Journal of KIIT. Vol. 19, No. 3, pp. 129-140, Mar. 31, 2021. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.3.129

Research on Big Data Privacy Protection based on the Three-Dimensional Integration of Technology, Law, and Management

Dekui Wang*[1], Hyung-Hyo Lee*[2]

This paper was supported by Wonkwang University in 2019

Abstract

Big data brings huge benefits to people, but also brings great risks to users' privacy leakage. In view of the risk of user information privacy leakage in the big data environment, select the "data use" stage of the big data privacy protection life cycle to study user privacy protection. From the three aspects of technology, law, and management, a "three-dimensional integration" big data user privacy protection model is constructed, and three aspects are coordinated to achieve the optimization of user privacy protection in the "data use" stage of the big data environment.

요 약

빅 데이터는 정보 이용자들에게 큰 이익을 가져다 줄뿐만 아니라 사용자의 개인 정보 유출에 큰 위험을 초래할 수 있다. 본 논문에서는 빅 데이터 환경에서 사용자 정보 프라이버시 유출 위험을 최소화하기 위해 빅 데이터 프라이버시 보호 라이프 사이클 중 데이터 사용 단계를 중심으로 사용자 정보 프라이버시 보호 방식을 제시한다. 제시된 방법은 기술적, 법적, 관리적 등 3가지 측면에서 사용자 정보 프라이버시 보호를 위한 방식을 제안하고 제시된 방식이 데이터 사용 단계에서 주요 사용자 정보 프라이버시 취약점에 대응할 수 있는지 제시한다. 또한 빅데이터 환경의 사용자 정보 프라이버시 보호를 위해 진행된 기존 연구들과의 차이점을 분석하여 본 논문에서 제시된 기술적, 법적, 관리적 측면을 함께 고려한 보호 방식의 장점가 특징을 보인다.

Keywords
adaptive big data, "data use" stage, three-dimensional integration, privacy protection

Ⅰ. Introduction

According to data from the Internet Data Center (IDC), data on the Internet is currently increasing by 50% every year, doubling every two years, and more than 90% of the data on the global Internet is only

* Department of Computer Engineering, Graduate School of Wonkwang University
- ORCID[1]: https://orcid.org/0000-0001-8654-4460
- ORCID[2]: https://orcid.org/0000-0003-4393-7365

· Received: Feb. 15, 2021, Revised: Mar. 25, 2021, Accepted: Mar. 28, 2021
· Corresponding Author: Hyung-Hyo Lee
Department of Computer Engineering, Graduate School of Wonkwang University, 460 Iksan-daero, Iksan, 54538, Korea
Tel.: +82-63-850-6259, Email: hlee@wku.ac.kr

generated in recent years. It can be said that mankind has entered the era of big data. The data scientist Victor Mike Schönberger, who was the earliest insight into the era of big data, pointed out in the book "The Age of Big Data": The benefits of big data to human life are manifold. It is not only a source of people gaining new cognition and creating new value, but also a way to change the market, organizational structure, and the relationship between government and citizens. But he also pointed out that big data will bring more threats to network security and greater challenges to user privacy than traditional Internet[1,2]. Although the data is objective, the right to interpret the data is in the hands of a few planners, designers, analysts and users. Therefore, differences in people's positions, interests, and values will cause biases and prejudices in the use and interpretation of data. The more widespread the collection and use of large amounts of data, the higher the privacy risk and the more urgent the need for privacy protection.

II. Related Work

2.1 A review of previous research literature on privacy protection

In this study, we searched the “Springer Link” database for the keyword "Disclosure of privacy" and found that there are nearly 10,000 articles on privacy leakage as of March 12, 2021, of which the English academic community occupies the main part; by searching the keyword "privacy protection of big data". Research through literature search shows that there have been relatively rich results in big data and personal privacy in recent years, and the research perspective also covers all aspects of daily life. Summarizing the current research on big data privacy protection, there are several characteristics: (1) The scope of research is all about the full life cycle (four stages); (2) The research content is all about a certain aspect It is researched either from the technical aspect or from the legal aspect; (3) Research blind spots, there are almost no research from the management aspect alone, generally they are in addition to the technical and legal research and assist in the management aspect Research.

In view of this, this study selects the "data use" stage in the life cycle of big data privacy protection as the research object, and conducts privacy protection research from three aspects: technology, law, and management.

