IMPACT: Journal of Business Information Systems and Technology (IMPACT: JBIST)
Vol. 1, Issue 1, Jun 2017, 7-18

THE ANALYSIS BASED ON BIG DATA FOR THE ENTERPRISE ETHICS & NETWORK GOVERNANCE

TANG SHAOQING[1] & GUO YIJING[2]

[1]Business College of Beijing, Union University, China

[2]Department of organization & Propaganda, Business College of Beijing, Union University, China

ABSTRACT

Background and Goals

Big Data have deeply influenced the People's Daily life style, work habits and thinking patterns. But the collection, storage and using process of Big Data are facing many security risks and also the false data will lead to wrong or invalid data analysis results.

Methods

This paper expounds the importance of users' privacy in using big data in China, and discusses the related concepts and problems of the network ethics and network governance, and put forward the "privacy" protection mechanism.

Conclusions

The current research on large data security and privacy protection is not enough both in China and abroad. The better way to solve the problem of large data security and privacy protection needs the combination of technical means and related policies and regulations. Enterprises need to strengthen self management and ethical constraints, while users need to raise awareness and abilities of privacy protection as well. That is to say to build up the "privacy" protection mechanism as follow: "self-discipline by enterprises, proactive governmental supervision, self-protection by users" and the effective effective credit network system.

KEYWORDS: Big Data, Enterprise Ethics, Network Governance

INTRODUCTION

China's internet companies have begun to enter the field of large data since 2008. They obtain the user's information resources and habits preferences by analyzing the user's registration information, consuming records, browsing records, using preferences and so on. When users are checking the map, finding a restaurant, watching videos, or shopping online, web sites and software automatically collect data timely and do real-time data processing, in order to recommend similar or related services and information to users who may interesting in. In the future, with the development of large data technology from behavioral analysis to identity authentication, commercial advertising will also achieve "cross screen marketing". Therefore, the security and privacy issues caused by the development of large data have become a hot topic, which led to the thinking about enterprise ethics and network governance. In fact, the meaning of big data security is more extensive. Besides the leak of personal privacy, people are facing lots of security risks in big data storage, processing and

transmission. It is essential to protect data security and personal privacy. But in fact, the big data security and privacy protection are more serious and difficult than other security issues (such as cloud computing and others) in the past. In the context of large data, businesses, such as Facebook, are not only the data producer, but also the one that store, manage and use the data. Therefore, it is very difficult to protect users' privacy, simply by limiting the use of users' information through technical means. There is no doubt that the constraints by corporate ethics and self-management, as well as the government's network governance are necessary.

HOW THE ISSUE BE PUT FORWARD

With the rapid development of information and network, especially the idea of "Internet plus", the growth of data is very quick. According to statistics[1], an average of 2 million users per second are in the use of Google search, Facebook users share more than 4 billion things per day, Twitter handle more than 34 billion the number of tweets per day. At the same time, scientific computing, health care, finance, retail and other retailer industries also have a lot of data in the continuous production. In 2012, global information has reached 2.7ZB, and this figure is expected to reach 8ZB in 2015. At present, big data has become another growth point after cloud computing in the field of IT. According to Gartner forecast, in 2013, the big data will cost $34 billion in IT field globally and the total cost of the world's big data will reach $232 billion in 2016. According to the digital universe research report of International Data Corporation (IDC), in 2011, the total amount of data that was created and copied is more than 1.8ZB and the grow thing trend follows the new Moore's law. That is to say, the global data volume doubles every two years, which is expected to reach to 35ZB in 2020. Meanwhile, the complexity of Data is also growing rapidly, and its diversity, real-time and other complex characteristics are increasingly obvious.

The rapid development of network technology has brought profound and significant social changes in the political, economic, cultural, educational, scientific and technological fields, and has changed people's living style. Therefore, network also has broken the limits of time and space, in spite of bring prosperity and convenience to mankind. It makes all social and personal activities public and the civilization of mankind faced with a deprived naked feeling. That is the reason why network privacy, business ethics and related issues have be paid more and more attention to, and become a new hot topic of interest in the academic circles.

