Contemporary Social Sciences

2021 | Number 4 Article 7

2021

A Comparative Analysis of the Regulatory Approaches to Personal Data between the EU and the US

Shi Zhengyu
Renmin University of China

A Comparative Analysis of the Regulatory Approaches to Personal Data between the EU and the US

Shi Zhengyu*

Renmin University of China

Abstract: The regulatory approaches of the EU and the US in the realm of personal data remain to be studied. This article analyzes regulatory approaches of the two digital economy giants from a comparative perspective. It finds that even though huge divergences exist in the substantive rules of personal data protection between the EU and the US, they share the de facto common strategies that have been applied to the regulation. In particular, the regulation focus of personal data has been shifted to the internal data protection systems of private sectors. For regulators, collaborative governance and contextual approaches are the preference in comparison with traditional top-down regulation. On this basis, this article analyzes the current regulatory approaches of the EU and the US. As articulated by Ari Ezra Waldman, the shift of regulatory approaches can be categorized as a "second wave of privacy law." This article also points out the potential pitfalls the current approaches may fall into.

Keywords: regulatory approaches, collaborative governance, internal compliance systems, contextual approaches

DOI: http://dx.doi.org/10.19873/j.cnki.2096-0212.2021.04.007

* Shi Zhengyu, Law and Technology Institute, Renmin University of China.
Correspondence concerning this article should be addressed to Shi Zhengyu, Institute of Law and Technology, Renmin University of China, Beijing. E-mail: zhengyushi0709@163.com

Introduction

In the era of "big data," The EU and the US, as two giants in the domain of the digital economy, have seen their legal protection of personal data being the focus of academic analysis. Although the US has played an important role in the early stage of the formation of global personal data governance, the legal force outside the US, mainly the EU, has evolved to shape another new model of personal data regulation. A large number of articles have pointed out that this new model, through empowering individuals to strengthen personal control over personal data, has gradually expanded with the introduction and implementation of the *Data Protection Directive (officially Directive 95/46/EC)* and *the EU General Data Protection Regulation* (adopted in April 2016) (GDPR). This phenomenon is also described as "The Brussels Effect" by scholars (Greenleaf, 2018, pp. 18-56).

However, less light has been cast on exploring how and what kind of regulatory approaches the EU applies to promote its value and philosophy in data privacy governance.

In the GDPR, the frequently mentioned personal litigation, purely top-down, command-and-control regulation is one of the regulation tools of the EU, but in fact, the regulatory mechanisms in the GDPR are far more than these harder law enforcement methods, and are more inclined to encourage supervising authorities and private sectors to jointly cope with the challenges of personal data protection through collaborative governance.

As for information privacy protection in the US, it shows a different logic from that of the EU.[①] While the Internet economy is booming in the US, it has chosen to reinforce the protection of user information privacy through self-regulation within the industry, whereas nowadays the US information privacy regulatory approach cannot be simply understood from the perspective of self-regulation within the industry. The US Federal Trade Commission (FTC) plays an important role in the regulation of US information privacy. The FTC has moved beyond promises in the private sectors' online privacy policy to substantive privacy protections, evolving from an almost entirely self-regulatory regime to one that resembles more of an actual regulatory regime. Every step of its law enforcement actions has led to detailed analysis and interpretation of experts, scholars, and practitioners in the field of information privacy protection. In the decades of practice, the scope and means of law enforcement of the FTC have been continuously expanded, and a complete set of information privacy regulatory approaches has been formed.

At present, China's personal data protection legislation is in progress. It is foreseeable that in the near future, China's *Personal Information Protection Law* (Bill for Second Deliberation) will be introduced, but the design of the regulatory approach is still worthy of our in-depth study. It is worth noting that the EU and the US had different logics in the field of personal data regulation in the beginning. Judging from the various legal instruments used by both the EU and the US, we can

① The concept of "information privacy protection" is equivalent to "personal data protection," which is more frequently used in the US. This article uses the two conceptions to refer to the same object.

conclude that the regulatory approaches of the EU and the US are showing more common grounds, which reflects inherent common principles in personal data regulation. Only by grasping these common grounds, can we provide a corresponding reference for China's legislations in the related field.

