FRONTIERS OF LAW IN CHINA
VOL. 13 SEPTEMBER 2018 NO. 3
DOI 10.3868/s050-007-018-0029-6

SPECIAL ISSUE

PARADIGMS OF INTERNET REGULATION IN THE EUROPEAN UNION AND CHINA

PERSONAL DATA PROTECTION: RETHINKING THE REASONS, NATURE, AND LEGAL FRAMEWORK

DING Xiaodong[*]

Abstract This paper rethinks the reasons for and the nature and means of personal data protection. The reasons for personal data protection are that it could promote the fairness and effectiveness of information flow, help individuals develop their independent personality, and equip them to deal with risks. With respect to the nature of personal data, this paper argues that such data should not be perceived from a purely individualistic point of view. Rather, there should be a contextualized understanding of the data, which considers the appropriate information flow of personal data within a particular context. Regarding the legal framework of personal data protection, this paper suggests that consumer protection law and public law are better equipped to protect personal data than tort, contract, or property law.

Keywords privacy, data protection, context, information flow, individualism

INTRODUCTION ····· 380
I. WHY SHOULD WE PROTECT PERSONAL DATA? ····· 382
II. WHAT IS PERSONAL DATA? ····· 384
III. HOW CAN WE PROTECT PERSONAL DATA? ····· 386
CONCLUSION ····· 389

INTRODUCTION

With the advent of the information age, the protection of personal data has achieved a consensus position. In the European Union (EU), the European Parliament and the Council have passed the General Data Protection Regulation (GDPR), which aims to return control to citizens and residents over their personal data and simplify the regulatory environment for international business by unifying the regulations within the EU. In China, the government is busy drafting a bill that would ensure comprehensive protection

[*] (丁晓东) Ph.D. in law, Law School, Peking University, Beijing, China; J.S.D., Yale Law School, New Haven, USA; Associate Professor, School of Law, Renmin University of China, Beijing 100872, China. Contact: dingruc@163.com

of data privacy. In the United States, as well, there are many specific laws to regulate personal data in different areas.

However, despite reaching a global consensus on personal data protection, several questions remain unanswered. First, why is there a need to protect personal data? What is the legitimate justification for such protection? Second, what is the essence of personal data? Do personal data naturally belong to individuals and, therefore, should individuals be endowed with an exclusive right to it, regardless of whether it is a property right or a right of personality? Third, what is the appropriate method for protecting personal data? Should law protect personal data through contract law, tort law, public law, or consumer protection law?

With respect to China, these are not simply theoretical questions that have been discussed by the academia for decades; they are questions that could significantly affect legal practice and even the future development of the entire internet industry. One example is the debate over the interpretation of Article 111 of the newly enacted General Principles of the Civil Law (GPCL), which states that "the personal information of a natural person shall be protected by law. Any organization or individual needing to obtain the personal information of other persons shall legally obtain and ensure the security of such information, and shall not illegally collect, use, process, or transmit the personal information of other persons, nor illegally buy, sell, provide, or publish the personal information of other persons."[1] For some, the enactment of Article 111 of GPCL implies that China endorses citizens' fundamental right to "information self-determination." However, others argue that this article only admits the need for personal information protection and does not mention the right to personal information as a fundamental right. During such a debate, answers for the aforementioned fundamental questions will inevitably be sought, especially for the question of whether individuals should be endowed with an exclusive right to their personal data. As pointed out by Ronald Dworkin, law always includes principles that are necessary to derive particular legal rights and duties. Legal interpreters must always engage in theoretical debate on the specific meaning of a rule.[2]

Another case is the ongoing discussion on the legislative model to be adopted for China's personal information protection law. Although there is general agreement on the legislative plan to enact a separate personal information law, we are yet to reach any kind of consensus regarding the standard, content, and method of this law. For example, some people argue that China should adopt the American model, which follows a market-oriented approach for data protection. The main reason is that they believe a strict data protection law will not be in the best interest of China, who is a major player in the

---

[1] Art. 111, General Principles of the Civil Law of the People's Republic of China.

