Systematic Regulation of Personal Information Rights in the Era of Big Data

FangBing Zhu¹,² and Zongyu Song¹

Abstract
Big data has an important impact on people’s production and life. The existing legal and judicial protection, sanctions, and mechanisms for the enforcement of information rights have proved insufficient to stem the serious consequences of rampant leakage and illegal activity. Based on Information Full Life Cycle Theory, this article combines qualitative analysis with quantitative analysis, uses data from the Survey Report on App Personal Information Leakage released by China Consumers Association as an example, and finds that illegal access, illegal provisions, and illegal transactions have become important sources of personal information leakage. The main reasons for this problem include limitations of the technologies used, the falsification of informed consent, the lag of legislative protections, and a lack of administrative supervision. Systematic regulation of the right to protect personal information should include a variety of initiatives. First, it should be used to identify who to protect and how to protect them. Second, there needs to be a shift from identifiable subject regulations to risk control. Third, legislation needs to be comprehensive, entailing a shift from fragmented to systemic reforms. Fourth, protection efforts should include supervision, self-regulation, and management. Finally, the jurisdiction of legislation should extend across cyberspace and physical reality as a means to achieve a balance between effective protection and the reasonable use of personal information.

Keywords
personal information rights, big data, systematic regulation

Introduction
The boom in mobile internet and big data technology has produced significant changes to the means and the extent of personal information collected. While enjoying the conveniences of user-customized services and targeted marketing that big data affords, people also have seriously suffered from personal information leakage and a seemingly unavoidable infringement upon their privacy. Facebook disclosed that more than 50 million users’ data had been leaked, triggering a Federal Trade Commission (FTC) investigation of Facebook’s privacy protections.¹ Twitter issued a declaration stating that the company might have put 330 million user passwords at risk.² Huazhu Group, the leading company in the hotel industry in China, reported a suspicious leakage of 500 million pieces of user information.³ The Office of the Information Commissioner of the United Kingdom (ICO) announced that it had imposed a fine of 18.4 million pounds on Marriott for failing to protect the security of customers’ personal data.⁴ A massive leak of Weibo user data has been disclosed and 538 million pieces of user information were sold on the dark web.⁵ Personal information has been leaked and infringed upon to a level that almost no one can avoid it.

Some scholars have called for new laws to address these challenges (Zhang, 2017). In their work on the protection of personal information, Yu (2013), a Chinese legal scholar, stated the following:

The era of big data has completed a series of data-centric technological transformations on concepts, technologies, and applications. This kind of widespread and fundamental transformation will inevitably lead to changes in the way of production and communication for people, and in social governance and structure. It will also call for a corresponding change in the legal system.

In some European countries, the needed laws and regulations for the protection of personal information were introduced. Currently, most countries and regions around the world have enacted personal information protection laws. Germany led the world in the legal protection of personal

¹Chongqing University, China
²Chongqing University of Posts and Telecommunications, China

Corresponding Author:
Zongyu Song, Law School, Chongqing University, Shazheng Road, Shapingba District, Chongqing 400044, China.
Email: 35323007@qq.com
information rights. The Hesse Data Protection Law, enacted in 1970, was the world’s first law relevant to the protection of personal information; the Federal Data Protection Act issued in 1977 was honored as a banner of the European personal information protection act; the Federal Data Protection Act passed in 2017 made it the first EU member state to localize the General Regulations on Data Protection. Other EU countries also have attended promptly to personal information protection. The Swedish Information Act of 1973, the French Information, Archives and Freedom Act of 1978, and other laws and regulations published by Ireland, Belgium, Spain, Portugal, Italy, and other countries all have been responses to the problem. The European Union passed the Data Protection Directive in 1995, created personal information capabilities, such as the right to access, corrections, deletions, and storage of personal information, and opposed information processing (Guo, 2011). In 2012, the EU began to promote the construction of integrated data protection regulations and the formation of a single digital market. In 2016, the EU promulgated the General Regulations on Data Protection, which distinguished pseudonymized and anonymized data. The EU also introduced the concept of the right to be forgotten and the right to data portability (Shi, 2012).

Some Asian countries also have implemented important legislation. The Japanese Personal Information Protection Law, passed in 2017, innovatively stipulated third-party authentication and anonymous use of information (Wei & Song, 2018). Article 111 of the General Principles of China’s Civil Code in 2020 stipulated that the personal information of natural persons is protected by law. Articles 1035-1039 of the Personal Code of Personality Rights of China’s Civil Code in 2020 explicitly specified the scope of personal information protection, the principles of collection and use, security responsibilities, and exemptions.

