CSCanada
Management Science and Engineering
Vol. 9, No. 4, 2015, pp. 64-67
DOI:10.3968/7945

ISSN 1913-0341 [Print]
ISSN 1913-035X [Online]
www.cscanada.net
www.cscanada.org

Personal Privacy Security Management in the Era of Big Data

HUO Zhenggang[a]; HE Haibo[b],*; WANG Ruifang[a]

[a]College of Civil Science and Engineering of Yangzhou University, Yangzhou, China.
[b]Information Engineering College of Yangzhou University, Yangzhou, China.
*Corresponding author.

Received 15 August 2015; accepted 19 November 2015
Published online 16 December 2015

Abstract

Big Data has brought new opportunities for development, but personal privacy security is facing new challenges. The characteristics of Big Data determine that the way of individual privacy which is collected, analyzed, managed, stored and distributed data in the large data ecosystem. Under the momentum of rapid development of Big Data, through individuals, enterprises and related policies and regulations of the multi-pronged approach to solve security problems, personal privacy.

Key words: Big Data; Personal privacy; Privacy security

Huo, Z. G., He, H. B., & Wang, R. F. (2015). Personal Privacy Security Management in the Era of Big Data. *Management Science and Engineering*, *9*(4), 64-67. Available from: URL: http://www.cscanada.net/index.php/mse/article/view/7945
DOI: http://dx.doi.org/10.3968/7945

INTRODUCTION

At present, the rapid development of information and network makes the Big Data become the hot research in the academia and industry, and the Internet industry is undergoing profound technological change. With the continuous development of science and information technology, social networks, cloud computing, networking and other new technologies and services are emerging as well as being applied, which leads to a large amount of data. These have produced a large amount of data. Their variety is increasing and the size of the data has also increased dramatically, which means that the era of Big Data has arrived.

Big Data has great commercial value, through the Big Data mining analysis, the enterprise can get great economic value and benefit. With the development of Big Data technology, enterprises can collect, store, analyze and sum up the data of individual and user in the cased of a person unable to control or unaware, aim to dig out potential patterns. Research on the regular pattern and development trend of individual and social movement, which can help companies, businesses adjust market policies, reduce risk, rational face of the market to make a decision. However, without the user's permission to access data behavior, which greatly violated the privacy of individuals. At present, people pay more and more attention to the problem of privacy protection, privacy issues have attracted wide attention of various countries and individuals, the government, enterprises in the privacy protection is being carried out some new practice and exploration. So, the era of Big Data, how should we protect the privacy of individuals?

1. PERSONALPRIVACYISSUESINTHE ERAOFBIGDATA

1.1 The Concept and Application of Big Data

1.1.1 The Concept of Big Data

At present, there's not a unified concept of "Big Data". The first Big Data era of Agency is the world's leading consulting firms McKinsey. However, it's widely believed that Big Data is the huge database, referring to valuable information which can help enterprises operate and decide, but can't be captured, managed, processed and digested manually or by mainstream software in a reasonable time frame. The following is four features of Big Data: volume, variety, velocity, value and online

1.2 The Application of Big Data

Current data analysis has been applied in various fields such as science, medicine, business, and their use have great differences. But its objectives can be summarized as follows:

(a) Access to knowledge and speculation trends. Data analysis has been carried out for a long time. The first and most important purpose is to obtain knowledge and use knowledge. Because of the Big Data contains a large number of original and true information, through data analysis can effectively abandon individual differences, so as to help people through the phenomenon, more accurately grasp the rules of things behind. Based on the mining knowledge, it is more accurate to predict the natural or social phenomena.

(b) Analyze and grasp the characteristics of the individual. Individual activities meet certain group characteristics at the same time, also have some distinct personality characteristics. The tail as the “long tail theory” in the long way, these characteristics may differ in thousands of ways. Through long time, multi-dimensional data accumulation, it can analyze the user’s behavior rule, and more accurately depict the individual profile, to provide users with better personalized products and services, as well as more accurate advertising recommendation. For example, Google analysis the user’s habits and preferences through its Big Data products, to help advertisers evaluate the efficiency of advertising, will estimate in the future there may be up to hundreds of billions of dollars of market size.

