A Discussion on the Privacy in Electronic Commerce

Xiang-Nan LI

PLA Academy of National Defense Information, No.45 Jiefang park Road, Wuhan, Hubei province, China, 430010

7410969@qq.com

Keywords: Privacy, Electronic Commerce, Security.

Abstract. Consumers' privacy is an issue of common concern in electronic commerce. By reviewing the current situation of e-commerce, the methods of collecting private information were presented, and consumers' freedom and sensitivity of treating personal information were discussed. On this basis, the FTC industry self-regulation recommendation and principles were studied, and a set of limitation of current privacy protection condition were analyzied.

Introduction

It is not a new phenomenon that sellers attempt to collect information about consumers and analyze this data to assist their business decisions. In this internet era, people are shifting their purchase behavior from physical retail store to online shopping websites. When consumers are enjoying the convenience of internet, they are losing anonymity in this progress [1]. They are tracked and their information are gathered by various channels. The situation becomes reverse. The salesperson could never know anything about you except your face in the past, while currently the website operators would collect numerous information about you, such as name, age, preference, and even financial details. Consumers are facing more and more risks through e-commerce business. What will merchants do with your personal detail? How can they reduce the information leakage risks?

This paper focuses on these aspects: How do merchants collect consumer's information and what kind of information do they gather? The scope of privacy. The practice of information privacy principles. Limitation of privacy protection.

Literature Review

Current Situation about Electronic Commerce

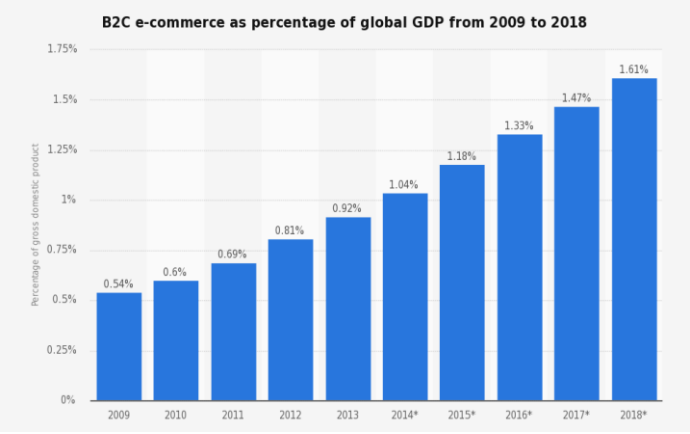

Figure. 1: B2C e-commerce as percentage of global GDP from 2009 to 2018 [4]

The IPO of China's e-commerce company, Alibaba, achieved a biggest amount at $25 billion in history in September 2014 [2]. That Chinese e-commerce giant has ever recorded a $3.1 billion sale in one day [3]. The online shopping market is growing at an amazing speed in the past decade. Statistics data shows that B2C e-commerce has doubled in percentage of global GDP from 2009 to

2014 and it will increase to 1.61% in four years (refer with: Fig. 1). The explosion in e-commerce attracts continuously new merchant entries. Digital payments, which are closely related to online shopping, set a fire to this sharp growth trend and itself is experiencing a high speed development.

How Information is Gathered

Self-Divulgence of Information

When shopping online, consumers proactively provide their personal information by three ways: purchase, website access and free merchandise [5].

A lot of people choose online payments to complete their online orders and input their residential addresses for postage. In this process, users are forced to reveal their most confidential personal information, including credit card details, full name, mobile number, billing address and numerous private information.

Almost all the merchants attempt to encourage people register on their webpages and leave personal information in their database in order to capture consumers' willingness to purchase and send promotion emails. Part of these merchants even induce users by announcing better service and collect information about users' age, habit, preference, gender, occupations and other personal details.

Some merchants claim that they provide free merchandise to anyone who matches their conditions. The only thing you need to do is just leaving your personal information and other shopping feedbacks. Although consumers would not reveal their financial information, they have to offer more consumption data to merchants.

Cookies

Cookies are log files that stored in website visitors' hard drive for tracking users' access to specific links. It is the most common method for merchants to identify and track consumers' activities [6]. Cookies are designed originally for viewing websites more effectively and should not be offensive against privacy protection. However, some service providers use them to locate users' behavior and attackers usually detect loopholes of vulnerable cookie mechanism.

Anonymous Profile Data

Website providers are able to track viewers' IP address and locate a rough physical address. By analyzing the traffic of clicking different sections on the page and users' IP addresses, merchants can make better market and advertisement decisions.