The first part of this article will focus on the different governance paths and regulatory tools adopted by the EU and the US in the process of information privacy protection and analyze their specific utility. The second part of this article will point out that the essential ideas of regulation of personal data in the EU and US are showing more commonality. The third part will conclude the current views concerning the isomorphism of the regulatory approach in the field of data protection law and illuminate a possible direction for China's data protection law.

The Regulatory Approaches: The EU vs. the US

EU Model

The implementation of the GDPR is a milestone in the development of a personal data protection regime. Since then, many experts and scholars have reached a consensus on the data protection of the GDPR, which is described as empowering the individual data rights in order to strengthen personal control of their own data, and emphasized its enforcement mechanisms that are categorized as ex-post remedy mechanisms, such as high administrative penalties, as well as comprehensive complaints and litigation procedures. This type of protection mode in the GDPR has been all the rage for data protection legislation in more and more countries (Greenleaf, 2011; Albrecht & Jotzo, 2017). However, literature has gradually pointed out that merely emphasizing the above regulation mechanism cannot fully cover the regulatory ideas inside the GDPR. It should be indicated that the regulatory methods in the general data protection regulations are more extensive and comprehensive. The GDPR has built a set of compliance systems based on the principle of accountability introduced in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Alhadeff, Alsenoy, & Dumortier, 2012, pp. 49-82).① The compliance systems are based on the interaction between data protection regulators and regulated private sectors, namely data controllers and data processors, which is different from the top-down regulation of traditional law enforcement regulatory approaches. Scholars describe it as collaborative governance in the general data protection regulations.② The implementation of the rules and principles of personal data protection through the collaborative governance is another aspect that cannot be ignored in the EU's regulation.

① Organisation for Economic Co-operation and Development (OECD), "Recommendation of the Council concerning *Guidelines governing the protection of privacy and trans-border flows of personal data*." For accountability principle, see Joseph Alhadeff, Brendan van Alsenoy, and J. Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions."

② See *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 26, COM (2003) 265 final (May 15, 2003) ("[The Commission] believes that self-regulation, and in particular codes of conduct should play an important role in the future development of data protection in the EU and outside, not least in order to avoid excessively detailed legislation.").

From top-down regulation to collaborative governance.

The construction of personal data rights, data protection principles, and data responsibilities in the GDPR has both breadth and depth. The interpretation and application of these different rights, principles, and responsibilities, in the GDPR are based on a regulation approach composed of two aspects; a comprehensive private remedy system and an EU-wide unified law enforcement and supervision system, which are the strictest aspects of the GDPR.

First, with regard to the private remedy system, the GDPR not only entitles individuals the right to file a complaint towards regulation authority and to litigate according to Article 77 and 79 of the *Council Regulation (EU) 2016* but also paves the way for mandating a non-for-profit organization to lodge a class action on behalf of individuals according to Article 80. In the level of case-law, the GDPR is backed by an increasingly involved court, the European Court of Justice (ECJ), which has in recent years repeatedly ruled in favor of data protection rights (Google Spain SL v. Agencia Española de Protección de Datos, 2014; Google Spain SL v. Agencia Española de Protección de Datos, 2014; Zakharov v. Russia, App. No. 47143/06, 2015).

Second, in regard to regulatory authority, the GDPR consolidates and further empowers an extensive national and transnational system of government regulators. The GDPR requires that each member state of the EU should establish an independent supervisory authority, and shall establish an EU data protection board at the EU level to protect personal data rights. Extensive investigation and correction powers have been given to the above authorities. In addition to this, to coordinate the enforcement actions of the regulatory bodies within the various member states of the EU, a complete set of cooperation and consistency mechanisms between the numerous authorities was constructed according to Article 51 to 76 of the *Council Regulation*. The GDPR has some profoundly serious teeth. However, if the focus is limited to the above-mentioned systems it will miss the forest for the trees. The top-down regulatory system is only one aspect of the GDPR. Enterprises that are under heavy regulation pressure[①] will turn to the other aspect of the GDPR regulatory system, namely a series of compliance measures built within data controllers and processors, and to participating in collaborative efforts to flesh out broader rules and to voluntarily comply with the outcomes of those efforts to avoid government sanctions (Kaminski, 2019, p. 1597).