The United States promulgated the Privacy Act of 1974 to protect personal information in the form of privacy rights. The federal government implemented the Electronic Communications Privacy Act of 1986, the National Information Infrastructure Protection Act of 1996, the Privacy and Personal Information Protection Act of 1998, and the Information Security Management Act of 2002. The State of California passed the Online Privacy Protection Act of 2004 to separately protect the personal information provided in credit, medical, financial, and other spheres (Liu, 2016). The state also enacted the California Consumer Privacy Act (CCPA) in 2018 that granted consumers the right to know, access, carry, and delete personal information. It also protected the right to refuse the sale of their personal information. The United Kingdom promulgated the Data Protection Law to regulate the collection and use of personal information. However, Zhou (2018a), a Chinese legal scholar, noted the following:

Personal information protection in the big data era is far more than just enacting protection laws. The real challenge is how to organize the relations between the legislative requirements and the intrinsic incentives of information possessors through scientific legislation and system design, making personal information protection an internal need of information possessors.

A review of existing research at home and abroad reveals that scholars typically have designed protection regulations with a focus on the performance of confidentiality obligations, default specifications for permits, contractual provisions, the interest measurement and institutional arrangement, the design of incentive-compatible mechanisms, the trend of social control, the regulation of public law frameworks, the protection of infringement liability, the application of technological means, and the role of government regulation. Litman (2000) emphasized the need to approach personal information rights from a concern for the violation of confidentiality obligations. Samuelson (2007) adopted contractual methods to guarantee the right to personal information through default permit specifications. The right to personal information should be regarded as a new type of property right and should give dual protection to property right and personal right (Liu, 2007a). Wang (2013) identified the need to pay attention to the correlation between personal identification and national security, and to adopt comprehensive protection based on prior prevention. Based on the measurement of interests related to personal information protection, Zhang (2015) emphasized the balance between the interests of personal freedom and personal dignity of individuals, the interests of information providers in using personal information, and the public interests of the state in managing the society. Wang and Jiang (2016) compared and analyzed the privacy protection laws and regulations of China and the United States, and proposed the establishment of ethical norms in legal exceptions to fight against big data pollution with small data thinking. Wang and Du (2017) suggested cross-border cooperation and cross-sector cooperation based on the personal privacy protection system of New Zealand. By comparing the legislative practices of the European Union, the United States and Russia, Ji (2017) proposed the introduction of scenario-based risk management, the establishment of special regulator independent of the government, and the localization of personal information considerations and differentiated relief for compensation. Government supervision also has been offered as a means to enhance the protection of personal information from the perspective of establishing administrative supervision institutions, administrative supervision systems, and punishment systems (Zhang, 2017). Zhou (2018b) identified the need to make incentive compatibility the core of institutional design and to advocate for fostering internal governance mechanisms for information controllers and constructing effective external enforcement deterrents. Gao (2018) examined the use of social cybernetics to establish a personal information protection system that balances personal interests and the overall interests of society and adapts to the era of big data. Chen (2018) also suggested that to protect public law, an ethical order and
rule system for personal information protection should be comprehensively established. Ding (2018) noted the need to activate the protection of personal data in private law through “consumerization” and regulating risks through the public law framework. Jiang (2019) claimed that personal information protection should be adjusted and improved accordingly, including the aspects of legislative perfection, technical protection, administrative supervision, industry self-regulation, and self-protection. Finally, Cheng (2019) claimed that a comprehensive protection method that emphasizes both public law and private law should be adopted for personal information.

Much of the legal analysis on the protection of personal information has been based on a framework of informed consent developed before the Information Age. Li (2019), a Chinese legal scholar, cautioned that novel technologies should not be confronted with outdated approaches:

The development of technology has always been an important factor giving rise to the change of legal theory and system. Legal theory and system should pay attention to and respond to new problems brought by technology, and must not hang on to what’s outmoded.

To face the new challenges that have emerged during the big data era, the protection of personal information should shift from a static approach of informed consent emphasized before the Information Age to a dynamic protection of data usage regulations, in which personal information protection is treated as an inherent demand made of information possessors. Based on Information Full Life Cycle Theory, we used the Survey Report on App Personal Information Leakage released by China Consumers Association as an example and combined a qualitative analysis with a quantitative analysis. This study examined the main types and causes of personal information right infringements, and the systematic regulation of the protection of the right to personal information in the big data era. This effort identified a means by which to create a balanced relationship between effective protection and reasonable use of personal information.

