, Tenerife, Spain, December 16-18, 2005 (pp1-6).

[20] Yoo, Boonghe & Donthu, N. (2001). "Development Scale to Measure Perceive Quality of an Internet Shopping Sites (SITEQUAL)", *Quarterly Journal of Electronic Commerce.* Vol. 2 (1)p. 31 – 46.

[21] Luhmann, N. *Trust and Power*, John Wiley and Sons, London, 1979.

[22] Kalakota, R., Whinston, A.B., 1996. Frontiers of Electronic Commerce, Addison-Wesley, Reading, MA.

[23] Jatinder N. D. Gupta, Sushil K. Sharma (2002), *Managing Business with Electronic Commerce : Issues and Trends,* Idea Group Publishing, p 237.

[24] Gary P. Schneider, James T. Perry (2001). *Electronic Commerce :*Second Annual Edition, Thomson Learning Inc, p 178.

[25] Donna L. Hoffman, Thomas P. Norak, Marcos Peralta (1999), *Communications of the ACM.*Vol. 42, Issues 4(April 1999).

[26] Anthony Ferraro, (1998), *Electronic Commerce: The Issues and Challenges to Creating Trust and Positive Image in Consumer Sales on World Wide World, University Hawthome, New York. http://www.firstmonday.dk.issues/issues3_6/ferraro/#author.*

[27] Norjihan bt Abdul Ghani. (2005). Building Consumer's Trusts toward Online Shopping : Malaysia Scenario. Paper Presented at *Seminar on E-Commerce,* Port Dickson, Malaysia.

[28] Westin, A. (1967). *Privacy and Freedom.* Atheneum, New York.