Third, the regulations emphasize the responsibility system of the data controller and processors. For the implementation of these responsibilities, the regulations no longer simply rely on individuals or regulatory authorities to supervise private sectors, but instead turn to the ongoing and interactive dialogue between regulators and private sectors (Kaminski, 2019, p. 1596),[②] and consequently form a set of compliance systems within these sectors through softer collaborative governance (Internal compliance systems).

① For data controllers and processors, if they fail to meet the standard of GDPR requirements, they might be facing the administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

② See *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 26.

In response to the specific needs of micro, small and medium-sized enterprises, the GDPR provides two methods: codes of conduct and certification systems to guide compliance. First, according to the provisions of the code of conduct, namely the code of conduct that contributes to the proper application of the GDPR, the industry can formulate a series of specific rules, taking into account of characteristics of processing data in different sectors.① The stipulated codes of conduct are so extensive that they cover almost every aspect of personal data protection, for example, the collection of personal data; the pseudonymization of personal data; the protection of children; and the exercise of the rights of data subjects.② The function of the code of conduct is similar to that of the safe harbor principle. Once the code of conduct in an industry is with the approval of the regulatory authority, the relevant enterprises can process personal data in accordance with it and therefore obtain an exemption in corresponding fields. Some codes of conduct may eventually become relevant EU-wide data protection laws.③

Second, certification is another softer co-regulatory mechanism, under which, the EU has adopted a strategy of using market certification to encourage the participation of private sectors in data protection. According to Article 42(1), the member states, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this *Regulation* concerning processing operations by controllers and processors.④ The underlying logic of this legal institution is that the certification standards are formulated internally by the industry, and then consumers would seek out those companies that are certified, like purchasers who search for goods or companies certified by the Better Business Bureau or Certified Humane (Edwards & Veale, 2018). Although certification does not function as the establishment of the code of conduct, which grants exemption towards these enterprises,⑤ it can serve to reduce enterprises' own compliance risk to a certain extent, because these regulatory authorities are involved in the creation of certification criteria.⑥

In addition, in order to mitigate the risk of personal data processing, the GDPR also stipulates some general measures, which essentially form a complete set of compliance systems within the enterprises and also reflect the nature of collaborative governance. The GDPR establishes a data protection impact assessment system that requires that when certain types of processing pose a high risk to the rights and freedoms of natural persons, the controller should carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.⑦ For the determination of "high risk," the GDPR outlines three situations, under which the data protection

① Article 40(1) of the *Council Regulation 2016/679*.
② Article 40(2) of the *Council Regulation 2016/679*.
③ Article 40(9) of the *Council Regulation 2016/679*.
④ Article 42(1) of the *Council Regulation 2016/679*.
⑤ According to Article 42(4) of the *Council Regulation 2016/679*, at 59 ("A certification pursuant to [Article 42] does not reduce the responsibility of the controller or the processor for compliance with this regulation and is without prejudice to the tasks and powers of the supervisory authorities . . . ").
⑥ Article 42(5) of the *Council Regulation 2016/679*.
⑦ Article 35(1) of the *Council Regulation 2016/679*.

impact assessments are necessary,[①] but at the same time, it also stipulates that regulatory authority has the right to publicize data protection impact assessment operations that comply with the regulations as the operating model and delineate the scope, within which data processing activities do not require data protection impact assessment. These provisions illustrate the central role of regulatory authority and its interactions with the private sectors in data protection impact assessments.[②]

To undertake the data protection impact assessment system, the GDPR has also developed a system of prior consultation and prior authorization. Aiming at the data processing activities with highrisk identified by the data protection impact assessments in Article 35, the controller should consult the regulatory authority prior to processing.[③] In addition, the laws of the EU member states may also require data controllers to consult the regulatory authority and obtain permission from it when data processing is in relation to the public interest.[④]

Under certain circumstances, the GDPR requires that the controller and the processor should designate a data protection officer.[⑤] The data protection officer is in a possession of a wide range of duties, and owns the power to intervene in every aspect of personal data protection,[⑥] in particular, to inform and advise the controller or the processor; monitor compliance with the GDPR and cooperate with regulatory authorities.[⑦]

The notification of a personal data breach is also introduced by the GDPR.[⑧] It consists of three main parts: The notification of a personal data breach to the supervisory authority;[⑨] the notification from data processor towards the controller;[⑩] communication of a personal data breach to the data subject when it is likely to result in a high risk to the rights and freedoms of natural persons.[⑪]

Sum up.