2.2 Analysis of privacy protection measures adopted in the past

2.2.1 Protection from technical dimensions: two main technical categories

The main technologies of big data privacy protection are basically divided into two categories: defensive type and tracing type. (1) Defensive personal information protection technology. Defensive personal information protection technology can truly prevent others from using their own information. (2) Retrospective personal information protection technology. Data traceability technology refers to derived information from data sources to data products[3].

For structured data (or relational data), defensive personal information protection technology is the key technology to protect privacy. The traceability type personal information protection technology is used to trace the origin of information, mainly based on the trace path to reproduce the historical state of the data and its evolution process, so as to realize the traceability of the historical data archives and facilitate the correctness of the results check, or you can quickly update the data.

2.2.2 Legal protection: three representative legislative forms

The current personal data protection legislation in

the United States, Europe, and Japan is currently three representative forms. (1) The US model is an industry self-discipline model. Focus on industry self-discipline, supplemented by national legislation. Based on the right to privacy, make relevant supplements in different laws. This is a decentralized legislation. (2) Europe adopts a unified legislative model. After the adoption of the General Data Protection Regulation, all existing personal data use links have been opened up. Because of the unified standards, this can promote the flow of information and resource sharing among all EU countries. (3) The Japanese model combines the characteristics of the United States and Europe and adopts the mature part of the two.

The adoption of this model in the United States has a certain relationship with its social atmosphere and the development status of the information technology industry. As the most advanced country in information technology in the world, the United States has developed rapidly in information technology, and practitioners in the information industry have extremely high professional qualities[4]. In theory, Europe can rectify the order of the industry, which will benefit the development of the industry in the long run. In Japan, legally, a unified legislation is adopted; in industry, the government encourages and guides the establishment of industry associations, taking into account the needs of personal information protection and social development.

Table 1. Comparison of privacy protection technologies

Classification	Technical name	Method	Advantage	Disadvantage
Defensive	Anonymity	K-anonymous	Better effect	Low data availability
	Data interference	Numerical and graph structure disturbance	Easy to operate	Cumbersome and not highly applicable
	Game control	Predictive model	Dan effectively prevent specific models	Limited protection
	Access control	Autonomy and coercion	Flexible control	New types are difficult to implement in time
	Role mining	Top down bottom up	Keep permissions up to data Eliminate security holes	First determine the role
Retroactive	Digital water mark	Robust watermark	Can maintain the accuracy of date and detection	Difficult to determine the balance of information
		Fragile watermark	Little impact on the data itself	Attackers can easily modify the content
	Data traceability technology	Notation	Simple to implement and easy to manage	Only suitable for small systems
		Discovery query	Tracking is relatively simple	The implementation is more complicated

Table 2. Comparison of legislative features

Attributes / Country	Legislation	Industry self discipline	Advantages	Disadvantages
USA	Dispersed	Primary	- Conducive to technological development - More democratic and free	High requirements for information practitioners
Europe	United	Secondary	- Facilitate the flow of information - Promote resource sharing	The standards are too high restricting international cooperation
Japan	Mixed	Mixed	- Each category is individually controlled - Fully avbsord the advantages of each category	Before selecting measures, prepare for classification and identification

2.2.3 Management protection: privacy management in representative areas

Countries or regions continue to take various measures to protect private information and reduce the occurrence of various leaks. Many countries around the world, including the United States, the European Union, and Japan, have established relevant institutions to formulate relevant management measures to improve privacy protection[5]. Representative regional privacy protection management in the world, as shown in Table 3.

There are regulatory methods such as technology, law, and management in the online world. Only by relying on any one method, the order in the online world cannot be perfectly regulated, and privacy protection cannot be protected. Based on this idea, the author believes that a variety of privacy protection methods can be reasonably used to protect the privacy of big data at multiple levels and three-dimensionality.

III. Research Model and Framework

3.1 Big data privacy protection life cycle model

The concept of life cycle is widely used. In psychology, it mainly refers to the life cycle of a person and the life cycle of a family, and refers to the process of its birth, growth, aging, illness and death. The term "privacy" comes from the United States. Privacy is essentially a kind of information, a kind of private and exclusive information that is unwilling to be known or interfered by others. Combining privacy protection with life cycle theory, some scholars have proposed a privacy protection life cycle model.