[2] See generally Ronald Dworkin, *The Model of Rules*, 35 Chicago Law Review, 14 (1967).

global technology field. Therefore, the new legislation should not include rights such as the "right to be forgotten" and "rights to data portability." However, others argue that China should follow the European model, which enhances individuals' control over their personal data. For these people, a higher standard of data protection is consistent with the reason, nature, and means of data privacy protection. Further, there are people who believe that China should seek a third road.

Against this background, this paper attempts to answer the fundamental questions mentioned above within the Chinese context. It examines the reasons for and the nature and means of data privacy protection. In this paper, Part I discusses why there is a need for data protection. Part II studies the nature of personal data. Finally, Part III examines the legal framework that should be adopted to protect data privacy.

I. WHY SHOULD WE PROTECT PERSONAL DATA?

It seems redundant to ask why there is a need for protecting personal data. People naturally consider personal data to be part of their privacy, which is a basic right that should be enjoyed by every citizen. However, it is noted that the legal protection of privacy has a history of only one hundred years. It was only after Samuel Warren and Louis Brandies published their classic article titled "The Right to Privacy" that the right to privacy gradually gained focus worldwide.[3] Meanwhile, many people do not consider the privacy right a fundamental legal right. According to them, privacy is more a way to disguise oneself than a legitimate interest.

Indeed, many people have proposed the "nothing to hide" argument to oppose the protection of personal data. In discussions on whether breach of personal data or data mining poses a threat to privacy, many people respond that they have nothing to hide. For instance, a blogger proclaims, "So, I don't mind people wanting to find out things about me. I've got nothing to hide!" The nothing to hide argument and its variants, as pointed out by data privacy specialist Daniel Solove, "are quite prevalent in popular discourse about privacy."[4]

One may respond to the nothing to hide argument with the following quick response: Do you have curtains at home? Do you want to have a private life that is not known to anyone else? However, such responses are not sufficient to answer the questions proposed above. It is noted that the intrusion of private life at home is very different from the disclosure of one's personal data to third parties. There is no direct interference of private life in the breach of personal data. Besides, the nothing to hide argument does have a

[3] See generally Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review, 193 (1890).

[4] Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego Law Review, 745 (2007).

credit. It rightly points out the importance of the free flow of information. The free flow of information is beneficial to society in that it would lessen the problem of information asymmetry and, under certain circumstances, help reveal the shameful secrets of some people.

Hence, we should find new responses to the nothing to hide argument. Fortunately, scholars have already carried out much research on this question. A review of this research will help us better understand the legitimate foundation of data privacy protection.

First, we should understand that the nothing to hide argument does not consider the problem of fairness of information flow. It is true that the free flow of information within the public sphere is a general good that would help us achieve a better understanding of each other. However, it is also noteworthy that the flow of information is not always fair or legitimate. Many people presuppose that there exists a "market place of ideas or information."[5] However, even if we accept the existence of such an information market, we still need to be aware that there is unethical or illegitimate acquisition of personal data. For example, many companies simply collect personal data without the consent or clear authorization of individuals.

Second, the nothing to hide argument does not consider the effectiveness of information flow. The nothing to hide argument argues that information flow is beneficial to society in that it would reduce information asymmetry; however, it is noted that there are different types of information or knowledge. In his book titled *The Unwanted Gaze*, Jeffrey Rosen emphasizes the "true knowledge of another person, in all of his or her complexity," which "can be achieved only with a handful of friends, lovers, or family members."[6] He reminds us that we now live in a world in which "information can be easily confused with knowledge"; however, "information wrenched out of context is no substitute for the genuine knowledge that can only emerge slowly over time."[7] Therefore, Rosen argues that not all information disclosed to the public would promote the effectiveness of information flow. On the contrary, the public disclosure of superficial knowledge would, under many circumstances, cause error and misrepresentation.