Analysis of Victims’ Personalities

The value of personal information has grown during the era of big data, and the security of personal information has become increasingly important. According to Information Full Life Cycle Theory proposed by Horton, a U.S. Information Resource Management scientist, information is a resource with a life cycle, and its life cycle is composed of a series of logically related stages or steps, which are based on the information carrier and information exchange. The information life cycle includes 10 stages: creation, exchange, use, maintenance, retrieval, reuse, repackaging, re-exchange, downgrading, and disposal (Horton, 1985). Among these stages, information collection, storage, and circulation are the key links that easily lead to personal information leakage. We used the Survey Report on App Personal Information Leakage released by China Consumers Association as an example and found that it was common for mobile apps to over-collect personal information. The analysis of the process of personal information collection, storage and circulation revealed that the unauthorized collection of user information, intentional release of user information, and intentional sale of the user information represented the main forms of personal information rights violations (shown in Figure 1). From this point of view, unauthorized and illegal acquisition, illegal provision, and illegal transactions were important sources of personal information leakage. The types of personal information rights infringed upon were concentrated in illegal acquisition during information collection, provision in the storage sector, and use while in circulation.

Personal Information Obtained Illegally

In practice, e-commerce platforms, social media platforms, mobile device terminals, fixed device terminals, scientific research, and national management activities all collect and obtain a large amount of personal information. As one scholar has noted, “From an economic perspective, companies internalize the benefits of using information but externalize some of their losses, so that there exists a systematic incentive of overusing information” (Peter & Litany, 1998). With the increasingly prominent commercial and social value placed on personal information in the big data era, commodity service providers often collect and analyze personal information as to engage in targeted marketing and scientific market decisions. The strategy may be summarized as follows:

If we perfectly amalgamate the data from different social networking services, we can construct a better and comprehensive personal information (profile) of a user for improving many online services; such as item recommendation, community detection, online marketing, etc. (Ahmad & Ali, 2019).

However, the pressing demand for market data, as well as the low cost of personal information data, has led to a situation in which information collection devoid of external supervision has created incentives to extend the range of personal information collected. The exaggerated collection of personal information on platforms has taken primarily three forms. First, personal information was improperly collected during the purchasing or selling process on commercial platforms. To achieve targeted market share, better goods or services, operators often are expected to make accurate market decisions through an analysis of customers’ consumer tendencies. Therefore, they asked customers to provide unnecessary personal information during the process of purchasing goods and services. Alternatively, customers were offered gifts or discounts in exchange for information. Second, network service providers or operators used their technical advantages to improperly collect personal information on social platforms. These means of personal data collection often proved quite subtle, frequently relying on network
behavior traces, cookie records of personal online operations, network background vulnerabilities, and applets. Third, software developers or providers improperly collected personal information through software functions, such as positioning, monitoring, and automatic feedback during the development process. Software developers or providers argued that everything they did was to improve user experience. However, often they were assuring access to personal locations, communications, transactions, and even behavioral information without the user’s consent.

Personal Information Provided Illegally

There are many types of personal information that were illegally provided, including information concerning identity, addresses, travel, location, accommodations, credit, transactions, health, and other areas that could be used to identify an individual or learn about their activities. According to the Judicial Interpretation on Criminal Cases Involving Infringement of Citizens’ Personal Information, personal information has been provided through four illegal means. First, location information was provided and then used by others to commit a crime or provided despite awareness of the fact that the information would be used for a criminal offense. Location information has been determined to be related to personal free will and freedom of action. Information leaked for an illegal purpose, represents a serious challenge to the social order and endangers personal safety and societal security. For example, a defendant (Mr. Zeng) used his position as a police officer of the Hecheng Police Station in the Gaoming Branch of the Foshan Public Security Bureau to query a victim’s car traveling data and provided it to the perpetrator. Consequently, the victim was illegally detained. Mr. Zeng actions represented an infringement of personal information.9

A second way that information could be illegal provided would be when sensitive information about location, communications, credit, and property could be provided to a third-party. The owner of personal information was under strict obligation to assure the security of that information. For example, a defendant (Mr. Xu) provided 22 bank credit reports to others while serving as the account manager of Gongbei Port Sub-branch of PingAn Bank of China. Mr. Xu did not do it for profit. However, he committed a crime of personal information infringement.10

A third way that information provided was determined to be illegal would be if it compromised someone’s personal safety or property. There have been approximately 500 distinct pieces of personal information identified that have undermined personal and property safety. Some examples include accommodation information, communication records, health information, and transaction records.
Because an individual’s involvement in social activities could be considered to be sensitive personal information, it should remain confidential as a means to maintain public order. For example, there was the case of a defendant, Mr. Tang, who took advantage of his position as an employee of the remote banking online banking department of the China Merchants Bank Shekou Headquarters to retrieve more than 200 copies of bank customer account balances and transaction records. He proceeded to provide them to others for illegal purposes. Mr. Tang was guilty of illegally providing citizens’ personal information.11

The fourth way that personal information could be provided illegally would be the release of any of 5,000 types of data identified. Compared to information considered to be personally sensitive and important information, the leakage of general information would cause the least social harm. However, a large disclosure of general information also would constitute the illegal provision of personal information. Additionally, personal information obtained during the course of employment or service delivery and sharing that with third parties would be illegal.