Table 3. Comparison of management features

Area	Management	Main responsibilities	Methods	Control
USA	Federal trade commission	Responsible for handling internet privacy complaints filed by consumers, congress and industry organizations, and conducting investigations.	Administrative measures	Afterwards control
	Federal communications commission	Regulation of the telecommunications industry has a limited role in monitoring internet privacy.	Administrative measures	Afterwards control
EU	Data protection agency	The data processing behavior of regulatory agencies, inspection plans and practices are in compliance with the data protection law.	Administrative measures	Afterwards control
	Data protection supervisor system	Strictly manage the collection, recording, storage, re-extraction, sending or enabling other personnel to obtain, delete or destroy data by institutions and organizations.	Administrative measures	Afterwards control
Japan	PIPC*	It has the right to supervise all personal information processing companies and can take necessary measures based on specific circumstances.	Administrative measures	Afterwards control
	PIPC* and FSC* jointly supervise	Regulate the use and transfer of personal information in the financial field.	Administrative measures	Afterwards control
	PIPC and JMHLW* jointly supervise	Regulate the use and transfer of personal information in the financial field.	Administrative measures	Afterwards control
Canada	Privacy committee	Has the right to dispatch commissioners to investigate complaints, make decisions, and issue non-compulsory suggestions.	Administrative measures	Afterwards control
	Office of privacy commissioner	Accept and investigate personal information infringement complaint and submit annual reports and special reports on the protection of personal information to the parliament.	Administrative measures	Afterwards control

A common big data privacy protection life cycle model is shown in Fig. 1.

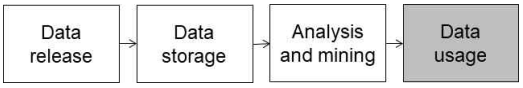

Fig. 1. Big data privacy protection life cycle

3.2 Infringement of privacy in the process of "Data usage"

With the increasingly frequent use of big data and the increasing maturity of technology, the leakage of private data has reached a shocking and frightening state. Cases of privacy data breaches abound. The scope of privacy data breaches is expanding, and more and more industries and departments are in trouble. The Internet information industry, big data industry, express delivery industry, hotel industry, aviation industry, comprehensive business, as well as medical industry, catering industry, etc., the more industries that are closely related to people's modern life, business, and travel, the greater the impact.

The value of big data is no longer purely based on the basic purpose of data collection, but more from its potential use value. In the era of big data, after the user's data is collected, it will be used for other purposes or transferred to a third party out of the background when it was collected.

Research has found that there are currently six main types of privacy data violations:

(1) Hacker attacks. The technical vulnerabilities of hackers invading companies are the primary cause of exposure of personal privacy and corporate secrets. A group of professional hackers for the purpose of profit, etc., specially load the other party's system without permission.

(2) Mistakes in enterprise technical operations. Some corporate departments have made particularly serious mistakes. They directly mis-transmit the data packets to the public network, so that ordinary netizens who do not have hacking skills can obtain it smoothly; or send emails by mistake, wrong permission settings, improper server configuration, etc. Mis-operations have led toa significant increase in data breaches, which also reflects the lack of basic security awareness or risk assessment capabilities of internal personnel.

(3) Enterprises have insufficient investment in information security. Enterprises' investment in information security does not match the commercial value and social value of the target that needs to be protected, and cannot meet the needs of safe operation and maintenance. It is also an important factor in data leakage. The lack of security investment does not match the value of the protection objectives. On the one hand, it reflects that the company has not yet reached the national security standards at the technical and management level; on the other hand, it also reflects that the awareness, cognition, and ability of network security assurance lag behind information network technology. The explosive growth of its applications.

(4) Leakage of data by internal personnel. Insiders, driven by high profits, take risks and use their positions to illegally obtain large amounts of personal information from citizens, which has become an important source of data leakage.

(5) Commercial companies sell personal data. Commercial companies steal or illegally obtain citizens' personal information by other means, and then use it for public sale to companies in need.

(6) Invisible leakage of privacy in government information management. As a public management department, the government collects a large amount of personal privacy data information according to work needs; it also develops and shares some data due to work needs, which invisibly causes citizens' privacy to leak.

Therefore, it is necessary to select the "data use"

(shaded part of the life cycle model diagram) stage of the big data privacy protection life cycle for special research.

3.3 Big data privacy protection "Data usage" stage privacy protection model

In response to the risk of user information privacy leakage in the big data environment, the "data use" stage of the big data privacy protection life cycle is selected to study user privacy protection from the perspectives of technology, law, and management. Construct a privacy protection model based on the three-dimensional integration of "technology, law, and management", and conduct privacy protection research.