A REVIEW OF THE RESEARCH ON LARGE DATA PRIVACY

Concept & Characteristics of Big Data

What's big data? ? There has not yet a recognized accurate definition by enterprises and the academic communities. Wikipedia defines the big data as the data that could not be grasped, managed and processed with the conventional software tools in a certain period of time.

Net App Company thinks[2] that big data should include A, B, C three elements: analysis, bandwidth, and content. Authoritative IT research and consulting company Gartner defined the big data as: extreme information management and processing in one or more dimensions that is beyond the processing power of traditional information technology. U.S. National Science Foundation (NSF) defined the big data as: large-scale, diverse, complex, long-term distributed data generated by scientific instruments, sensing devices, internet transactions, e-mail, audio and video software, network click stream and other various sources. Although there are different expressions, there is a common

point of view as that There is similarity between the concept of big data and “massive data”, “massive data”, but it has been greatly beyond the traditional data in the data volume, complexity and speed and beyond the existing technical means of processing capacity too.

To sum up, big data refers to the large scale and complex types of data, so that it is difficult to use the existing database management tools or data processing applications to deal with. Big data has three main features, includes volume, velocity and variety. Big data can be divided into the following three categories according to the different sources:

1. Data from human: kinds of data generated by people’s online activities, which includes text, pictures, video and other digital information; 2. Data from computer: data generated by different types of computer systems, in the form of documents, databases, multimedia, etc. which also includes log, audit and other automatically generated information; 3. Data from the object: data collected by various digital devices, such as the digital signal generated by the camera, the various features of the human generated in the medical internet of things, and a large number of data generated by the astronomical telescope.

A Review of the Research on Big Data

Big data is once again a disruptive technological change in the IT industry. It will have a great impact on the concept of the management of modern enterprises, organizational business processes, marketing decisions, as well as consumer behavior patterns and so on, which makes the business managemental decisions more and more dependent on data analysis rather than experiences or intuition.

The domestic and foreign well-known enterprises, such as Ebay, Amazon, Wal-Mart, Taobao, China Mobile and VANCL etc., have launched the corresponding large data products and platforms, and carry out a variety of business analysis and application. From the perspective of management, the application of big data technology to support business analysis and decision-making has become a hot direction of the business school education. Data driven financial, strategy, marketing and operational management research and practice guidance will become the focus of future business schools.

In 2008, R.E.Bryant from Carnegie Mellon University in the United States, R.H.Katz from University of California, Berkeley, E.D.Lazowska from University of Washington, rely on the Computing Community Consortium, published the white book “big data computing: Science, business, and social revolutionary breakthroughs”. The researchers and industry executives are aware of the new uses and insights of big data. Subsequently, EMC, IBM, HP, Microsoft and other global well-known companies have adopted the acquisition of large data related vendors to achieve technical integration and implement their big data strategy. Domestic and international advisory bodies have also released big data related research reports, and actively follow up research and development and application in the field of big data. May 2011, EMC made a special lecture “When Cloud Computing Encounter Big Data”, in World EMC 2011 conference, which described the concept and technical development trends of cloud computing and big data. In October 2011, Gartner listed big data into the ten major strategic emerging technologies in 2012. In November, China's big data technology conference hosted by CSDN held in Beijing successfully. Big data industry gradually formed a new trend of development. In March 2012, the U.S. government invested $200 million into “big data research and development program”. In April 2012, the United Kingdom, the United States, Germany, Finland and Australia researchers jointly launched “the world's big data week campaign”, that is designed to promote the government to develop a strategic big data measures. In July 2012, Japan launched “the new ICT strategic research program”. Most of the existing big data researches are based on the

information science, focusing on the acquisition, storage, processing, mining and information security of big data. There are fewer researches that based on the changes and impacts of the big data for the production management and business operation of the modern enterprise from the point of view of management. There lacks the analysis and research on value creation of socialization, the network of enterprises operation and the real time market observation.