From the preliminary exploration of the regulatory approach in the general data protection regulations, it is not difficult to find that the construction of the private remedy system of individual data rights and the top-down regulatory system in the regulations forms part of its enforcement, but on a factual basis, the regulatory approach provided by the regulations is more complicated. Through collaborative governance, it introduces different legal instructions to build a set of compliance systems within the data controller to implement its own rules more softly. This system concentrates on the interaction between regulators and private sectors, and encourages private sectors to participate in the formulation of rules. However, this system also relies heavily on the supervisory role of regulatory authority. Drawn from the above analysis, it can be found that no matter what legal tool is in place, the

① Article 35, 53 and 54 of the *Council Regulation 2016/679.*
② Article 35(4), 53 and 35(5) of the *Council Regulation 2016/679.*
③ Article 36(1) and 54 of the *Council Regulation 2016/679.*
④ Article 36(5) of the *Council Regulation 2016/679.*
⑤ Article 37(1) of the *Council Regulation 2016/679.*
⑥ Article 38(1) of the *Council Regulation 2016/679.*
⑦ Article 39 of the *Council Regulation 2016/679.*
⑧ Article 33 and 34 of the *Council Regulation 2016/679.*
⑨ Article 33(1) of the *Council Regulation 2016/679.*
⑩ Article 33(2) of the *Council Regulation 2016/679.*
⑪ Article 34(2) of the *Council Regulation 2016/679.*

data supervisor is in the foremost position. Oriented toward the nature of risks posed by processing activities, the private sectors need to meet different compliance requirements of the regulator. It is clear that the collaborative governance mechanism in the general data protection regulations is not completely self-regulated by the enterprises, but relies more on the control of data controllers and processors by the regulatory authority.

American Model

This part mainly focuses on the regulatory approach adopted by the US in the protection of user information privacy. Numerous academic articles have pointed out that the US has adopted a legislation model completely different from that of the EU in the field of data protection. It did not establish an omnibus legislation system as that of the EU. From the perspective of the heaviness of regulation, scholars and advocates charge that the US law fails to protect privacy adequately. The dominant critique denounces the existing patchwork of privacy statutes as weak, incomplete, and fractured. It decries the absence of an agency dedicated to data protection and the consequent lack of clear guidance, oversight, and enforcement. And it argues that the US privacy framework fails to provide across-the-board procedures that empower individuals to control the use and dissemination of their personal information (Bamberger & Mulligan, 2011). The most recent scandal involving the British company Cambridge Analytica seems to have proven the incapacity of American regulations on a factual basis. Nevertheless, simple judgment would not be helpful to the insight into the regulation mechanism of the US. To evaluate its approach, the in-depth analysis concerning the approach itself is still indispensable.

From the perspective of the regulation strategy, unlike the EU, the US has turned to its booming Internet industry. At the beginning of regulation, self-regulation based on market and user needs was preferable in comparison with hard regulation. By contrast, the emergence of the federal trade commission (FTC) as a de facto privacy regulator has redirected the regulatory approach, in which the FTC is functioning as the supervisor of self-regulatory norms. It is worthwhile to pay attention to that the FTC is more than a mere supervisor. As a rule-generator, it has reconstructed privacy norms in consumer terms, and encouraged various actors to participate in the diffusion and institutionalization of those norms. The settlements (Solove & Hartzog, 2013, pp. 620-625) and sorts of reports, materials, based on different contexts in law enforcement practices, issued by the FTC have evolved into a set of substantive protection rules. Daniel Solove described this as the "new common law" system.

Regulatory developments by the Federal Trade Commission.