The premise of the design of this model: First, fully understand the current main privacy protection methods; second, carefully study the typical privacy protection models in the past; and third, compare multiple privacy protection methods and analyze typical privacy protection models. After completing the prerequisite work of the model design, it was discovered that each method may have loopholes and imperfections in the protection. The comprehensive use of multiple privacy protection methods can complement each other and coordinate protection. Therefore, three main protection methods were selected to construct a comprehensive application and coordination protection model, namely, a three-dimensional integrated big data privacy protection model based on "technology, law, and management".

3.4 Analysis of three existing typical protection models

3.4.1 Brief introduction of existing protection models

(1) Privacy protection model based on game theory

In the process of the visitor's access to the interviewee's private information, it is assumed that both the protector of the private information and the visitor must pay a certain price for the possible actions, and the price paid and the benefits obtained are the decisions of both parties. Factors to be considered and weighed at the time. Based on the above point of view, this article regards the visitor and the owner (visited) of private information as two parties in a mutual game, using game theory to determine whether to visit in good faith or maliciously (for the visitor) and to allow access (leak) or deny access(Non-disclosure) (for the interviewee). During this process, the strategies adopted by both parties and the corresponding benefits obtained are analyzed to establish a game model as the basis for realizing user privacy information protection, and ultimately achieve effective protection of user privacy information[6].

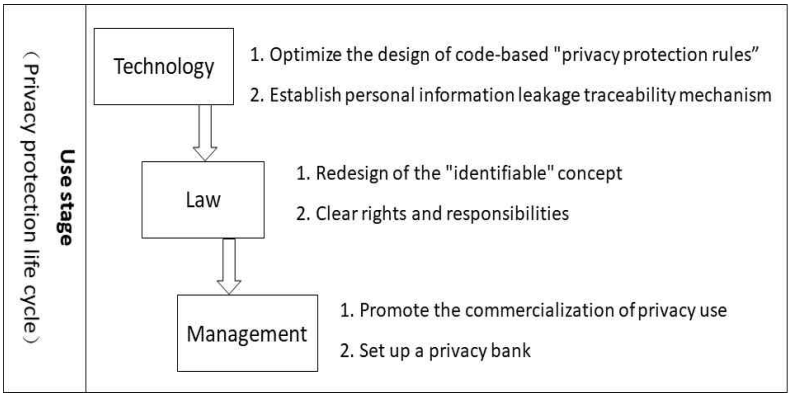

Fig. 2. Three-dimensional integrated privacy protection model

(2) Privacy protection model based on trusted third parties

Whether it's a two-party interaction model where the website collects user information on its own, or an open platform with rich user resources

In the three-party interaction mode, it is difficult to avoid transferring user privacy information to more websites for storage. In addition, users cannot guarantee sufficient management authority for their personal information, which makes the abuse of private information increasingly serious. In this case, it is proposed to build a personal information service platform for network users as a trusted third party to store users' personal information and provide personal information management and application services to network users and websites[7].

(3) Privacy risk inspection control model based on cyber insurance

In the big data environment, even if the data collector has made the most adequate privacy guarantees, privacy leakage may still occur. Once a data set is leaked, because the data set itself involves many individuals and groups, the number of individuals and groups whose privacy is leaked is also very large. Under this circumstance, if these privacy leaked individuals and groups require data collectors to compensate for the losses caused by the privacy leak, this will be a very large number. In order to solve this problem, the use of network insurance has emerged to reduce the loss of data producers and data collectors due to privacy leaks. However, due to the unique characteristics of data hidden risks, data producers and data collectors may use certain loopholes to reduce their own privacy parameters or obtain illegal benefits in the process of network insurance applications. The use of network insurance contracts can solve these two types of problems, incentivizing data producers and data collectors not to reduce their own privacy, and avoiding some illegal means to obtain additional benefits[11].

3.4.2 Model comparison and analysis

In the era of big data, a useful data privacy model must adapt to the requirements of 3V. In order to measure model's effectiveness, Jordi Soria-Comas and Josep Domingo-Ferrer proposed three characteristics: (1) Composability(COMP); When the model is repeatedly applied independently, the privacy of the model can still be guaranteed. (2) Low computational cost(LCC); The cost of data conversion in order to meet the requirements of the privacy model is low, so an appropriate conversion method must be selected. (3) Linkability(LINK); The possibility of establishing a connection between individual data in the anonymized data set must be lower than that of the original data set[6].