Application & Development of Big Data

The big data mining and application in marketing, sales, human resources, e-commerce and other business areas have been widely carried out, and have achieved remarkable results. From this point of view, big data marks the data-oriented research and application has gone through the initial stage, into a mature and deepening new era. Enterprises obtain a trillion bytes of information about consumer, supplier and operations management from the constantly generated transaction data. Millions of network sensors are implanted into mobile phones, smart meters, cars and machinery and other devices to sense, create and exchange data. Real-time communication and content sharing from hundreds of millions of Internet users in social media play a key role in exponential growth of big data. Big data can be applied to various fields like science, medicine and business, etc. With the “internet plus” mode, it can be used in following three aspects:

- To obtain objective knowledge and forecast the development trend. The first and most important purpose of data analysis is to obtain and take use of knowledge. Because the big data contains a large amount of original, real information, big data analysis can effectively abandon the individual differences and more accurately grasp the essence of rule through the phenomenon. Based on the knowledge and characteristics, it can predict the natural or social phenomenon more objectively and accurately. Google Flu Trends website is a typical case. It released the world's influenza situation analysis and prediction through the statistical information searched by people and the source of the search determined by querying Google server log IP address.
- To analysis individual data and master personalized features. When individual activities meet the characteristics of certain groups, it also has a distinctive personality characteristic. These characteristics may vary widely as in the “long tail theory”. Enterprises can analyze users’ behavior through a long multi-dimension data accumulation, and depict the outline of the individual more accurately, which helped to provide better personalized products, services and more accurate advertising recommendation to users. Enterprises as Jing Dong and Tao Bao did personalized analysis for the user's habits and preferences through its big data products to help advertisers to assess the efficiency of advertising activities and forecast market scale in the future.
- Truth identification through data analysis. No information is better than wrong information. As the spread of information is more convenient by internet, so the false information may cause greater harm. For example, in April 24, 2013, the Associated Press Twitter released the false news that President Obama suffered terrorist attacks because the account was theft. Although the false news was banned in a few minutes, it still led to a brief dive in the U.S. stock market. Due to a wide range of data sources and its diversity, to a certain extent, it can help to distinguish true information. At present, people began to try to identify false information using big data. For example, Social site Yelp uses big data to filter false comments and provide more authentic comments to users. Yahoo and Think mail filter spam using big data analysis techniques.

IMPORTANCE ANALYSIS ON BIG DATA "PRIVACY"

According to Wikibon's research report, in 2013 the size of world's big data market is about $18.1 billion which has an increase of 61% than in 2012. And it is expected to keep the growth of 30% per year in 2017. It is also expected that the total amount of data in China in 2020 will reach 8.4ZB (1ZB =1024GB4) that accounts for 24% of the global data, which will surely become the world's first data power and the "world data center".

The Concept and Characteristics of Privacy

Privacy [3] is sensitive personal information that does not want to be disclosed. Banisar et al. divided personal privacy into four categories:

- Information Privacy. Information privacy means personal data management and use, which includes the identity card number, bank account, income and property status, marriage and family members, medical records, consumption and demand information (such as shopping; buy a house, a car or insurance), network activity traces (such as IP address, browsing traces, activities) etc.
- Communication Privacy. Communication privacy refers to communication information through various ways of communicating, which includes telephoning, QQ, E-mail, We Chat, etc.
- Space Privacy. Space privacy refers to information in specific space or area that people access, which includes home address, work units, and public places.
- Body Privacy. Body privacy means the protection of the integrity of body that to prevent invasive operations, such as drug testing, etc.

Personal privacy mentioned in this paper, refers to personal information in private life that not be willingful to be known by others, such as those sensitive information including user's identity, track, position and so on. The scope of privacy includes personal information, activities and space. Network privacy is the extension of privacy right in the network. It refers to the rights that personal life, information, and activities should be protected by law, and should not be infringed, known, collected, copied, used and disclosed by others. It also refers to forbidd to reveal sensitive personal information on the internet, including the facts, images and the opinions of the smear. In November 26, 2013, the United Nations adopted the resolution for protection of network privacy launched by Brazil, Germany.