Due to the fact that there is no such omnibus law as the GDPR at the US federal level, the legislation of information privacy is fragmentedly distributed, existing in different industry sectors and states. A sectoral approach according to the different needs is one important characteristic in the American legislation (Hartzog & Solove, 2015, p. 2267). For instance, in the public health area, *the Health Insurance Portability and Accountability Act (HIPAA)* would function as a goalkeeper, and *Fair Credit Reporting Act (FCRA)* would exert its influence to regulate the collection and processing

concerned with financial data. However, it is worth noting that this kind of sectoral patchwork has left a large legislation gap. With the continuous development of the digital economy, the collection and use of user data are becoming the norm, while the vast majority of areas are not covered by legal protection.

At the other end of personal data, users have begun to show some concerns about the large-scale collection and analysis of personal data. Consumer confidence and trust have become a central theme in arguments both for and against new privacy regulations in the US (Bamberger & Mulligan, 2011, p. 282). Legislators and regulators were relatively quick to join a conversation about addressing privacy risks to advance electronic commerce.

To resolve users' concerns about the possible abuse of personal data, the Internet industry has also begun to self-regulate. Industry favored a self-regulatory regime, which consisted largely of what has become known as "notice and choice." For the "notice" part, companies began to include privacy policies on their websites, especially commercial sites (Scott, 2008, pp. 130-131).① The privacy policy was typically a special page that users could read by clicking a link at the bottom of a website's homepage (Haynes, 2007, p. 587, p. 594).② These policies described the various ways in which websites collected, used, and shared a visitor's personal information, as well as the various ways that information was protected. For the "choice" part, users were given some choices about how their data would be collected and used, most commonly in the form of an opt-out right, whereby companies could use data in the ways they described in the privacy policies unless users affirmatively indicated they did not consent to these uses.

Nevertheless, this plausible protection regime implies a huge crisis. Privacy policies as tools of self-regulation, although aiming to construct the users' trust in the companies, turn out to be a beautiful long-cherished wish. In practice, because of the ambiguity of its text, the complexities and challenges involved in human decision-making, and the lack of corresponding enforcement mechanisms, privacy policies played only a marginally important role (Solove, 2013; Koops, 2014).

At the fact level, although the US does not have a unified law enforcement authority, the US Federal Trade Commission has become a leader in this area with its unique advantages. Be it within the industry, consumers, or practitioners of information privacy, it is highly acknowledged that the FTC is the de facto enforcement authority in the US (Solove & Hartzog, 2013, p. 627). Widely divergent from the EU's approach, the FTC has adopted a regulatory approach that matches its highly developed Internet industry. How to maintain a balance between industrial development and user privacy remains the trickiest problem facing regulators. Following the above, with the help of extensive privacy policy protection practices in the industry, the Federal Trade Commission did not shape a new set of rules, but turned to monitoring and implementing these privacy policies (Hartzog

① The main element of self-regulation included the FTC enforcement of those privacy policies that companies collecting personal information posted on their websites.

② Typical privacy policies are accessed via hyperlinks at the bottom of the screen on a website's homepage.

& Solove, 2015). The underlying logic of this regulatory system is that once an enterprise fails to implement or violates the requirements of the privacy policy during the collection, processing, and transfer of personal data, it will fall into investigation and enforcement from the FTC. The primary source of authority for the FTC privacy enforcement was Section 5 of the Wheeler-Lea Amendment to the *Federal Trade Commission Act*, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[①] An "unfair or deceptive" act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment" or a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." [②] Thus, in its enforcement under Section 5, the FTC had two bases for finding privacy violations—"deceptive" trade practices and "unfair" trade practices.