**Illegal Use of Personal Information**

A variety of polls and survey reports have demonstrated that people have a strong interest in the protection of privacy and personal information (Nisenbaum, 2010). The illegal use of personal information actually exceeded the limit of fair use stipulated by Chinese law, in which the owner of information should endure only minor harm from the use of personal information by others (Chen, 2019). Common forms of violations of the purchase of personal information included: business promotion, the registration of a Taobao account intended for scalping, the creation of a fake ID photocopy for Alipay real-name authentication, bank credit card information used to steal credit cards in the name of others, and impersonation of public security agencies or bank staff. For example, criminals purchased the leaked personal information of Xu Yuyu via the Internet for the purpose of illegal possession and impersonated the staff of state agencies to carry out targeted telecom fraud, resulting in the loss of life and finances.14 In *N.Y. Times Co. v. United States*, the Supreme Court of the United States held that even though the Pentagon Papers were merely factual information, the disclosure of the information itself could constitute views or opinions, which are protected by the free speech clause in the United States.15 In 1977, the U.S. Supreme Court in *Whalen v. Roe* made clear that the government’s handling of personal information was a matter of constitutional privacy.16 In addition, personal information has been leaked by banks, educational institutions, telecom enterprises, delivery service providers, securities, firms, and e-commerce companies. The unreasonable exploitation of personal information by big data companies also has constituted an illegal use of personal information. In particular, the use of technological advantages to identify the information subject through the user’s traces has resulted in making the information subject vulnerable to privacy leakage and the improper use of Alipay and financial accounts.

**Analysis of Possible Explanations for Leaks**

The accumulation of the value of personal information is reflected. Although certain types of personal information packaged and processed are not for the purpose of identifying individuals, such treatment after classification will also result in the infringement of the rights of personal information subject (Wang, 2018). We used the Survey Report on App Personal Information Leakage released by China Consumers Association as an example and found that the primary reasons for personal information disclosure were as follows: weak awareness of security protection, inadequate supervision, imperfect laws, and difficulty in technical evidence collection (shown in Figure 2). Upon further analysis and reflection, it could be concluded that existing legal and judicial protection, sanctions, and mechanisms for the enforcement of information rights proved insufficient, high-tech capabilities tended to be underestimated, the informed consent mechanism proved nominal, legislative protections lagged, and administrative supervision was rather weak in the face of the serious consequences of rampant leakage and illegal activity. All of these have contributed to the argument that personal information in the big data era is insufficiently protected. There are several possible explanations for this lack of protection.

**Limitations of the Technologies Used**

During the “pre-information era,” personal information was stored in physical space on hardware. The total amount of information and the risks of information leakage were small in comparison to the current situation. Therefore, what damage resulted was minor. Additionally, the anonymization of personal information further reduced the risk of information leakage. However, in the era of big data that is no longer true. As one scholar has noted, where there exists a large amount of user identity information, attribute information and behavior information, and the possibility of cross-checking of data across channels, privacy is very fragile (Zhang et al., 2014). Anonymity has gradually disappeared. Another scholar observed that “the highly interconnected nature of the Internet, and the vast and growing volume of data found there, make even the most innocuous-seeming information capable of being linked to an identified individual” (Fred, 2010). At the same time, the development and application of storage technology, has made obsolete the need for a physical device on which to store massive amounts of personal information. Instead, network virtual storage has become increasingly common. The lack of attention to the security
risks posed by the high-tech means adopted to store personal information has made it possible for lawbreakers to obtain a large amount of personal information illegally through technical loopholes or attacks on the technologies. This situation has heightened the risk of large-scale leaks of personal information. Additionally, the high cost of technical protection measures, such as encryption technology, has informed decisions to ignore or reduce investments that could address the problem of leakage.

The Falsification of Informed Consent

The basic premise of the informed consent mechanism is the existence of an informed and rational individual who can make appropriate decisions regarding the collection, storage, use, and disclosure of various forms of personal data (Liu, 2017). Individuals could and should control all personal information. However, the application of big data analysis technology makes the dichotomy of personally identifiable information and non-personally identifiable information meaningless (Liu, 2019). Following data fusion and cross-validation, the subject of the information subject could be identified through multiple sources of unidentified information. As one scholar noted,

In an ecosystem where personal information is intensively collected and transferred by multiple parties, users in many cases are unaware of the collection of their information, making it difficult to exercise rights over first-party collectors, let alone exercise control over third-party institutions with which direct contact is hard to be established (Fan, 2016).