Commercialization and Openness of Personal "Privacy" By Big Data

In 2014, during the "double 12" period, Jing Dong, Tao Bao, and other shopping sites provide many similar goods on the bottom of the page as "you may need" column when you search for items, which makes consumers facing a variety of choices that are difficult to choice. Online consumers worried about the commercialization and openness of personal "privacy" as "big data may lead to meaningless buy" and "It's affecting my decision and I feel like I'm losing my freedom."

Under the influence of the herd mentality, consumers will think that the majority of people's choice is reasonable and correct, for which their shopping decisions are easily be controlled. Compared with the traditional operation mode, the network platform greatly enhanced the influence and control on users through the big data computing and its analysis result. Consumers sometimes really do not know it is their own choice, or the choice of large data. The less you cannot do

without big data, the more deeply you are controled by it.

The Dilemma of Personal Privacy and Security Protection

With the coming of big data era, data collection and storage are more convenient. But users cannot determine the use of their own privacy information because the lack of standardization and regulation and the reling on corporate self-discipline. In October 2013, A report released by the domestic vulnerability monitoring platform “clouds” said that the check-in records of 20 million customers in Home Inn and Hanting hotel were compromised due to the existing third party storage and system vulnerabilities. In May 2014, user database of MIUI forum was spreaded in the hacker community, which caused worries to a large number of fans of MIUI. In January 2015, the personal information of 1.3 million candidates who participate in the examination of postgraduate was sold at the price of 15 thousands. Lots of facts as above showed that the essence of big data era is a battle between the businesses and between individuals and the businesses.

At about 17:30 of May 27, 2015, due to the network failure, the payment account of Alipay are unable to login. Alipay's official response explained it is due to the fiber broken in Xiaoshan District of Hangzhou, and they will switch users’ requests in emergency to other computer-room. Although Alipay stated that the user's financial security will not be affected, but the users are still worried due to the undisplayed account balance. After that, in the morning of May 28th, the Ctrip's official website and app suddenly collapsed and the page reported the wrong code 404. Although Ctrip responded that it is because some of its servers suffered unknown attacks and the data is not lost, users are also worried about the potential risks of users’ information leakage.

The big data will be related to the user's personal and property security in the future, it is necessary to publish relevant law to clearify the rights and ways to use personal data by enterprises, and establish mechanism for rights safeguarding to information disclosure, and gradually improve a set of data security system that linked up multiple aspects as law, technology, management, application and development.

Absence of Legislation for Privacy Protection by Big Data

A large number of facts show that big data will cause great harm to the user's privacy if it is not be properly handled. According to the difference of the content that needs to protect, privacy protection can be further divided into location privacy protection, identifier anonymity protection, connection relationship anonymous protection and so on. The threat people faced with is not limited any to personal privacy leak, but also lies in the people's status and behavior prediction based on big data. A typical example is that a retailer knows that a woman has been pregnant through her historical records even early than her parents and mails her related advertisement. And research on social network analysis also shows that users’ attributes can be found through the group characteristics of big data. For example, users' political leanings, consumption habits and preferences for which sport team can be found through the analysis of their Twitter messages.

Some enterprises often think that the information that does not contain the user's identifier after an anonymous process can be published. But in fact, it cannot achieve the goal of privacy protection only through anonymous protection. For example, AOL has announced parts of searching history after be anonymously processed for three months for people to analyze and use. Although personally relevant identification information is carefully handled, some records can also be accurately positioned to specific individuals. The New York Times immediately announced a user that was recognized,

the user NO. 4417749 is a widowed woman who raised 3 dogs and is suffering from a certain disease. The users' privacy protection in China should be the same, or similar.

At present, China's user data protection mainly relies on the self-discipline by enterprises due to the lack of regulations and supervises for data collection, storage, management and use. In the commercial area, users should have the right to decide how their information is used in order to achieve the controllable privacy protection by users. For example, the user should be able to decide when and how their information to be disclosed and when to be destroyed. Such rights includes:

- Privacy protection in the process of data acquisition, such as data accuracy.
- Privacy protection in the process of data sharing and publish, such as the anonymous. Processing, artificial interference, etc.
- Privacy protection in the process of data analysis.
- Privacy protection for life cycle of data. (5) Privacy data destruction that can be trusted.

