Advances in Economics, Business and Management Research, volume 68

International Symposium on Social Science and Management Innovation (SSMI 2018)

Consumer Privacy Protection of E-commerce

Guorong Zhong [1, a, *], Zhaoqing Wang [2, b]

[1]International School, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2]School of Information& Communication Engineering, Beijing Information Science& Technology University, Beijing 100101, China

[a, *] 2016213302@bupt.edu.cn, [b]mj741561@163.com

Abstract. The advent of big data is putting our society opportunities as well as challenges. In fields where, big data is widely applied nowadays, e-commerce is undoubtedly one of the most significant, however, full of uncertainties and bad effects as well. This paper will examine current situation of consumer privacy leakage in e-commerce and give corresponding scientific suggestions on both technological and legal level.

Keywords: E-commerce, privacy leakage, privacy protection technology.

1. Introduction

With the rapid development of internet technology and perfected network mechanism, society is undergoing an explosive data growth. With the era of big data approaching, the public has gradually grew an interest in the emerging and promising field of data mining and processing. Researchers begin trying to understand people's demands from the perspective of data, the mean time use data to predict new opportunities, and develop new markets in order to improve social benefits and produce greater profits. Nowadays, numerous fields are enjoying convenience thanks to big data, such as medical treatment and public transportation. Among these fields, e-commerce is one of the most vital one where big data plays a role as core driving force. However, due to the frequent leakage of personal privacy during online shopping, e-commerce platforms have an inescapable responsibility. Characteristics of users will be exposed to online merchants as soon as users' traces are left in the network. What comes next is a better adjustment in product release and its higher similarity to users' preference, which usually leads to greater economic benefits.

This paper aims to discuss the safety concerns in personal privacy information of online consumers in e-commerce. Based on the analysis of privacy protection technologies, this paper demonstrates how to strengthen the privacy protection of online consumers, and puts forward feasible suggestions on both technical and legal level.

2. Background

2.1 The Trend of Big Data in E-Commerce

The arrival of the era of big data makes our society in the face of unprecedented opportunities and challenges. On the one hand, as a powerful economic and technological entity, e-commerce is affecting the global economy. Compared with the traditional offline commerce, the larger commercial information database generated by e-commerce is operating a more highly interconnected manner through the Internet. By collecting, integrating and analyzing these data, businessmen can orientate users' needs more accurately, distinguish new business opportunities, and thus make progress in decision-making process and improve operational efficiency. In 2006, the MIT Technology Review remarked that Alibaba has become a world technology pioneer, when the double eleven global shopping carnival of the company created a dozen of new miracles in the world history of commercial industry. It is reported that during the carnival, the turnover in a single day is 120.7 billion yuan, while covering 235 countries and regions and with trading peak of 175,000 transactions per second [1]. With these statistics, it is not difficult to see that e-commerce provides an excellent stage for big data applications. On the other hand, many limitations are set to the applications of big data in e-commerce as well, among which privacy security is undoubtedly to be the biggest hinder for the

steady development of e-commerce in big data era. With the in-depth development of internet technology, the openness of big data in e-commerce is gradually enhanced while data interaction is more and more frequent. In the meantime, the risk of privacy leakage is also on the increase. Only by improving the current situation of having a lot of security risks in personal privacy and perfecting consumer privacy protection mechanism can the problem that limits the long-term development of this field be solved fundamentally.

2.2 The Traditional Consumer Personal Privacy

The concept of privacy is very extensive. To some extent, privacy is described as a multidimensional, overlap, flexible and dynamic concept, and varies in different time and circumstances in the face of various social groups. Thus, it is hardly possible to make a general definition [2][3].In a conclusion, it is widely confirmed that under the specific conditions of the big data era, the traditional definition of privacy is gradually transforming from sensitive information (such as illness, bank deposits, etc.) which is considered unwilling to be shared by individuals or groups to information that can mark personal characteristics (such as identity card number and life trajectory).

2.3 Recent Trend of Consumer Privacy Leakage

commerce is a booming field in the past resent few years as public dependence towards the internet is gradually increased. However, network privacy security situation is not optimistic in China at the present stage. CCTV "news studio" column once revealed detailed process of an online shopping fraud case involving privacy leakage of in e-commerce. According to news report, the victim received a phone call from a worker at the official mall in disguise, who gave exactly the same personal information as the victim previously offered the mall, such as article number, true name and personal phone number. Therefore, the victim was tricked to scan the fake payment code that leads to economic fraud [4]. Such cases happen endlessly, which leaves us warnings on security vulnerabilities in online shopping.