It would seem that personal information has been valued yet treated rather carelessly. On the e-commerce platform, for example, consent often has been a prerequisite for obtaining services. Therefore, consumers have had no choice but to consent to obtain the services and goods they need; the option of consent or choice has proved meaningless and impractical. Most people merely have skimmed or even ignored the privacy terms or policies offered by merchants or platforms. Merchants or platforms often have used formatted
contracts to obtain user consent and authorization for all possible uses, due to cost. The informed consent mechanism has proved practically useless.

**The Lag of Legislative Protections**

There were nearly 100 regulations on personal information protection in China by 2021. They could be divided into five broad categories of regulations: direct legal provisions, indirect legal provisions, national standards, industry self-regulation standards, and judicial interpretations. There are numerous examples, including the following: Articles 111 and 127 of the General Principles of Civil Law that stipulate the protection of virtual property in data networks as well as the personal information of natural persons; Article 286 of the Criminal Law Amendment (9) that clarified criminal penalties for the infringement of personal information rights by network service providers; the Liability under Internet Security Law Provisions on the Protection of Personal Information of Telecommunications and Internet Users; Postal Law, Commercial Bank Law, Law on the Protection of Women’s and Children’s Rights and Interests, Law on the Protection of Minors; and Information Security Technology—Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems. This list is not even comprehensive. The People’s Republic of China has enacted personal information regulations and guidelines that cover telecommunications, banking, insurance, securities, and credit reporting as well as other industries and sectors. Yet the country’s personal information protection efforts have been fragmented and it is not crystal clear about what interests are to be ensured. In addition, the legal effect is rather low, and the role and jurisdiction of law enforcement agencies are not clearly defined (Zhang, 2015). This is why the deficiencies concerning legal protection of personal information have continued.

**The Lack of Administrative Supervision**

The mining, comparing, and exploitation of personal information have become the main sources of the creation of value. As has been noted,

The existence of multiple information processing entities and the lack of direct contact with users has made third-party entities, especially data intermediates, the subsequent users of personal information beyond the reach of supervision (Liu, 2019).

To date, there have been no regulatory bodies with unified oversight. The regulatory function of the Ministry of Industry and Information Technology in China is limited to the internet industry and the telecommunications industry. Moreover, the administrative department has imposed merely light penalties on those found guilty of personal information leakage. In Article 23 of the Provisions on the Protection of Personal Information of Telecommunications and Internet Users and Article 17 of the Provisions on the Registration of Real Identity Information of Telephone Users, the telecom regulator only has been required to issue warnings and fines of between 10,000 and 30,000 Yuan. Given the large profits earned from the leakage of personal information, such fines have proved too low to curb the illegal collection and sale of personal information (Shi, 2013).

**Potential Improvements to Current Law**

A legal fiction is a revelation of the normative structure; it is also a theoretical improvement based on norms (Maine, 1984). In the big data era, the norms of personal information rights protection have revolved around an empowered and responsible subject. It would prove crucial to identify the party responsible for the protection and the means used to protect. Additionally, there would be a need to shift from the identification to the control of risk in efforts to regulate responsible subjects. That is, there should exist a system of responsibility for data users globally. Legislative norms have transformed from a fragmented to a unified system regarding personal information. The process for the protection of data should entail a multi-faceted approach that includes supervision, self-regulation and management systems for personal information management, personal information security, administration supervision, and industry self-regulation would all have to be put in place. Contentious jurisdiction could be addressed with a multifaceted approach: personal information litigation takes place across the space of the network and real society. Therefore, efforts should be devoted to achieving unified national legislation, strengthen the oversight of implementation, improve data use security management by enterprises, support the establishment of self-regulation by industries, and provide relief for infringements. It is not only beneficial to punish the offenders, but also can provide general warnings to society, prevent the occurrence of infringement, and better safeguard social harmony and stability (Yang, 2018).

**The Responsible Subject: From Identifiability to Risk Control**

The principle of informed consent has been widely used to protect personal information rights globally for a long time. Data collectors should not only obtain the consent of the owner of the personal information, but also clearly inform them of the scope and purpose of the collected data. That type of protection has had a significant effect on personal information rights in the “pre-information age.” However, as some scholars have noted, “[. . .] because a large part of the value of data is reflected in secondary uses, and data collection does not take this into account, the action of informing and permitting can’t be helpful” (Victor, 2013). However, as
another scholar has observed, how to ensure the authenticity, validity, and remedy of consent remains unclear (Jinn, 2017). Therefore, there needs to be a shift from a focus on personal information rights protection from the perspective of their owners to the regulation of personal information users. The regulation of data users should be central to efforts designed to protect personal information rights. Consequently, a data user responsibility system would emerge and the obligations and responsibility of personal information rights protection would be transferred to data collectors and users. Furthermore, we could establish a scenario-based risk assessment mechanism and promote diversified subjects to jointly safeguard personal information rights (Zhang & Zhou, 2019). The effective protection and rational utilization of personal information rights should be implemented. Data users know more about the secondary use of data value, and it would prove more feasible for them to evaluate the risks associated with the use of personal information. A data user responsibility system would force the user to strengthen risk management. The threat of liability could serve as an incentive for them to evaluate the risks associated with the collection, processing, analysis and mining of personal information. The protection of personal information rights should be strengthened for further prevention.