However, the role of the FTC is by no means limited to being a supervisor of these privacy policies. What is more important is that the FTC has systematized its regulatory approach through consistent settlement order according to different law enforcement scenarios. These FTC settlements with enterprises form guidelines with significance for the practice of information privacy protection in the US. Viewing the operation of the FTC's enforcement actions, the FTC "may initiate an enforcement action if it has 'reason to believe' that the law is being or has been violated." If after conducting an investigation the FTC staff determines corrective action is needed, the staff issues a proposed complaint and order setting out the nature of the illegal act and the remedy.[③] After the FTC issues a complaint, the respondent can choose to either settle the FTC's charges or dispute the charges in front of an administrative or federal district court judge. The FTC negotiates and settles the majority of actions it initiates through prescribed consent order procedures.[④] the FTC's Subchapter A—"Organization, Procedures and Rules of Practice" allows anyone being investigated to submit a proposed consent order agreement where "time, the nature of the proceeding, and the public interest permit."[⑤] Generally, however, the FTC initiates the consent order procedure. According to the FTC, if the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), to consent to entry of a final order, and waive all rights to judicial review. If the FTC accepts such a proposed consent agreement, it places the order on the record for thirty days of public comment (or for such other period as the FTC may specify) before determining whether to make the order final.[⑥] Gradually, the consent order has become the most effective tool of law enforcement actions of the FTC.

① According to Article 45 (a) (1) of the *Federal Trade Commission Act 15 U.S.C.*
② According to Article 45 (n) of the *Federal Trade Commission Act 15 U.S.C.*
③ 16 C.F.R. § 2.31–.32 (2013).
④ 16 C.F.R. § 2.31–.34.
⑤ 16 C.F.R. § 2.31.
⑥ 15 U.S.C. § 45 (a) (1). *Overview of FTC Authority.*

The strategy embedded in the settlement order is obvious. The FTC would adjust the content of a consent order in accordance with the enforcement needed in different data processing contexts, in order to protect information privacy. In fact, the FTC has also virtually unrestrained discretion to define the "access and scope of the consent order process." The common FTC consent order contains financial penalties, bans on certain activities, and requirements for corrective action. It also commonly contains reporting, audit, and compliance requirements for up to twenty years. However, first, it should be noted that the duration of many requirements in the agreements is varied, even within the order itself. For example, most of the requirements in the US v. Godwin (Skidekids) consent order lasted for five years, while the recordkeeping requirement lasted for eight years. If no termination date in a settlement order is given, the agreement may be perpetual, binding the entity's successors and assigns.

Second, the FTC has also developed a variety of specific corrective actions against information privacy violations in long-term practice. Daniel Solove has summed up nine corrective measures in the settlement: Prohibitions on wrongful activities; fines and other monetary penalties; consumer notification and remediation; deleting data or refraining from using it; making changes in privacy policies; establishing comprehensive programs; assessments by independent professionals; recordkeeping and compliance reports; notification of material changes affecting compliance (Solove & Hartzog, 2013, pp. 614-619).

It is not difficult to see from the above various corrective measures that FTC's privacy protection enforcement practice is by no means limited to the implementation of privacy policies, but has formulated different strategies according to different situations in practice which have highly scenario-based characteristics. As noted by Joel Winston, who served as associate director for DPIP from 2000 to 2011, consent decrees are often "designed" to "have a huge impact on other businesses in the same industry or that use similar practices" because the FTC "must be strategic in bringing its cases, since it does not have the resources to pursue more than a relatively small fraction of law violators." Thus, "the cases are designed to send a message to others similarly situated" (Solove & Hartzog, 2013, p. 624).

The latest settlement published by the FTC with Facebook is a example of the above regulatory system. In addition to the high fines of up to $5 billion, the FTC's 20-year settlement agreement also puts forward corresponding compliance requirements for Facebook in other aspects. The main requirements include: to designate compliance officers who will be responsible for Facebook's privacy program; to establish a new board privacy committee; to enhance the independent third-party assessor's ability to evaluate the effectiveness of Facebook's privacy program and identify any gaps; to conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy; to exercise greater oversight over third-party apps.

The FTC adopts a variety of measures to regulate privacy violations. The establishment of such a set of systematic measures allows the FTC to occupy a pivotal position in the protection

of information privacy in the US. It developed loads of legal tools to serve as backups for enforcing the privacy policies and to make the FTC's enforcement actions extend to more than simple deceptive and unfair commercial practices. What is important is the FTC's settlements, various reports and materials function as the guideline to enhance the protection of information privacy with regard to the external management. The FTC's actions seem to be the stirrings of a much more complete and substantive regime than simply requiring companies to follow their promises (Solove & Hartzog, 2013, p. 666), which in substance is in line with the EU's regulatory idea to set up the internal compliance system.