To cope with massive and frequent privacy leakage issues concerning online shopping, there are several steps we should take as solutions. Personally speaking, apart from individual awareness of privacy security being strengthened, the e-commerce companies should work hard in privacy protection technology and improve level of data security. Besides, relevant legal departments should also speed up legislation of relevant law sanctions, and enable consumers to use efficient laws against privacy violation when necessary.

3. Consumer Personal Privacy Leakage in E-commerce

The high degree of freedom and interactivity of big data result in great changes in the traditional way people make purchases. Despite bringing people great convenience, online shopping also put users' personal information in an unprecedented security crisis. Information leakage in online shopping is not individual case any longer, but a focus issue affecting the development of the entire e-commerce industry. Faced with this problem, both e-commerce platform and e-merchants have unshirkable responsibilities. To some extent, the immaturity of relevant law increases resistance for consumers to protect individual rights.

3.1 The Definition of Consumer Personal Privacy Leakage

In order to clearly understand the concept of consumer privacy leakage on e-commerce platform, we must first clarify the meaning of privacy right for any consumer involved in online shopping. Zhao Liqin has pointed out in her study that network privacy right has its own characteristics, under the premise that network service system has great liquidity and convenience in content performance, actual utility of the right is weakened in the prevention of privacy events [5]. What’s more, since the definition to network privacy differs in various countries, there is also a deviation in the emphasis to protection of privacy.

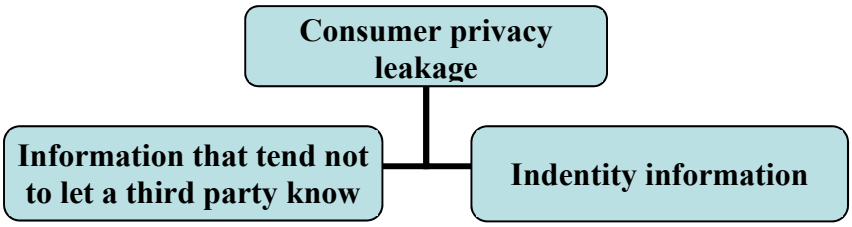

Figure 1. Computing definition of consumer privacy leakage

There are two mainstream views on consumer privacy leakage at present, as shown in Figure-1. One is described as information that a consumer is not willing to public accessed by a third party and cause material, spiritual and even reputation loss. The other is the identity information that can locate a single consumer in network, although consumers don't usually tend to hide these kinds of information. Personal information of online consumers has a wide range of meanings, including not only consumers' personal information, but also the online purchase behavior of consumers, which grants economic significance to the buying and selling of personal information. The phenomenon that some businessmen or individuals illegally collected or exchange personal information for financial interests makes serious influence on rights of online consumers and lays danger for the future [6]. To sum up, this paper's point of view on consumer privacy leakage is incidents that any information concerning consumers' identity and therefore has any economic value was inadvertently abused, maliciously stolen or illegally traded.

3.2 The Reasons of Consumer Personal Privacy Leakage

The cause of consumer privacy leakage is complex and extensive, which can be roughly classified into three classes as is shown in Figure-2, which are lack of personal information protection consciousness, impressive economic value of privacy information, and imperfection of relevant legal system. This paper holds the opinion that driven by factors given above, online merchants will make use of bias privacy policy to maximize interests of their own.