Third, the nothing to hide argument ignores the value of privacy in ensuring the autonomy and independence of individual citizens. As Julie Cohen points out, "the self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate." Privacy "shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render

---

[5] See *Abrams v. United States*, 250 U.S., 630 (1919).

[6] Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, Random House (New York), at 8 (2000).

[7] Id. at 10.

individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops."[8]

Fourth, the nothing to hide argument ignores the risk posed by the breach of personal data. This argument claims that only people with skeletons in the closet require privacy protection; however, it is pointed out that even innocent individuals would face great danger if their personal data are not properly protected. For example, telecommunication fraud occurs largely because fraudsters manage to illegally obtain certain personal data. A tragic case of this type drew much public attention in China in 2016. The victim, an 18-year-old girl named XU Yuyu who was about to start her college education, died from a heart attack after her tuition fees, which were raised by her family, were swindled in a telephone scam. In this case, the fraudsters illegally obtained XU Yuyu's personal information and defrauded her by claiming that they wanted to award her a student grant. It was with the help of leaked personal data that the fraudsters could win XU Yuyu's trust.

In conclusion, there is a legitimate foundation for the protection of personal data. Although free flow of information is generally beneficial to society and privacy protection might slow down this flow of information, protection of privacy and personal data is beneficial to the society.

II. WHAT IS PERSONAL DATA?

After examining the reasons for protecting personal data, we proceed to the second question: What is personal data? Or rather, what is the nature of personal data?

Many scholars have researched this topic in detail. According to some researchers, individuals have property rights over their personal data, "because individuals generally have a legal right to exclude other people from access to their private data, they may have a sense that they have a property right in the data as well as a legal right to restrict access to it."[9] As summarized by Pamela Samuelson, even when "data about individuals are in the hands of others (such as banks, doctors, and insurance companies), individuals may perceive themselves to have a protectable interest in records of their financial transactions or medical histories. Because the law will sometimes protect these and other types of data from unauthorized uses and disclosures, this too may reinforce a sense of ownership in personal data."[10]

Many other scholars argue that individuals have a personality right or moral right over their personal data. They consider the right to personal data to be different from the right

[8] Julie E. Cohen, *What Privacy Is for*, 126 Harvard Law Review, 1905 (2013).

[9] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stanford Law Review, 1130 (2000).

[10] Id.

to property, of which the latter focuses on only the economic interests of individuals.[11] They argue that the fulfillment of one's personality is a core principle for protecting personal data, and such an approach to personal data protection is consistent with the right to dignity enshrined in the constitutions of many countries.[12] In line with this argument, Warren and Brandies formulated the right to privacy as the right to "an inviolate personality" and viewed "the right to privacy, as a part of the more general right to the immunity of the person — the right to one's personality."[13]

This paper does not intend to resolve the debate between the "property right" and "moral right" understanding of personal data. Both theories would face great difficulty if they were to view personal data from a purely individualistic perspective. The property right theory, for example, would greatly obstruct the free flow of information and formation of the public sphere. If individuals have an absolute property right over their personal data, we should always obtain the consent of others when we see their information. It would mean that a search of somebody's name on Facebook, Baidu, and Google would violate the person's property rights because an absolute property right means that an individual would have absolute control over his or her personal information. Similarly, if individuals naturally have moral rights over their personal data, then anyone could possibly claim that their moral right is infringed if they find others making any mistakes in their personal data. It would put others at an eternal risk of violating the law. For sensible and meaningful rights, both the property right and the moral right understanding of personal data must be viewed from a communitarian approach, rather than a purely individualistic one. Personal data belong to not only individuals but also the community. It is only by resorting to the communitarian standard that we can determine whether the right to personal data is a property right or a moral right and whether it has been infringed.[14]

The main argument of this paper is that the protection of personal data should always be considered in combination with the appropriate flow of information within a specific community. It is true that personal data should enjoy strict protection in this digital age. However, it is also noted that such protection aims at promoting the aforementioned values, not the existing natural rights of individuals over their personal data. Individuals do not have natural rights over their personal data or rights of informational

---

[11] Bart van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data,"* 31(80) Utrecht Journal of International and European Law, 25–50 (2015).