**The Legislative Norms Adopted: From Fragmentation to Systematization**

China’s personal information legislation has yet to have shifted from protection from decentralized legislation, a focus on the credit industry, and limited legislative attention to the Internet. The country’s protections have suffered from unclear protection objectives, a lack of information with regard to subject rights, incomplete rights and obligations, as well as inadequate legal responsibilities (Wang, 2016). The legislative norms for personal information rights protection in the big data era have focused on the formation of a unified legislative system for personal information, and make it clear that personal information rights have independent value and connotation (Zhang & Han, 2016). We should enact the Law of Personal Information Protection as soon as possible. The old fragmented legislative norms should be transformed into a systematic normative framework to build a sound legal system for personal information protection. The national personal information protection law not only should be promulgated, but corresponding legislative norms also should be implemented for different industries. They could regulate the illegal actions of the government departments, e-commerce platforms, and public social platforms that infringe upon personal information rights. There also should be standards for the strict protection of information by public service enterprises and institutions, such as telecommunications, banking, finance, transportation, education, and healthcare. Moreover, the application of the industry’s self-regulatory code should be encouraged to achieve the effective protection and rational use of personal information equity.

**The Process Protection: Supervision, Self-Regulation, and Management**

The property interests and commercial value of personal information have attracted much attention. The intentional or unintentional infringement of those rights has become increasingly frequent. There has been a growing consensus about the need to strengthen national supervision, enhance industry self-regulation, and improve security management. A first step would be to create a unified organization responsible for oversight on a national level. The Ministry of Industry and Information Technology in China shall carry out general supervision over the implementation of the Personal Information Protection Law, conduct research and consultation on personal information protection, and submit work reports regularly (Liu, 2007b). The second step would be to strengthen the implementation of supervision and regulate national standards for the collection, processing, analysis, mining, utilization, and storage of personal information. The third step would be to promote the creation of specialized evaluation institutions and encourage the development of third-party service markets responsible for the protection of personal information. Fourth, administrative discipline and punishment should take place promptly. Enterprises should be encouraged to self-regulate through the use of reporting, exposure, and blacklist systems. Self-regulation could be achieved through organizations represented primarily by the banking and telecommunication industries, important websites, and social platforms. Technology companies should be formed to elaborate self-regulatory norms for data collection and use. Fixed supervision and management agencies and personnel could be created to ensure effective compliance with industry standards. The mechanisms for punishment also need to be updated. There should be greater internal management and punishment for industry malfeasance through the use of warnings and other measures. Security management should be developed to ensure internal data information protection and develop a data information risk control system to normalize vulnerability verification and emergency follow-up procedures. Additionally, a system for the safe transmission and utilization of personal information that would ensure confidentiality and the integrity of the process should be created. There also should be efforts to build a personal information security technology protection system and adopt critical technologies for big data security that would include the following: anonymous protection technology for the release of data, anonymous protection technology for social networks, data watermarking technology, and data traceability technology (Feng et al., 2014). Finally, security management should include a legal training system for employees that could be targeted to them in accordance with their different levels of data access. The purpose
of such training would be to improve employees’ understandings of legal issues and reduce the risk of leakage.

Relief Protection: Spanning Cyberspace and Real Society

The subject of rights and the subject of infringement often are separated geographically. Criminal behavior does not only occur in cyberspace, and it can also occur in the two platforms of cyberspace and real society at the same time (Yu, 2013). The resolution of existing litigation jurisdiction regarding personal information is imperative. The experience of The Internet Court of Hangzhou provides a useful example of ways to explore a new trial mode for Internet-related cases, establish a network trial process, perfect the system specification, and establish an efficient, convenient and low-cost network trial mechanism (Zhou, 2017).

Litigious parties could adopt the jurisdiction mode agreed upon and be centralized by special courts, which would address the problem of the denial of personal information rights in the context of disputes that expand across regions, borders, and airspace. Electronic evidence data preservation and information communication technologies could be used to examine matters such as identity authentication, electronic service, and burden of proof all of which entail online filing, consultation, mediation, and trials. The ability to improve the efficiency of approvals would save litigation costs. The problem of evidence admissibility could be addressed through the adoption of a doctrine of presumption, compensation for injured parties, and a guarantee of personal information protection in the future.