(c) Analysis and identification of the truth. The error message is less than that without information, due to the spread of information on the Internet more convenient, so the damage caused by the false information network is greater. Due to the large diversity and a wide range of data sources, to a certain extent, it can help to discard the false and retain the true information. At present, people began to try to identify false information by using Big Data. For example, the social comment website Yelp through using Big Data to filter false comments, in order to provide users with a more realistic comments; Big Data analysis techniques to filter spam by Yahoo and Think mail etc..

1.3 Personal Privacy Challenges in Big Data

The Internet has become a part of our lives, leaving us to visit the major sites of data footprint. In the Big Data environment, this makes our privacy leaks become easier, we are exposed in the “third eyes”, such as Taobao, Amazon, JD and other major shopping sites are monitoring our shopping habits; Baidu, Bing, Google and other monitoring our query record; QQ, Microblogging, phone records and other eavesdropping our social relations network; surveillance system to monitor our E-mail, chat, Internet records, etc..

In the era of Big Data, the collection of personal information is more convenient, more comprehensive, not only including relevant data like citizenship, but also further include financial transaction class data such as citizens consumption and daily business activities、social networking issued various statements and other interactive class data, interpersonal class data based on the network social, Through integrating all kinds of data, it can be done to achieve a comprehensive and accurate reduction of personal life, and then to predict the full picture of the social situation, and ultimately produce unimaginable huge economic benefits.

1.4 Personal Privacy Security Issues

With the development of information technology, information has gradually become a commodity, it can be collected and stored in the database equipment for others to pay or free use. For example, information about the residents gathered by the government departments, such as the motor vehicle management department in the process of issuing licenses to the driver’s name, age, home address, occupation, etc.. Although according to law to collect all kinds of personal data, but the information security is not sufficient security, there is a systemic risk, it is difficult to avoid information leakage. And some hidden in the enterprise internal staff or external hackers is often illegal to steal massive personal information, and illegal to sell to some bad information intermediaries, and spread to the survey firm, sales companies, network crime groups, etc.. The use of large data integration information, to take data mining, can be legitimate for the majority of customers precise marketing, to achieve effective customer management, but inevitably encounter illegal identity theft, suffered financial fraud. This information is very easy to collect and deal, and finally sold to some conduit company, marketing companies. But with a large amount of personal information has become more transparent, so that the personal safety of the damage, so as to bring significant harm to personal personality.

Therefore, privacy security is the biggest threat to the security of personal information security in the era of Big Data, but also the biggest obstacle to restrict the development of Big Data. In data collection and data analysis, processing and data destruction process, will touch the user’s personal privacy. People’s personal identity information, as well as people on the Internet all kinds of behavior, without any prompting by site storage, use, or even leaked, which is the main problem of the Internet in the privacy of individuals.

2. PERSONAL DATA PRIVACY VIOLATIONS IN THE ERA OF THE TIMES

2.1 Invasion of Privacy in the Process of Data Acquisition

The concept of Big Data is accompanied with the development of Internet technology, the data acquisition method is mainly through computer networks, mobile internet. Users use in the Internet every time of the process, the behavior will be recorded in the cloud server on the record, especially in the background of today's internet mobile and Internet smart phone, we are connected with the network at all times, and we are all the time by network records, these records are stored on the formation of a huge database. From the whole process, we are not difficult to find that the acquisition of large data is not through the user's license, but secretly behavior. A lot of users do not want to have the behavior of the data generated by the Internet service providers, but cannot stop. Therefore, this is not the user's consent to collect user data behavior itself is a violation of personal privacy.