The Scope of Privacy

In relative research in sensitivity about personal information, it shows that the majority of consumers feel comfortable to share with their own preferences, such as favorite TV (82%) and snack food (80%). A fairly great part of respondents are willing to provide their email addresses (76%) and age (69%). The situation changes in providing other personal data, such as health condition (18%), income (17%) and phone number (11%) [7]. It is suspected that the different sensitive levels of personal information are related to unsolicited communications [8]. Foxman and Kiicoyne argued that intrusions of unsolicited communications are individual specific and information related to transactions, such as purchase history and recommend purchase promotions should not be defined as privacy violation. They proposed that the key point is who stores the data and how they use the data. In Federal Trade Commission's report, it defined personal information by two dimensions: identification information such as name, postal address or email address; aggregation, non-identifying, can be used for market analysis or in conjunction with identification information to create personal profiles such as demographic and preference statistics [9].

Freedom of Choice

No matter which level of sensitivity consumers treat their personal information, the fact is privacy is privacy. It was defined many years ago that privacy is the right that one person could control its flow and disclosure of the personal information him or herself [10]. The mechanisms of consumer

choice or consent can be developed into opt-in or opt-out [11]. Opt-in term means the storage and use of consumer's private information require consumers' confirmation. Opt-out rules the affirmative process of preventing such private information collection or use (refer with: Fig. 2). However, different from driver licenses and criminal record database, commercial databank serves private interests and is built up by merchants. As a result, it is accountable for commercial companies, not consumers [5].

		Consumer Control	
		No	Yes
Consumer Knowledge	No	**Surfing** ● Movements tracked by software. ● Consumer no longer owns information. **Purchasing** ● Use credit card, no privacy statement. ● Consumer no longer owns information.	**Surfing** ● Technology solutions, consumer can dismantle tracking software. ● General control maintained. **Purchasing** ● Use cash (not feasible online), technology ● General control maintained.
	Yes	**Surfing** ● Able to access privacy statement, no opt-in and opt-out options, no technology solutions. ● Consumer no longer owns information. **Purchasing** ● Have to use credit card. ● Privacy statement. No opt-out. ● Consumer no longer owns information.	**Surfing** ● Able to access privacy statements. Opt-in and opt-out options, technology solutions. ● Consumer owns information. **Purchasing** ● Able to access privacy statement with opt-out option if using credit card. Ability to pay cash with opt-in option. ● Consumer owns information.

Figure. 2: Control and Knowledge of Online Surfing and Purchasing Activities [1]

Discussion

Industry Control (Industry Self-Regulation)

Many have researched the FTC's recommendation of five fair information principles as industry self-regulation practice in order to protect consumer's privacy in collection, use and dissemination.

Notice/awareness

Before information collection, merchants must provide the notice that user's information is being collected during the following process. It points out that consumers should be informed sufficient information about: who is collecting the information, what kind of information would be stored, how it would be used after collection is completed and what would happen in the future.

Choice and Consent

This term forces merchants to offer opt-in and opt-out options that would give consumer various choices to trade their information for any benefit by standing on a fair place. It includes what kind of outcome would happen regarding specific options.

Access and Participation

Individuals can access their personal information and confirm the accuracy and completeness of the information. It is essential for merchants to ensure that consumer's information is accurate and completive on behave of consumer's willingness.

Integrity and Security

The fourth principle is that merchants need to assure data quality by adopting suitable data collection methods from reliable source. Security is the key feature to protect consumer's privacy rights. Make sure users can access data correctly and prevent disclosure of it by managerial and technical measures, such as convert into anonymous formation. In the biggest hacking case in

China's Internet history, CSDN leakage, 6 million users' information was leaked and the most fatal issue was all users' information was stored in plaintext formation.

Enforcement and Redress

The absence of mechanism of enforcement would change the principles into suggestive perspective instead of practice rules. The potential enforcement consists of three aspects: self-regulation, private remedies and government enforcement. Self-regulation can be driven by consumer's awareness of privacy protection that promotes merchants to provide better service. Certification companies can be seen as an example of private remedies that, no qualification no market entry. Governments should explore existing and future regulations that can improve the industry standards [12].

Limitation of Privacy Protection

Although great effort has been taken in privacy protection, the current situation cannot meet consumer's satisfaction and there is significant limitation in privacy policy.