Conclusion

Personal information in the big era represents a symbol of a natural person. The information may guarantee the personality value of its social existence. Personal information is still highly valued, but its property value is of greater concern to society. Today, personal information has become a fundamental strategic resource with important market value. It is urgent to standardize the protection of personal information rights. Focused on the empowered and responsible subject, we can develop a system of responsibility for data users; a unified system regarding personal information; supervision, self-regulation, and management systems for personal information management; personal information security; administration supervision; and industry self-regulation. In addition, we can construct a dynamic risk prevention system for personal information by empowering the subject that could identify personal information and control the subject that holds the personal information. It would prove beneficial to understand the value of effective protection as well as the rational utilization of personal information. We could promote localization of personal information rights protection in the big data era through the criminalization of violations and other means to address these urgent concerns for greater protection. Future research could further explore the means to enhance the protection of personal information.

Acknowledgments

We would like to thank LetPub (www.letpub.com) for providing linguistic assistance during the preparation of this manuscript.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by National Office for Philosophy and Social Sciences in China “Research on Personal Information Rights and Obligations System from the Perspective of Data Strategy” (No. 17BFX193).

ORCID iD

Zongyu Song https://orcid.org/0000-0001-8679-1322

Notes

1. Report about Federal Trade Commission launches probe into Facebook’s privacy practices. See https://www.sharecast.com/news/international-companies/federal-trade-commission-launches-probe-into-facebook-privacy-practices-3212377.html.
2. Report about Twitter discloses hashing bug, recommends that everyone change their password. See https://venturebeat.com/2018/05/03/twitter-discloses-hashing-bug-recommends-that-everyone-change-their-password.
3. See http://news.cctv.com/2018/08/29/ARTIJS0HUzjL8or3ewnb3oa180829.shtml.
4. See https://www.bbtnews.com.cn/2020/1103/375017.shtml.
5. See https://ishare.ifeng.com/c/s/7uy7bsyQuBF.
6. See The Californian Customer Privacy Act of 2018, §1798.110.(a), 100.(d), 105.(a), 120.(a).
7. This survey report was conducted by China Consumers Association from 17 July to 13 August 2018 by means of an online survey, with 5,458 valid questionnaires from online consumers, and included information on the frequency of personal information leaks, the ways in which personal information is leaked, and the methods to avoid personal information leaks, etc. For details, see China Consumers Association: The Survey Report on App Personal Information Leakage. http://www.cca.org.cn/jmxf/detail/28180.html?tdsourcetag=s_pctim_aiomsg.
8. Interpretations of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Application of Law in Handling Criminal Cases Involving Citizens’ Personal Information (2017). See https://www.spp.gov.cn/xwfbh/wsfbt/201705/20170509_190088.shtml.
9. See the Sanshui District People’s Court, Foshan City, Guangdong Province (2015) FoSanfaXing Chu Zi No. 99 Criminal Judgement. See https://wenshu.court.gov.cn/website/
References

Ahmad, W., & Ali, R. (2019). Social account matching in online social media using cross-linked posts. *Procedia Computer Science*, 152, 222–229.

Chen, L. (2018). Research on criminal protection boundaries on personal information. *Journal of Henan University (Social Science)*, 58(3), 72.

Chen, J. (2019). Research on the fair use system of personal information in the big data era—Taking 773 criminal judgments published in 2011-2017 as research samples. *Journal of Dalian University of Technology (Social Science Edition)*, (2), 90.

Cheng, X. (2019). Protection of personal information from the perspectives of the compilation of civil code. *China Legal Science*, (4), 26.

Ding, X. (2018). Dilemma and outlet of private legal protection of personal information. *Chinese Journal of Law*, (6), 194.

Fan, W. (2016). The path reconstruction of personal information protection in the age of big data. *Global Law Review*, (5), 94.

Feng, D., Zhang, M., & Li, H. (2014). Big data security and privacy protection. *Chinese Journal of Computers*, (1), 250–253.

Fred, H. C. (2010). Protecting privacy in health research: The limits of individual choice. *California Law Review*, 98(6), 1775.

Gao, F. (2018). Protection of personal information: From individual control to social control. *Chinese Journal of Law*, (3), 84.

Guo, P. (2011). Individual information rights and EU protection. *Journal of Political Science and Law*, (1), 8–9.

Horton, F. W. (1985). *Information resources management* (pp. 20–21). Prentice-Hall.