2.2 Invasion of Privacy in the Process of Data Storage

Internet operators tend to put their collection of data on the cloud server, and the use of a large number of information technology to protect these data. But at the same time, due to the failure of infrastructure and encryption measures, it will produce a new risk. Massive data storage requires strict access control and identity authentication management, but the cloud server and the Internet makes this management difficult to increase, account hijacking, attack, identity forgery, authentication failure, key loss and other potential threats to user data security. In recent years, driven by the interests of large data, many network hackers targeted internet operators, making the user data leakage incidents occur, a large amount of data is stolen by hackers through technical means, to bring huge losses to the user, and a great threat to personal information security.

2.3 Invasion of Privacy in Data Use

In recent years, due to the rapid rise of online shopping in China, the user through the Internet shopping has become a new fashion and a choice of many people. But at the same time the network shopping involves a lot of user privacy information, such as real name, ID number, address, contact phone number, and even the user's shopping list itself is stored in the electricity business cloud server, so the electricity suppliers become the largest storage of large data, but also the biggest beneficiary. Electricity suppliers through the user's past consumption records and it have similar consumer records user's cross analysis can predict your interest, or your next time buy goods, so as to put these items of advertising to promote the user's purchase, no wonder netizens joked that now most people who understand you is not your own, but electricity suppliers". Of course, we cannot deny that the use of Big Data for the benefits of life, but also it has to admit that in the presence of ordinary users before the electricity business has no privacy. When users want to protect their privacy, will find it has been quite difficult to exercise their right to privacy.

2.4 Invasion of Privacy in the Process of Data Destruction

Due to the low cost of digital information is easy to copy the characteristics, resulting in large data once it is difficult to complete the removal of the operation is completely destroyed, it will be a long process of user privacy violations. When the user's behavior is digitized and stored, even if the Internet service provider committed to the destruction of these data after a certain period of time, but the actual destruction is not complete, and it meet the requirements of law enforcement, national laws will usually provide a period of large data storage, and mandatory Internet operators provide the required data, public rights and privacy conflicts are also a threat to the security of personal information.

Therefore, in the era of Big Data, the protection of privacy information in the data has a unique significance, the traditional privacy protection theory and technology has been unable to cover the content of Big Data privacy, it is necessary to re think and locate the problem of large data privacy protection. According to the privacy of the personal privacy in the Big Data ecosystem, this paper makes some corresponding measures from the technical and legal aspects of security awareness, and thus provides a safe protection for personal privacy under the background of Big Data.

3. BIGDATAPERSONALPRIVACYSECURITYPROTECTION

3.1 Personal Privacy Technology Protection

The existing privacy protection technology is mainly divided into 3 categories: data perturbation technology, data encryption technology and data anonymity technology. Personal privacy data experiences collected, stored and used process (use include the use of data for the two time, data sharing and data distribution), so it should implement multi-level security data protection, this paper which combines the characteristics of Big Data from the data layer, application layer and data presentation layer describes personal privacy protection technology and related work.

3.1.1 Personal Privacy Protection of Data Layer

The data in the communication can be used in SSL protocol to ensure data security. Therefore, the data protection of the data layer mainly refers to the storage and management of data. To ensure the security of the data layer personal information is the basis of all other applications based on data, including the confidentiality, integrity and availability of the data. It consists mainly of personal privacy protection of data encryption, personal privacy protection of the database, privacy protection of personal privacy in the cloud storage, and data tracing technology.

3.1.2 The Protection of Personal Privacy in Application Layer

For the large data applications, the research of the corresponding personal privacy protection technology is more practical and meets the practical needs of the specific application for the enterprise. This paper mainly describes the technical method of personal privacy protection by popular applications of the Big Data era, 3 aspects of online social networks, mobile positioning and RFID technology. It consists mainly of online social network privacy, mobile location privacy protection, RFID security and privacy.