Table 4. Comparison among protection models

Model	COMP	LCC	LINK	Service object
Game theory based	yes	yes	no	Both sides
Trusted third party based	no	no	yes	Individual-oriented
Network insurance based	yes	no	no	Group-based
Three-dimensional based	yes	yes	yes	All users

According to the analysis and comparison of the three characteristics of useful privacy protection models, the foundation of the model, and the service objects, it can be seen that the "three-dimensional integration" privacy protection model is better.

IV. Model Analysis

In the Internet era, the value of personal data has become increasingly prominent. However, the enhancement of information fluidity and the development of information processing technology have made the boundaries of the rational use of information more and more blurred. A large amount of personal data is disseminated and used without restrictions,

resulting in. There are endless crimes committed by using personal data. The abuse of personal data by enterprises and authorities and the infringement of personal privacy have made people pay more and more attention to the security of personal data. With the development of the times, people's concepts are constantly changing, and personal data has been developed from a technical problem in the past to a complex system problem integrating law, technology, and management.

4.1 Technical aspects

4.1.1 Redesign of "Privacy Protection Rules Since Design"

Privacy protection since design is one of the main principles for personal information protection: Privacy embedded into design, that is, privacy protection rules since design. The development and implementation of system programs must ensure privacy protection and system performance. Integration. Therefore, it can be seen that the privacy protection since the design started with an open attitude, providing conditions for legal rules and code rules to jointly build a new normative model in the protection of personal information. The current application of the "privacy protection since design" rule is still Stay on the basis of informed consent rules, and its manifestation is that at each stage of collection and use, the information subject's express consent is required. The principle is fixed and the form is variable. The privacy protection rules from the beginning of the design may be redesigned by combining scenario-oriented and risk-oriented concepts. Following the basic requirements of privacy protection rules "active rather than passive", "throughout the life of data", "user-centered", and "transparency and openness" from the design of the privacy protection rules, at each stage where notification and consent were originally require. Use the efficient calculation of the code to evaluate the usage scenarios and risks, and calculate the risk minimization strategy in the background. If the system determines that even after the risk minimization process, the behavior is still high-risk or medium-risk, the original The notification consent procedure of the user can continue to use the personal information after obtaining the user’s consent.

4.1.2 Establishment of personal information leakage traceability mechanism

Personal information leakage traceability mechanism According to the data stream information generated by the personal information movement, when faced with the need for personal data privacy leakage traceability, technical means can reproduce the historical evolution path of personal information, so as to more accurately lock the personal information leakage incident responsible body, and provide evidence basis for related post-processing. Effective tracking, prevention and control of personal information protection will reveal the high-speed invisible personal information flow and processing path in the era of big data, and increase the possibility of the big data industry being supervised.

4.2 Legal aspects

4.2.1 Redesign of the "identifiable" concept of personally identifiable information

Objectively speaking, the purpose of the Personal Information Protection Law is to "prevent abuse, not to protect". It emphasizes collecting information through legal means and following the principle of "fair information practice" in the process of information processing. Therefore, if the boundary of the right of information privacy is defined too broadly, it is a manifestation of "too much is not enough".

"Identifiable" is the key to solving this problem. It is divided into direct identification and indirect identification. No matter which one, their status is the same, that is, only those personal information that can be identified are protected.

It is more feasible to differentiate protection on the basis of “identifiable” classification. For example, Professor Schwartz and Solovei proposed to divide the concept of “identifiable information” into “identified individual” data and "Data that can be used to identify individuals", and treat these two types of data differently. This process can be divided into two steps: In the first step, the privacy law is directly applied to personal information that has been "identified", and the personal information that is "identifiable" is specifically measured. The second step is to see whether these personal information constitute a complete "image map" of a person, that is, whether it contains the elements of personal dignity, where only "identifiable" personal information is involved.

4.2.2 Clarification of rights and responsibilities

Combined with fair information practice, two loopholes in the theory of personal information control will be discovered:

(1) The value-added of personal information is mainly in the secondary and tertiary applications, and it is obviously not a complete realization of the "right of informed consent" at this stage.

(2) Personal information control theory ignores or even ignores the huge power gap between data collectors and processors and citizens.