But the fact is that users could not know all these above. Furthermore, even if they knows these above, they are still in disadvantage and unable to protect their legitimate rights and interests without the related laws and regulations.

Harms of Personal Privacy Leakage

The frequent occurrences of personal privacy leak are a threat to personal safety and even the major factors that affected the public security. According to the statistics of Beijing Zhongguancun police station, in 2012, the annual report of telecommunications fraud accounted for 32% of the filing, which are the highest proportion in all case types. Six means are often used in fraud:

(1) To pose as public security organs, postal services, telecommunications, banking, social security staff or relatives to commit fraud after the disclosure of information from individual or friends circle; (2) To pose as sellers to fraud after the disclosure of shopping information, this accounted for 42% of the filing; (3) The winning fraud after the disclosure of communication information, such as phone, QQ or mail; (4) False recruitment information after the job-hunting information leaked; (5) Online dating fraud after dating information leaked; (6) Kidnapping fraud after family information disclosure.

Thus, many companies, in varying degrees, are disclosing the users' personal information.

Personal privacy information leakage caused panic, some users fear that the privacy data is lost or malicious theft. A public opinion survey report shows that 72% people are worrying about their online behavior being tracked and analyzed by the company. As a result, most people raise the awareness of privacy protection, but many companies do not pay enough attention to the user's privacy protection which caused the loss of potential customers and economic benefits.

Analysis on Dishonesty of Big data

Information security is related to the credibility of the data analysis, that is, "dishonesty" analysis. A common view for big data is that data themselves can explain everything and the data itself is the fact. But in fact, if it is not been carefully screened, the data will deceive, which likes that people sometimes are deceived by their own eyes.

One threat to the credibility of the big data is to deliberately make fake data that can lead to erroneous conclusions. If data application scenarios are clear, it may be deliberately manufactured to create a “false impression” to induce favorite analysis. False information hidden in a large amount of other information, make it difficult to identify the authenticity, so as to make the wrong judgment. Some false comments on site that mixed in real comments are difficult to distinguish, which may mislead users to choose some goods or services of poor quality. The emergence and dissemination of false information in the current network community is becoming more and easier, so its impacts cannot be underestimated. It is impossible to identify the authenticity of all sources of information by information security technology.

The other threat to the credibility of the big data is progressive distortion of data in propagation. One of the reasons is that the manual intervention in the data acquisition process may lead to error, and those data distortion and deviation may affect the accuracy of the data analysis. Moreover, the change of the version of the data is also a factor for data distortion. In the process of communication, because of the changed reality, the early data collection has been unable to reflect the real situation. For example, the phone number of a restaurant has been changed, but it has been collected early by other search engines or applications, so users may see conflicting information and be affected in making a judgment.

So data users should have the ability to understand the reliability of data and prevent meaningless or wrong analysis results based on authenticity of data sources, data transmission, data processing process, etc.

SUGGESTIONS AND COUNTERMEASURES TO STRENGTHEN THE NETWORK ETHICS & GOVERNANCE

Privacy protection is a complicated social problem. In addition to the advanced technology, it’s also needs to be combined with the relevant national policies and industry regulations to protect personal privacy and avoid the threats to personal safety and property losses.

Network Ethics

Network ethics [4] means the moral consciousness, behaviors and the legal rules people should abide in network. Its manifestations are on three levels: On the conceptual level, the prevalence of personal liberalism; on the standard level, the failure of operation mechanism of moral standard; on the behavior level, the spread of immoral behavior. And the reasons are as follows: network structure defects, economic interests and the lack of laws and regulations related, etc. The constructing of network ethics needs obey the principle to adhere to the promotion of a better life for mankind; and the principle of equality and mutual benefit, freedom and responsibility, informed consent and harmless.