Sum up.

The underlying logic of regulation of the US and the EU diverged at the very beginning. The US way relies on the self-regulation of the industry, while the EU paves the way for strong regulation. Besides, the US did not introduce a comprehensive private remedy system of personal data rights and uniform enforcement authority, but rather select the FTC as the regulatory authority to fill the gap brought by self-regulation. The FTC has assumed the responsibility of supervising the companies' commitments and reshaped the information privacy regulation in the US through its enforcement actions. However, to a large extent, the two data giants are showing more convergences in their regulatory approaches. The next part of this article will focus on the analysis of these common regulation practices.

An Analysis of the Similarities between the EU and US Regulatory Approaches

In the field of personal data protection, there are significant differences in legislation between the EU and the US, due to the different understanding towards the right to protect personal data. The right to protect personal data is regarded as a fundamental right in Europe continental, which is stipulated in Article 8 of the *European Charter of Fundamental Rights*. For the substance of this fundamental right, it is suggested that individual control should be explicitly recognized as a facet of the right to data protection (Lynskey, 2015, p. 228). Besides, it is not hard to draw such a conclusion, from the rights-based regime in the GDPR and the narrative of the recital of GDPR, that strengthening the individuals' self-control is the core of personal data right.[①] By contrast, in the US, personal data right, namely information privacy is not understood as a fundamental right (Schwartz & Solove, 2013, p. 880), but rather as one interest that is balanced against others (Schwartz & Peifer, 2010, pp. 1953-1954). In practice, information privacy tends to be understood from the perspective of consumer expectation (Bamberger & Mulligan, 2011).

Nevertheless, the divergence concerning the personal data does not impede the fact that

① Recital 7 of the GDPR states that: "Natural persons should have control of their own personal data."

both of them have adopted similar regulatory approaches. They are confronting some common problems through the process of supervision and enforcement. In one aspect, the highly detailed and proceduralized behavioral mandates in the traditional regulatory and enforcement models cannot meet the challenges caused by rapid technological development and change, and it is easy to induce data privacy protection regimes that focus on meeting formalities to create paper regulatory compliance within industry sectors rather than effective data protection practices. In another aspect, the various interests embedded in personal data are intertwined. No matter in the EU's rights-based regime or the US consumer expectation regime, the scope of data protection principles, data rights and the responsibilities of data controller and the processor are still in a vague state, because to a large extent these are newly generated rights, principles, and responsibilities. Consequently, it is necessary to determine the reasonable relationship in specific application contexts between the data subject and the controller and the processor. After an in-depth analysis of the regulatory tools of the EU and the US, it is explicit that both have put into practice some common regulatory principles. Specifically, first, the focus of regulation has shifted into the construction and supervision of the internal data privacy protection system of private sectors. Second, in the process of regulation, the EU and the US did not adopt a top-down regulation model, instead, they both have chosen to apply a model of cooperation with the Internet industry. Through collaborative governance, they are continuously exploring the optimality of personal data protection practices in different contexts.

The Shift of Regulatory Focus

Be it in the EU or the US, private remedy systems are not the only option to regulate personal data processing activities. Among the regulation tools in the EU and the US, the regulatory authority has already shifted the regulatory focus from consumers' consent into the internal personal data protection system.

In the EU, many regulation tools in the GDPR, such as data protection impact assessment system, Prior Consultation, and Prior Authorization, notification of a personal data breach, and Data Protection Officers, require companies to establish a complete protection system for processing data. In the US, the application of various regulatory measures in the FTC consent order also reflects a similar idea. This point also supports the opinion of Daniel Solove, according to whom the focus should be more on downstream uses rather than on the time of the initial collection of data (Solove, 2013, p. 1902). The essence of personal data is in data transfer and reuse, and the protection of personal data should also proceed based on this point. Embedding the substantive principles of data protection in the stages of personal data collection, use and transfer rather than leaving it to market would effectively protect the personal information. without a substantive touchstone, data protection regimes can focus resources on developing a host of often meaningless consent processes (Cate, 2006).