Due to the huge differences in knowledge, resources, and platforms between individuals and large institutions, the status of both parties is unequal. It is unrealistic to try to eliminate this inequality with personal information cybernetics. We need to change our thinking. Since the purpose of the privacy law is to prevent abuse, we should put a shackle on "abuse", that is, we should focus on making data collection and users accountable.

Data users must respect the basic rights of citizens around privacy in the development and utilization of data resources. In the event of infringement, the data user must bear the corresponding responsibility. Because data users know better than anyone how they want to use data. Their assessments (or assessments conducted by experts they hire) avoid the disclosure of trade secrets. Perhaps more importantly, data users are the biggest beneficiaries of secondary data applications, so of course they should be held accountable for their actions.

4.3 Management aspects

In the United States, with regard to the protection of personal information, the dominant trend in the law since the 1990s is that consumers can control information in the market regardless of whether the use of information causes harm. Columnist William Safire wrote in The New York Times in 1999: "Your bank account, your health record, your genetic code, your personal and consumption habits and interests are all your own business. Information is valuable. Yes, if someone is willing to pay to peek into your life and ask them to send you an offer, you will consider it.” Therefore, commercial methods can be used to better protect private information.

4.3.1 Commercialization of private information

According to a Ponemon Institute's "Privacy and Security of Internet Life; A Survey of Consumers in the United States, Europe and Japan", Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute, pointed out: "Privacy , it is to protect the right of personal sensitive and private information not to be disclosed, unless you want to send some information to be disclosed. However, we were surprised to find that as long as the manufacturer provides a certain level of compensation, most

consumers are willing to use their names , gender, buying habits, and even physical health status and account login information are provided to manufacturers. When asked, they can even open bid codes for their personal information, ranging from US$2.75 to US$80. "The survey covers 1,903 consumers from Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Japan, Luxembourg, the Netherlands, Poland, Russia, Slovenia, Spain, Sweden, Switzerland, the United Kingdom and the United States. Although the price of personal information varies in different regions, overall, respondents believe that the average price of a single piece of information is US$18.5.

4.3.2 As a production factor, a privacy bank can be established

In the long run, with the rapid development of information technology, the economic value of data has gradually emerged. Data is as important as land, equipment, raw materials, capital, labor, and technology, and can generate high economic value.

In the use of private information, there are two aspects, one is for personal use, and the other is for other people or organizations. A third party trusted by both parties is needed to achieve this task. As a third party trusted by both parties, the privacy bank can not only protect privacy, but also allow privacy to play a normal role as a production factor and realize the value of privacy.

According to the value characteristics of personal information, personal information can be voluntarily stored in a privacy bank.

Organizations or individuals that need to use personal privacy information can obtain private information through this intermediary. Privacy banking is the correct and safe channel for companies or individuals to obtain personal information.

Private information may be leaked during use, so it must be protected. In use, there are two aspects, one is for own use, and the other is for other people or other organizations or departments. Whether other people, other institutions, or departments are credible has become a question that needs to be considered. At this time, a third party trusted by both parties is needed to achieve this task. As a third party trusted by both parties, the privacy bank can not only protect privacy, but also allow privacy to play a normal role as a production factor and realize the value of privacy. According to the value characteristics of personal information, personal information can be voluntarily stored in a private bank for a fee. Organizations or individuals that need to use personal private information can obtain private information through this intermediary. Privacy banking is the correct and safe channel for companies or individuals to obtain personal information.

4.4 Three-dimensional integration of technology, law, and management

In the Internet age, the leakage of user privacy may occur at any time, and the methods and means for privacy information users to steal privacy are also diverse. There may be loopholes in user privacy protection technology, incomplete law, and lack of management. Therefore, from the perspective of technology, law, and management, private information can be stolen at any time. A certain technical loophole in privacy protection can just be remedied by certain provisions of the privacy protection law; if technical loopholes and legal incomprehensions occur at the same time in a certain situation, there are still management methods that can restrict it. In this way, the organic integration of the three methods of technology, law, and management has achieved coordinated development; this is like a comprehensive use of three methods for users' private information, which actually achieves the effect of multiple protection. These three different methods are interconnected and compensate each other, and jointly promote the protection of private information.

Therefore, the protection of personal user privacy information in the era of big data cannot be done by a single company or by one means. Three methods such as technology, law, and management must be used in concert to achieve a "three-dimensional integration".