To Formulate & Improve the Rules and Laws for the Protection of Internet Privacy

The Civil law draft assented by the 31st session of the Ninth Standing Committee of the NPC, Dec 23rd, 2002, had clearly defined that private information, activities and paces are all categories of privacy. The "Protection Regulation for Minors" stipulates that the privacy of minors is forbidden to disclose. That is to say the right of privacy is one of the civil rights of citizens. Guo Yu [5] researched how to establish the legal system of personal data protection in China and put forward specific suggestions on how to develop an independent and comprehensive personal data protection and on how to use personal data correctly for personal data users.

In the era of big data, the original specification of tinkering has been unable to meet the needs of the protection of personal privacy, and to suppress the risk brought by big data. It is needed to redefine rules to meet the new demands. Data providers, businesses, and governments need to update the attention for privacy protection. Taking responsibility for the behavior of the data use, establishing and perfecting the laws and regulations on the protection of personal privacy, and strengthenting industry self-discipline by shaping industry privacy law are ways to protect personal privacy.

Mar 8th, 2006, The CDNCA central enterprise Committee submitted a “Personal Information Data Protection Law” proposal to the Congress in the NPC Conference, which requires to set clear limit on personal information data collection, using, marketing and other aspects through the development of regulations, and punish violations so as to improve the protection of civil rights and security, to ensure social stability and national security, and to enhance economic development. “Personal Information Data Protection Law” proposes changes from four aspects as: data acquisition, data-use limitations, data -marketing limitations and criminal penalties. Although the proposal has certain significance at that time, but for the era of big data today, these proposals are not able to meet the needs of personal privacy data protection. So, it is time to establish a general large data “personal privacy data protection law” based on the characteristics of big data and privacy data. The rights to protect personal privacy in the era of big data should be asserted, and the scope of personal privacy protection should be clarified. The object of legal jurisdiction is the users and the enterprise or the specific organizations. It is better to set up or entrust a special trade associations and industry self-regulatory organizations to assist the relevant government departments to supervise the implementation of the law, such as China Internet Association. The collection, use, dissemination, sharing and criminal punishment of personal data should be concerned when the law is being established.

- Regulations on data collection: Any enterprise or organization cannot collect personal information for a particular purpose. Eavesdropping should be sure to avoid in the process of information transmission. Specific user groups could not be tracked in order to attempt to obtain more detailed information about them. The personal information collected by enterprises or organizations should not be abused or sold without the acknowledgement of the individuals.
- Regulations on data use: The secondary use of personal privacy data should ensure that they cannot be lost, leaked or abused. A strict hierarchy access control strategy should be established to ensure the security of sensitive data in the process of data using.
- Regulations on data publishing: Published data information is not only conducive to data mining research but also to protect the privacy of personal information. The data publishing should have a very clear defind authority, which can help to avoid the leakage of personal privacy.
- Regulations on data sharing: In the process of data sharing, the two sides need to sign a legally contract or agreement to ensure that the user's data could not be compromised. Once the disclosure of privacy data occured, all participating parties should take corresponding criminally responsibilities.
- Criminal punishment: In violation of the above regulations, the related enterprise or organization should take severe criminal penalties according to the severity of the harmness to personal life or property.

Aug 21, 2015, The Supreme People's court trial committee discussed and passed “the provisions of the Supreme People's Court on Several Issues concerning the application of law in the case of civil disputes over the use of information networks to infringe upon the rights and interests of the people's court” which will carry out from October 10, 2015. In many places, the relevant local laws and regulations are set up based on local actual situation, such as “Regulations of the Shenzhen Special Economic Zone on Internet Information Service Security”.

The Insistence of Business Ethics and the Responsibility of Privacy Protection

July 2013, Ministry of industry and information technology issued the "Regulations on the protection of personal information of telecommunications and Internet users", which put forward clear requirements for telecommunication service operators and Internet information service providers when they collect the users’ information. That is to say, without the user's consent, they should not collect or use the users’ personal information.