Merchant Issue

Anyone who ever owns a Paypal account or iTunes account should have experienced the long conditions & terms announcement while registered. It is obvious that common user would never check the list one by one before clicking confirm button. Anyone who attempts to use the service on the specific website has only one choice in fact, otherwise you cannot even access the website. Merchants usually stand in a strong position that can easily add unfair terms hiding among the long list.

In some cases, merchants would provide multi-choices that it seems like consumers have freedom of choice. For example, in payment process, the webpage lists a few online payment methods: input credit card detail, pay by Paypal account or pay by other online payment agencies. The truth is there are no significant differences between these choices, because they all need consumers to upload their bank information.

Currently, although most e-commerce websites conform to the privacy policy, such as notice and choices principles, it does not really work in practical situations. They in fact set notice barrier that makes consumers seldom check the conditions and have to take the risks of financial information leakage.

Market Burden

The privacy protection technology may set a burden for most websites who want to entry e-commerce market [13]. Information security and privacy protection need numerous resources to handle. New companies may not have enough professional personnel and financial resource at the beginning. For the limitation of consumer scale, it is not cost efficient to build up a strong and comprehensive protection mechanism. If it sets a rigorous entry barrier, the industry would create a monopolistic market and the only survivors would tend to overlook consumer's requirements.

The Balance between Usability and Privacy Security

To hold a high-level security, users may face a vast decline in user experience. In order to minimize the risk of leakage, merchants have to design protection processes to the greatest extent. When you recovery from your iCloud backup, you need to click so many "Accept" or "Confirm" buttons. If consumers attempt to change the system settings or purchase from iTunes store, they have to input the password over and over, even they typed in just a few minutes ago. In current technical condition, it seems fairly difficult to achieve the balance between user experience and privacy security.

Conclusion

As discussed in this paper, e-commerce merchants are trying to collect information from consumers through different ways in order to optimize their service, capture most consumer profit, assist for

business decisions and advertisement strategies. The risks of consumer's private information derive from inappropriate use and data leakage. By analyzing the methods of information collection, this paper focuses on the FTC industry self-regulation recommendation and principles. It develops a set of limitation of current privacy protection condition. Although merchants are using a number of methods to control and announce the information collection, the actual effect is not significant as consumers can take quite limited options. The market burden and unacceptable user experience are issues caused by rigorous privacy protection practice. Governments and merchants need to explore more effective ways to reduce the risks in online purchase and improve technical performance.

References

[1] Caudill, E. M. and P. E. Murphy (2000). "Consumer online privacy: legal and ethical issues." Journal of Public Policy & Marketing 19(1): 7-19.

[2] Demos, T. (2014). Alibaba IPO Biggest in History as Bankers Exercise 'Green Shoe' Option. The Wall Street Journal. Retrieved from http://online.wsj.com/articles/alibaba-ipo-biggest-in-history-as-bankers-exercise-green-shoe-option-1411334271

[3] Ong, J. (2012). China's Alibaba brings in a record $3.1b in sales during 24-hour e-commerce shopping frenzy. TNW. Retrieved from http://thenextweb.com/asia/2012/11/12/the-alibaba-backed-chinese-version-cyber-monday-just-brought-in-3-1b-in-e-commerce-sales/

[4] Sachs, G. (2014). B2C e-commerce as percentage of global GDP from 2009 to 2018. Statista. Retrieved from http://www.statista.com/statistics/324612/b2c-e-commerce-as-percentage-of-gdp-worldwide

[5] Kelly, E. P. and H. C. Rowland (2000). "Ethical and online privacy issues in electronic commerce." Business Horizons 43(3): 3-12.

[6] Bayan, R. (2001). "Privacy means knowing your cookies." Link-up 18: 22-23.

[7] Ackerman, M. S., et al. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. Proceedings of the 1st ACM conference on Electronic commerce, ACM.

[8] Culnan, M. J. (1993). "How Did They Get My Name": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use." Mis quarterly: 341-363.

[9] Federal Trade Commission (1999), Self-Regulation and Privacy Online: A Report to Congress, (July 27). Washington, DC: Federal Trade Commission.

[10] Warren, S. D. and L. D. Brandeis (1890). "The right to privacy." Harvard law review: 193-220.

[11] Shalhoub, Z. K. (2006). "Trust, privacy, and security in electronic business: the case of the GCC countries." Information Management & Computer Security 14(3): 270-283.

[12] Federal Trade Commission. (1998). "Privacy online: A report to Congress." Washington, DC, June: 10-11.

[13] Hinde, S. (1998). "Privacy and security—the drivers for growth of E-Commerce." Computers & Security 17(6): 475-478.