[12] See, for example, Arts. 1 and 2 of the German Basic Law.

[13] See van der Sloot, fn. 11 at 26; See Warren & Brandeis, fn. 3.

[14] See generally Robert C. Post, *The Social Foundations of Privacy: Community and the Self in the Common Law Tort*, 77 California Law Review, 957 (1989); Ari E. Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 Miami Law Review, 559 (2015).

self-determination. If individuals have exclusive rights over their personal data, regardless of whether these are property or moral rights, information would become largely privatized. No one is an island. Without appropriate information flow, all personal data would become meaningless.

To view personal data from the perspective of appropriate information flow, we should have a contextualized understanding of personal data protection. When considering the appropriate degree of personal data protection, we should always pay attention to the specific context. For example, we should consider whether the personal data have already become part of public information and whether the individual at issue is a "public figure." It is only by paying attention to these specific contexts that we can appropriately limit the scope and extent of personal data protection.[15]

III. HOW CAN WE PROTECT PERSONAL DATA?

The traditional legal method for protecting privacy is tort. When Warren and Brandeis developed a theory of privacy, they largely imagined protecting privacy through the common law tort. As widely known among privacy law scholars, William Prosser summarizes privacy torts into four categories: (1) intrusion upon seclusion, (2) public disclosure of embarrassing private facts, (3) false light publicity, and (4) appropriation of name or likeness.[16]

However, as pointed out by many scholars, the tort law of privacy has become ineffective in remedying the collection, use, and dissemination of personal data in this age of information. Danielle Citron argues that privacy torts have severe limitations in combating internet harassment.[17] Similarly, James Whitman states that "it is generally conceded that, after a century of legal history, [the privacy torts as inspired by Warren and Brandeis] amount to little in American practice today."[18] Finally, Lawrence Friedman states that "in hindsight, it looks as if the Warren and Brandeis idea of privacy — protection from the despicable nosiness of the media — never got much past the starting post; and is now effectively dead."[19]

The main reason for the ineffectiveness of the tort law of privacy is that the risk

---

[15] I adopted this idea from Helen Nissenbaum's work, in which Nissenbaum proposes a theory of contextual integrity. For Nissenbaum, privacy could only be understood by considering the appropriate information within a community. See generally Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Washington Law Review, 119 (2004); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press (Stanford), (2010).

[16] William L. Prosser, *Privacy*, 48 California Law Review, 388–389 (1960).

[17] Danielle K. Citron, *Cyber Civil Rights*, 89 Boston University Law Review, 89 (2009).

[18] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 Yale Law Journal, 1204 (2004).

[19] Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 Hofstra Law Review, 1125 (2002).

accompanying the collection, use, and dissemination of personal data is accumulative. There is usually no discernable harm in a single act of collecting, using, and disseminating personal data. However, a tort is a civil wrong that causes someone else to suffer loss or harm, resulting in legal liability for the person who commits the tortuous act. A tort requires the plaintiff to prove the existence of loss or harm.[20]

Therefore, some scholars have argued for endowing individuals with a property right over their personal data. According to these scholars, such a property right would enable individuals to bargain over the personal data that should be revealed to different firms for different purposes. Contrastingly, many other scholars recommend a contractual approach for the protection of personal data in cyberspace. Some suggest that the law should try to facilitate, and perhaps approximate, the "privacy agreement the two sides would reach if they were both well informed and it was not expensive to reach an agreement."[21]

In any case, the problem with property law and contract law is that both rely on individuals' self-management. However, privacy self-management is not very effective in resolving privacy breaches. As summarized by Daniel Solove, it has two broad problems: (1) cognitive problems, which comprise the challenges caused by the way in which human beings make decisions, and (2) structural problems, which refer to the challenges arising from the way privacy decisions are designed.[22]