3.1.3 The Protection of Personal Privacy Data Released

Governments, businesses and individuals can analyze the collected data, thereby enhancing services or making decisions, driven by the interests, they need to share or publish some data. If the publisher publishes data without considering privacy protection, it will cause the serious consequences of economic or reputation losses for enterprises. Therefore, the challenge is to data release to ensure that the data can not only ensure that the personal privacy information is not compromised, but also to maximize the effectiveness of publishing data. It consists mainly of the personal privacy protection of anonymous method, PPDM data release, differential privacy protection, personal privacy protection of data access control, personal privacy protection assessment of data release.

3.1.4 The Identity Authentication Technology

The technology through the data acquisition and analysis of user behavior and use of equipment, access to the behavior characteristics of the user and application device, which can be verified by using the information on the behavior of the operator and the use of equipment to determine its identity. The use of identity authentication technology increases the difficulty of the hacker's attack, reduces the burden of the user and unify the authentication mechanism for different systems.

3.2 Personal Privacy Law Protection

Personal privacy protection is a complex social problem, in addition to the protection of advanced technology, but also the needs of the industry norms combined with relevant policies and regulations formulated by the state and industry to protect personal privacy, ensure that individuals from threats to personal safety and property loss. However, in the Big Data era, the original standard has been unable to meet the needs of the protection of personal privacy, not enough to risk which is caused by the suppression of Big Data, therefore, it no longer apply these rules, need to redefine the rules to meet the needs of the present.

3.2.1 Build Personal Privacy Data Protection Law

In the era of Big Data, the use of technical means to protect personal privacy is not enough, it cannot replace the legal system. The laws and regulations and the basic rules of the personal privacy protection we must establish, and increase efforts to crack down on violations of personal privacy behavior.

3.2.2 Establish Personal Privacy Protection Industry Standard

The customer is the source of enterprise benefit. the enterprise is in compliance with the "personal privacy data protection law" at the same time, it should also comply with the relevant industry standards according to the application demand of the enterprise, to avoid the potential loss of interest and attract more customers.

CONCLUSION

The protection of personal information security consciousness should be strengthened. One of the most important aspects of protecting personal privacy is the participants themselves. As Internet users, we should have the ability to identify the information. In the face of every kind of registered website, we should first consider the security of the website; then determine what information is not needed to fill out the real information; finally decide whether to register the site. In addition, we need to clean up the Internet traces in a timely manner, to remove personal information; we usually pay more attention to information security issues, to grasp the solution. Information security related to their own interests, everyone should hold enough attention to view personal privacy, focus on the protection of personal privacy.

REFERENCES

Campan, A., & Marius, T. T. (2008). *Data and structural k-anonymity in social networks*//Proceedings of the 2ndACM SIGKDD International Workshop (PinKDD2008) (pp.1-10). Las Vegas, USA.

Li, G. J., & Cheng, X. Q. (2012). Research status and scientific thinking of big data. *Bulletin of Chinese Academy of Sciences, 27*(6), 647-657.

Mayer-Schonberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work and think.* Boston: Houghton Mifflin Harcourt.

Men,g X. F., & Ci, X. (2013). Big data—management: Concepts, techniques and challenges. *Journal of Computer Research and Development, 50*(1), 146-169.

Sweeney, L. (2002). K-anonymity: A model for protecting privacy. International Journal on Uncertainty. *Fuzziness and Knowledge based Systems, 10*(5), 557-570.

Sweeney, L. (2002) k-anonymity: Achieving k-anonymity privacy protection using generalization and suppression. *International Journal on Uncertainty, Fuzziness and Knowledge Based Systems, 10*(5), 571-588.

Wybourne, M. N., Austin, M. F., & Palmer, C. C. (2009). *National cybersecurity research and development challenges*. Institute for Information Infrastructure Protection. Retrieved from http://www.thei3p.org/docs/publications/i3pnational cybersecurity.pdf

Zheng, J., et al. (2011). *On the ethics of the network society* (p.22, 55). Beijing: China Social Sciences Press.