Ji, L. (2017). Comparative study of legislation path of personal information protection. *Library Development*, (9), 19.

Jiang, P. (2019). Research on the theoretical dilemma and protection path of personal information protection in the big data era. *Journal of Modern Information*, 39(6), 151.

Jinn, Y. (2017). The review and remodeling of the rules of personal information protection for consumers—Based on the privacy control theory. *Zhejiang Social Science*, (11), 61.

Li, C. (2019). On the methodology of legal analysis of AI: Taking copyright as an example. *Intellectual Property*, (7), 14.

Litman, J. (2000). Information privacy/information property. *Stanford Law Review*, 52(5), 1283–1313.

Liu, D. (2007a). Proprietary right protection of personal information. *Chinese Journal of Law*, (3), 89.

Liu, J. (2016). Legal research on personal information protection in the Era of Big Data (pp. 24–26). Zhejiang University.

Liu, J. (2017). Personal information and rights system—The dilemma and future of right to information self-determination (p. 57). Law Press China.

Liu, W. (2007b). On the protection of personal information by administrative. *Administrative Law Review*, (2), 33–34.

Liu, Y. (2019). Rethinking personal information protection in the Era of big Data—From the perspective of the public welfare of big data development. *Journal of Social Science*, (3), 103.

Marine, H. S. (1984). *Ancient Law* (p. 15). The Commercial Press.

Nisenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life* (pp. 104–105). Stanford University Press.

Peter, P. S., & Litany, R. E. (1998). *None of your business: World data flow, electronic commerce, and the European privacy directives* (p. 8). Booking Institution Press.

Samuelson, P. (2007). Principles for resolving conflicts between trade secrets and the first amendment. *The Hastings Law Journal*, 58(4), 777.

Shi, J. (2012). Personal information protection legislation in network environment. *Journal of Suzhou University*, (6), 92–93.

Shi, W. (2013). Personal information in big data era: Predicament and path selection. *Journal of Intelligence*, (12), 158.

Victor, M. S. (2013). *A Revolution: That will transform how we live, and think* (S. Yangyan & Z. Tao, Trans. p. 220)). Zhejiang People’s Publishing House.

Wang, L. (2013). Legal protection of personal information: Entered on the line between personal information and privacy. *Modern Law Science*, (4), 62.

Wang, M., & Jiang, Z. (2016). A comparative study on the protection of personal privacy between China and the United States in the era of big data—A comparative analysis based on the latest privacy policies and regulations of the two countries. *Journalism and Mass Communication Monthly*, (15), 55.

Wang, S., & Du, W. (2017). The progress of personal privacy protection in New Zealand in the era of Big Data and its enlightenment to China. *E-Government*, (11), 65.

Wang, X. (2016). Empirical research on the legislative protection of personal information in China. *Orient Law*, (3), 66.

Wang, X. (2018). The reconstruction of personal information law system in big data era. *Legal Forum*, (6), 117–118.

Wei, J., & Song, R. (2018). Legal protection of personal information rights in Japan and its reference. *Journal of Shenyang University of Technology (Social Science Edition)*, (7), 1–2.

Yang, L. (2018). Personal information: Legal interest or civil rights—An interpretation of “personal information” in Article 111 of the General Principles of the Civil Law. *Legal Forum*, (1), 44–45.

Yu, Z. (2013). The applicable space of traditional criminal law in double-layer society—Against the judicial interpretation on Internet defamation issued by the Supreme People’s procuratorate and the Supreme People’s Court. *Law Science*, (10), 68–69.
Zhang, H., & Zhou, X. (2019). The legal path of personal information protection in the Era of big data. Journal of Guizhou University (Social Science Edition), (2), 69.
Zhang, L., & Han, X. (2016). The private law nature of personal information right in the Big data era. Legal Forum, (3), 119–129.
Zhang, M. (2017). The formulation of the general principles of the civil law of the people’s Republic of China. Chinese Law Science, (2), 13.
Zhang, N., Zhang, Y., & Hu, K. (2014). Big data security: Technology and application (pp. 62–72). People’s Posts and Telecommunications Press.
Zhang, X. (2015). From privacy to personal information: Theoretical and institutional arrangements for reweighing interests. China Legal Science, (3), 44–45.
Zhou, H. (2018a). Explore the way to encourage compatible personal data governance—The legislative direction of China’s personal information protection law. Law Research, (2), 6.
Zhou, H. (2018b). Exploring an incentive-compatible personal information protection regime. Chinese Journal of Law, (2), 3–23.
Zhou, Q. (2017). Vigorously strengthen the Internet court in Hang Zhou and explore an innovative model for Internet justice with the purpose of serving and ensuring the Internet power strategy. China Review of Administration of Justice, (5), 3–4.