With respect to cognitive problems, Solove points out that a number of cognitive problems plague privacy self-management. "Privacy self-management envisions an informed and rational person who makes appropriate decisions about whether to consent to various forms of collection, use, and disclosure of personal data." However, empirical evidence and social science literature demonstrate that "people's actual ability to make such informed and rational decisions does not even come close to the vision contemplated by privacy self-management."[23]

With respect to structural problems, Solove points out the problems of scale, aggregation, and assessing harm. First, although a person may be able to manage his or her privacy with a few entities, "privacy self-management does not scale well. Even if every entity provided people with an easy and clear way to manage their privacy, there

---

[20] See generally Diane L. Zimmerman, *Requiem for A Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell Law Review, 362 (1983).

[21] Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press (Washington, DC), at 8 (1998).

[22] See generally Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review, 1879 (2013).

[23] Id. at 1883. For the cognitive problem, see also George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 Journal of Interactive Marketing, 20–21 (2004); Lorrie F. Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 Journal on Telecommunications and High Technology Law, 274 (2012).

are simply too many entities that collect, use, and disclose people's data for the rational person to handle."[24] Second, even when people make rational decisions about sharing individual pieces of data in isolation, they "greatly struggle to factor in how their data might be aggregated in the future."[25] Third, people often favor immediate benefits over long-term ones even when there may be future detriments. "The aggregation effect shows that privacy is an issue of long-term information management, while most decisions to consent to the collection, use, or disclosure of data are tied to a short-term benefit."[26]

This paper does not completely abandon the privacy self-management approach, since privacy self-management does have certain virtues. For example, it could enhance the legitimacy of a company's collection, use, and dissemination of personal information. It could also help arouse individuals' awareness of protecting their own personal data. However, as shown above, privacy self-management has severe shortcomings that cannot be resolved easily. We can neither naively believe that individuals by themselves are fully equipped to manage their privacy nor completely rely on tort law, contract law, or property law to protect personal data.

Therefore, the appropriate means of protecting personal data should focus on consumer law and public law. Consumer law could help individuals to manage their privacy, particularly when they are facing big technology companies. Consumer protection law, as it is widely known, is an area of law that regulates private law relationships between individual consumers and businesses that sell various goods and services. It is a way of preventing frauds and scams from service and contracts. With respect to protecting personal data, consumer protection law could require big technology companies to disclose details regarding their collection and processing of consumers' personal data in a manner that is easily understood by consumers. Meanwhile, consumer protection law could also require big technology companies to provide additional protection of personal data to the most vulnerable sections of the society, such as minors.

On the other hand, public law could help the market to regulate risk, in general. It could require companies and other entities to conduct risk assessments and undertake substantial activities to reduce the risk that accompanies the collection, use, and dissemination of personal data. For example, it could require companies to implement technical and organizational measures to ensure a level of security appropriate to the potential risk, including "the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process

[24] See Solove, fn. 22.

[25] Id. at 1889.

[26] Id. at 1891.

for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."[27]

CONCLUSION

Personal data or personal information is a core concept of privacy protection in the information age. Many countries have already enacted or are intending to enact legislations to protect personal data. In order to understand the characteristics of data protection laws implemented worldwide, we should rethink the fundamental questions pertaining to personal data protection, such as the reasons for personal data protection, nature of personal data, and appropriate legal framework for personal data protection.

As suggested by this paper, the reasons for personal data protection are that it could promote the fairness and effectiveness of information flow, help individuals develop their independent personality, and make them well equipped to deal with risks. Regarding the nature of personal data, the most important thing we should remember is that personal data should not be viewed from a purely individualistic perspective. Rather, we should have a contextualized understanding of personal data protection and analyze the appropriate information flow of personal data within a particular context. Regarding the legal framework of personal data protection, this paper suggests that consumer protection law and public law are better equipped to protect personal data than tort law, contract law, or property law.

[27] Art. 32, GDPR.