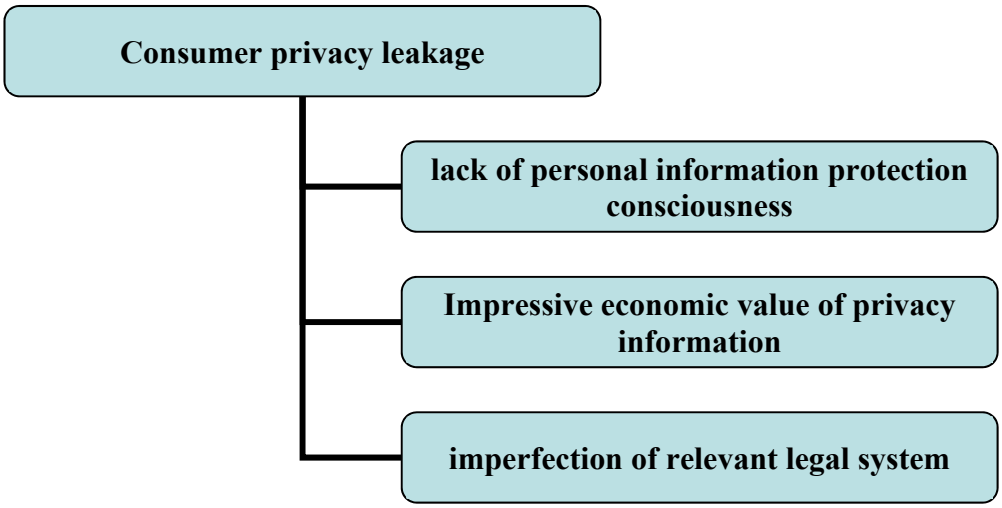

Figure 2. Reasons for consumer privacy leakage

Zhang Lei concluded through his study in 2015 that 83.5% of his respondents said they experienced troubles of privacy leakage, but only 37.6% of them took corresponding measures to protect their individual information security. Nowadays technology of dealing with big data is highly developed, especially well off when applied on e-commerce platform. However, the collection, analysis and usage process are all in the form of electric data or code and are realized in the backstage. As ordinary users of internet, it is almost impossible for us to learn about specific links and paths where this information transfers, and it's even tougher to grasp the skill to manipulate the process. Thus, it is obvious that during online purchases, online merchants have the advantage over consumers in occupying purchase information. Many online merchants find that they stand a chance to win a

profit, with the use of cookies or Trojan technology to monitor users' purchase information, while most consumers won't even know how and in which one of the several links their information is accessed. Hence, the phenomenon that puzzle terms and clauses appear unscrupulously on e-commerce platform derives. Such terms and clauses can help illegal merchants to get away from penalties the meantime benefits them greatly. Personal information was made commodity invisibly, a grey economy chain was formed in the same time as well.

3.3 Consumer Personal Privacy Leakage Would Undermine the Advantages of E-Commerce

By far, domestic or international situation of solutions to consumer privacy leakage is not considered to be optimistic. Ensuing and mounting network information leakage and fraud incidents not only causes consumers suffer different levels of spiritual and economic loss, but also fluctuates public confidence towards online shopping and brings shadow to the long-term development of e-commerce field.

Throughout the rapid development of e-commerce market, its advanced pace in multidisciplinary cooperation and technology innovation has brought the world about numerous amazing sales legend. While Chinese consumers are still immersed in the pleasure brought by rapid development of e-commerce and selectively refused to accept bad news about the platform, public concerns on privacy issues has already resulted in decreasing online shopping in the United States, where e-commerce originated from. According to a survey conducted by the ministry of commerce and the census bureau of the US, at least 45% of households have choked back an impulse of online shopping, 30% of them have already restrained an online shopping impulse in a second chance, while 26% have completely avoided online shopping[7]. In nowadays China, where e-commerce is momentum goodish, there have been many illegal merchants eyeing on consumer privacy. If the society doesn't attach great importance to the phenomenon, network information crime will become overwhelming, fundamentally undermining the foundations of the development of e-commerce in China. It follows that in China, information security issue is pretty grim and researches aiming at finding a solution are therefore impending.

4. The Analysis of Privacy Protection Mechanismin E-commerce

In the face of endless incidents involving consumer privacy leakage in online shopping, the culpable e-commerce platform and the government must take corresponding steps in the massive voice of reforms. First and foremost, e-commerce platform should focus on the technical level, actively adopt advanced privacy protection technologies in other fields, and eventually improve and build up an effective privacy protection mechanism which is suitable from its own perspectives. Secondly, from the legal level, the government should also reflect more on the lack of relevant laws and explore ways towards legislation.

4.1 Differential Privacy

Differential privacy, in the light of privacy leakage issues of statistical database, is a new concept of privacy proposed by Dwork in 2006, which is somewhere slightly different from traditional privacy definition[8]. Under the definition of differential privacy, the results of computations of data sets are insensitive to the changes of a specific record. Therefore, the risk of privacy disclosure caused by being added to a data set of a single record is controlled in a tiny and acceptable range, and therefore, the attacker will not be able to obtain accurate individual information by observing the calculation results[9].

Due to its excellent characteristics, differential privacy has emerged a lot of achievements in empirical researches in many fields, and gradually developed into an official privacy standard in many industries. Taking big companies as examples, Apple[10] announced on WWDC in 2016 that it would deploy differential privacy mechanism in iOS 10 to count Emoji usage frequency without knowing user keyboard input. In addition, Samsung and Mozilla are also working on the development and deployment of differential privacy mechanisms in their products.