If a user wants to use a certain service on the internet, service providers often require users to apply for registration and fill in the login name, age, address, ID card, mobile phone number, work units and other identity information. In addition to, users are asked to agree with some of the terms and conditions they have made. Lots of users will tick agreement without reading them carefully, which makes the rights to control and use users’ information legal. In the era of big data, it is essential to set up a different privacy protection model that focuses on the responsibilities data-users should take but not on the agreements in registration. Such responsibility transmission is meaningful.

Data users understand how they want to use data than anyone else. They should responsible for their activities as that they are the biggest beneficiaries of the second applications of the data. Service providers need to use a formal evaluation method to evaluate the impact of the behavior of the data reuse on the individual, and this impact can not pose a threat to the user's life.

To Establish an Orderly Network Governance Space by Law

It is necessery to promote the rule of law in cyberspace in order to promote the development of the “Internet +”. One of the ways to keet network security is to protect the Internet economic information and market transaction security, and to protect the personal privacy of consumers. In view of the current bottleneck problem and the blank field of laws and regulations, it is essential to sort out relevant laws and regulations and to promote the application of the current law to the network space to establish honesty credit environment, in which faithfulness will be motivated and dishonesty will be punished.

“Internet plus” brings convenience to our daily life, but also brings a series of problems. There are two main reasons for the appearance and long-term existence of internet privacy loopholes as follows: Firstly, legal punishment is not strict enough, so that the interests-related subjects get the “speculative psychology”. In western countries, personal privacy is strictly protected, whatever it is by self-disciplined or legislative mode, it has a strict definition and legal protection for network privacy. But here in China, with the illegal thinking that “the law could not punish numerous offenders”, internet users, media, businesses and other related responsibilities, in the protection of internet privacy, are extremely irresponsible. Secondly, there lacks credit consciousness and system of Network privacy and personal information. Although the relevant sites clearly promised not to leak personal information when they require users to fill in personal information, they are not strict in self-management under the driving of market interests.

To protect internet privacy, it is necessary to increase the cost of disclosure and invasion of personal privacy by law. To rectify internet privacy vulnerabilities, increase the cost for illegal activities, and adhere to the law could establish a social consensus to protect the privacy of individuals.

To Enhance Self-Discipline by Building a Network Integrity System

It is essential to adhere to the “integrity system” for safe and long-term protection of the Internet personal privacy. Punish the leak by means of law is the only way to promote “Four Comprehensives” and realize legal Governing. However, the function of law also has its boundary and limitation which could not solve all the problems. It is also essential to build more perfect credit system and try to create a credit environment on the internet for internet users and related subjects. When the related subjects lose their credit, it is equal to lose the future and market as well, which could cause the less of motivation for information leak.

To Form Social Consensus by Propaganda

All coercive means are for better protection of personal privacy. While strengthening the construction of internet privacy laws and the integrity, it is also need to strengthen the work of propaganda. Creating and protecting internet privacy should establish a broader consensus on social privacy, law and security and the internet environment of combination of respect and credit.

CONCLUSIONS

To sum up, the current research on large data security and privacy protection is not enough both in China and abroad. The better way to solve the problem of large data security and privacy protection needs the combination of technical means and related policies and regulations. Enterprises need to strengthen self management and ethical constraints, while users need to raise awareness and abilities of privacy protection as well. That is to say to build up the "privacy" protection mechanism as follow: "self-discipline by enterprises, proactive governmental supervision, self-protection by users" and the effective credit network system.

REFERENCES

1. Feng Dengguo, Zhang Min, Li Hao, Data Security & Privacy Protection（J），Journal of Computer Science，Jan 2014, the 37th Ⅰ P247-255
2. Yu Liping, Economics of Big Data and Big Data（J），Chinese Soft Science, 2013 the 7th, P177-183
3. Liu Yahui, ect, Personal Privacy Protection in the Era of Big Data,（J），Computer Research and Development, 2015, 52(1), P229-244
4. Song Zhenchao, Huang Jie, The Ethics of the Network Information and It’s Reason and Countermeasure under the Background of Big Data（J）, Theory and Reform, Feb, 2015, P172-175
5. Guo Yu, Research on personal data protection（M）, Peking University press, Mar, 2012, P33-38