Table 5. Relationship between privacy violation types and privacy protection integration model

Types of privacy violation	Technology	Law	Management
Hacker attack	○	○	
Mistakes in enterprise technology operation			○
Insufficient investment in corporate information security	○		○
Enterprise internal data leakage		○	○
Commercial companies selling personal data	○	○	
Invisible disclosure of privacy in government management	○	○	○

4.5 Suggestions for model application

Ideally, we build a three-dimensional integrated big data privacy protection research model based on "technology, law, and management", which can realize the coordinated development of technology, law, and management in three dimensions, and jointly realize the protection of big data privacy. But the actual situation is not exactly the case. The main reasons are: first, privacy protection has always had multiple protection dimensions such as code, law, management, and social norms; second, the big data privacy protection life cycle model has four stages: data release, data storage, analysis and mining, and data use. In the case of multiple protection dimensions and four cycle stages, the model constructed by using "three-dimensional integration" and focusing on the "data use" phase can protect privacy to a certain extent. Therefore, under suitable conditions, this model can be applied.

V. Conclusions

On the one hand, big data has brought convenience to people's lives, on the other hand, it has also brought troubles, always worrying about the infringement of personal privacy information. In this context, we have learned about various privacy protection methods and found that a variety of protection methods can be reasonably used for coordinated development. When considering the comprehensive application of multiple methods, we should fully compare the previous privacy protection models, especially the models in the data use phase of the privacy protection life cycle. Therefore, considering the existing environment and proceeding from the actual situation, construct a three-dimensional integrated privacy protection model based on "technology, law, and management"; adopt a variety of three-dimensional protection methods to realize the coordinated development of privacy protection.

References

[1] Guoyong Lin, "Information security opportunities and challenges in the era of big data", Journal of Information Construction, Vol. 1, No. 1, pp. 19-20, Jan. 2016.

[2] Hyung-Hyo Lee, "An Alternative Resident Registration Number System and Management Framework for Privacy Protection", The Journal of Korean Institute of Information Technology, Vol. 8, No. 6, pp. 49-58, Jun. 2010.

[3] Jinnian Zhang, "The status quo and hotspot analysis of personal information research in the era of big data in my country", Journal of Library and Information Guide, Vol. 5, No. 4, pp. 56-66, May 2020.

[4] Jianzhen Zhang, Yuyan Niu, and Qiang Li, "Research on the privacy protection of online learning users under the background of big data",

Journal of Intelligent Computers and Applications, Vol. 10, No. 2, pp. 236-239, Oct. 2020.

[5] Yuting Jiang, "Research on privacy information protection methods based on big data analysis", Journal of Information Recording Materials, Vol. 20, No. 11, pp. 244-245, Nov. 2019.

[6] Yixuan Zhang and He Jingsha, "A privacy protection model based on game theory", Journal of Chinese Journal of Computers, Vol. 39, No. 3, pp. 618-620, Mar. 2016.

[7] Han Wang and Ling Zhang, "Research on Network Privacy Protection Model Oriented to Personal Information Management", Journal of Information Science, Vol. 33, No. 10, pp. 48-50, Oct. 2015.

[8] Jordi Soria-Comas and Josep Domingo-Ferrer, "Big Data Privacy: Challenges to Privacy Principles and Models", Journal of Data Sci. Eng, Vol. 1, No. 1, pp. 21-28, Jan. 2016.

[9] W. Huang, "An analysis of the relationship between anti-terrorist intelligence work and the protection of personal privacy information in the era of big data", Journal of Library Information, Vol. 1, No. 1, pp. 43-50, Apr. 2018.

[10] Runbo Ji and Xuan Fei, "Personal information protection in the era of big data", Journal of Telecommunications Network Technology, Vol. 1, No. 1, pp. 53-56, Mar. 2017.

[11] Xiaotong Wu, "Research on Privacy Protection and Its Key Technologies in Big Data Environment", Journal of Chinese Journal of Computers, Vol. 36, No. 7, pp. 202-204, Jul. 2018.

Authors

Dekui Wang

2005 : BS degree in Department of Management, Yangtze University, China

2011 : MS degrees in Department of Management, Nanjing University of Aeronautics and Astronautics, China

Research interests : privacy protection, big data, E-commerce

Hyung-Hyo Lee

1989 : MS in Department of Computer Science, KAIST

2000: PhD in Department of Computer Science, Chonnam National University

2001 ~ present: Professor, Wonkwang University

Research interests : access control, privacy protection, digital forensics