4.2 K-means

K-means is a privacy protection technology which is like differential privacy in its principle, aiming to realize data sharing while perfectly protect user privacy. Privacy protection objects in the process of data publishing with k-means technology are mainly the individual user and the corresponding relationship between user and identity sensitive data. Traditional privacy protecting method of deleting identifiers cannot fundamentally prevent privacy disclosure. Attackers can still link the published data obtained from other channels through chain attacks, to infer privacy data and locate individuals. K-means algorithm refers to the technology of generalization (more generalization and abstraction of data) and concealment (not publishing some data items) to publish data with low precision, so that each record has the same identifier attribute value as other k-1 records in the same database, thus reducing the link attack.

So far, the application direction of k-means technology is mainly consisting of data publishing privacy protection and location service privacy protection. The applied occasions cover census, medical and social services data publishing and financial data sharing [11]. According to the definition of consumer privacy in e-commerce given above, k-means technology has a promising future in the field.

4.3 GDPR in Legal Level

With the rapid development of big data, radical changes have taken place in society, and e-commerce has emerged as the times require. Online merchants can collect and process data in a more extensive way, and are increasingly eager to use these data for various purposes, such as personalized services and marketing, which makes it more difficult to protect personal privacy information at the legal level. Although the personal information protection law has long been on the legislative agenda of China, it has not yet been promulgated due to its complexity, which results in victims of privacy leakage incidents in e-commerce of the country often suffer losses when they resort to law.

By comparison, in May 2016, the new General Data Protection Ordinance (GDPR), which was passed by the European parliament, has a strong practical significance in the protection issue of e-commerce in China. GDPR is conducted to more vigorously suppress the abuse of personal information and strengthen the privacy protection efforts [12]. According to GDPR, enterprises should obtain the users' consent in any behavior involving the usage of personal information, which means users have absolute control over their personal data. As far as I am concerned, normative systems and a more detailed legal process should be established with lessons from GDPR performances in China, in order to achieve a highly matured privacy protection legal mechanism.

5. Conclusion

The information society is experiencing a violent wave of data convenience and privacy crisis in the era of big data nowadays. With the development of mobile internet data processing technology, the increasingly serious privacy leakage phenomenon has become a major malady profoundly affecting the long-term and steady development the times. From the perspective of current situation of consumer privacy protection in e-commerce, this paper tries in discussing the issue of consumer privacy protection in manners as follow.

Summarize the concept of online consumer information privacy and online consumer privacy leakage from domestic and foreign literatures and then analyzes the cause and effect in current situation of consumer privacy protection in e-commerce as well as expectations of future improvement.

Based on existing researches on the theory of several privacy protection technologies and their application instances, put forward a new idea of introducing advanced privacy protection technologies such as differential privacy and k-means technology into the field of consumer privacy protection in e-commerce. It is without doubt that as one of the focus areas in data mining and processing, e-commerce platform desperately needs an indispensable driving force that do go to its further development by applying new concepts and introducing new technologies.

References

[1]. Sohu News. http://www.sohu.com/a/119101428_197955.

[2]. Liu Yahui, Zhang Tieying, Jin xiaolong, Cheng Xueqi. Personal privacy protection in the era of big data. Computer research and development. 2015,52(1) :229-247.

[3]. Wu Xiaotong. Research on Privacy Protection and Key Technologies in Large Data Environment. Big Data and Privacy Protection, 2017.

[4]. CCTVnews.http://tv.cntv.cn/video/C10616/74beb00c630a41b0acdb2f82b5b1f0a7.

[5]. Zhao Liqin. The Definition of Consumer's Privacy Right and the Construction of Protection System in the Process of Online Purchase. 2014.

[6]. Zhang Lei. Research on Prevention and Protection of Personal Information Leakage in Online Purchase. Information management. 2015.

[7]. Sohu News. Shi Gaotao: Information insecurity may affect the development of e-commerce. http://www.sohu.com/a/100088186_237335.

[8]. C. Dwork, F. Mcsherry, K. Nissim, A. Smith. Calibrating noise to sensitivity in private data analysis, in Proceedings of Theory of Cryptography, Springer, 2006: 265-284.

[9]. Xiong Ping, Zhu Tianqing, Wang Xiaofeng. Differential privacy protection and its application. Journal of computer science, January 2014, volume 37, issue 1.

[10]. Apple Differential Privacy Team, “Learning with privacy at scale,” Apple Machine Learning Journal, vol. 1, 8 Dec. 2017.

[11]. Sun Guangzhong, Wei shen, Xie Xing, De-anonymization technology and its application in the era of big data. Research and Development.

[12]. Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula. EU General Data Protection Regulation Changes and implications for personal data collecting companies. computer law & security review 34 (2018) 134–153.