As for relying on empowering individuals with the right to litigate and file a complaint is

incapable of covering the regulation needs. When facing a new technology gap, it is extremely difficult for individuals to measure the costs of certain forms of collection, use, and disclosure of personal data. Because of the dynamism of this area, assessing such costs and benefits requires a fair degree of speculation about the future. However, individuals are unlikely able to master the relevant knowledge. Problems such as unauthorized use of personal data, the discrimination in algorithmic functions are continuing to be unsolved at the level of personal data rights (Kaminski, 2019, pp. 1611, 1613).[①] In sum, for "privacy self-defense operates at the individual level...surveillance operates at the collective level," thus the "logics of surveillance require a considered, collective response" (Cohen, 2008).

The Collaborative Mechanism and Contextual Enforcement

The boundaries of data protection principles, data rights, and responsibilities have not been clarified yet. Although the GDPR adopted a rights-based regime, the connotations and denotations of a series of specific rights are waiting to be explored. In particular, the rights to access, to correct, to delete, and to be forgotten are outlined in a broad and ambiguous legislative language, and there is no specific stipulation of their application in a concrete context. The problem of ambiguity lies not only in the data rights, but also in the responsibilities of data controllers and processors. In the US, this circumstance remains the same. Due to the fact that there is no uniform data protection legislation, personal data protection rules are distributed among various sectoral laws, and the federal-level law enforcement authority, the US Federal Trade Commission, could only enforces on the broad basis of "deceptive or unfair practice."

Indeed, this ambiguity of legislation brings many more possibilities to the EU and the US regulation. From the perspective of the legal institution design, one trend is not relying on the traditional regulation system from top to bottom, but rather turning to collaborative governance to implement the principles and responsibilities of data protection. Another trend to cope with this legal ambiguity is the adoption of a new regulatory strategy—contextual enforcement. In this part, this article will be divided into two parts to introduce these two characteristics

The core of this kind of collaborative governance is that the supervising authority gives the industry a certain amount of regulation space, enabling them to discuss the boundaries of various data rights and data protection principles with the supervisor to form a personal data protection system from bottom to top.

In the GDPR, there are several means to encourage the industry to participate in collaborative governance. The code of conduct and certification mechanism are the most typical examples. In these different mechanisms, different industry departments are entitled to formulate data protection rules based on their own contexts of collecting and using data and the rules are then

① This is not to deny the value of the personal data rights system. The private remedy system of personal data rights is still indispensable.

approved by the regulator.[①] For the US, after the role of the US Federal Trade Commission as an enforcer of information privacy in the US continues to be clear, its supervision and enforcement mechanisms are no longer purely self-regulation within the industry, but are more inclined to the essence of collaborative governance. The privacy policy on user protection is drafted and formulated by the private sector itself, and the FTC supervises whether it has complied with the commitments in the privacy policy. Besides, the utilization of consent orders for enforcement also reflects the collaborative governance aspect of personal data protection in the US. Judging from its specific operation, the settlement reached between the FTC and the enterprises involved is based on mutual consensus between the two parties. A settlement is mutually agreed upon by both the FTC and the defendant, so it represents a workable compromise. Judicial decisions need not reach this compromise point. The benefit of reaching a compromise is that the doctrines emerging from such a compromise are likely to be workable for at least several key stakeholders, whereas there is no such guarantee with judicial decisions, which can be entirely unworkable or unsatisfactory to any stakeholder (Solove & Hartzog, 2013, p. 624).

There is also some consensus regarding the benefits brought about by collaborative governance compared to command-and-control regulation on the one hand and self-regulation on the other. By involving the private sector and other third parties, collaborative governance can purportedly (a) increase the amount of private sector expertise in governance, (b) contribute to the perceived legitimacy of governance, thus contributing to increased compliance, (c) harness nongovernmental mechanisms towards compliance and enforcement, thus increasing the state's enforcement capacity, and (d) solve the "pacing problems" caused when the technology at issue is evolving at a rate top-down regulation cannot keep up with by shifting from onetime, specific rules to an ongoing, iterative system of monitoring and compliance (Hirsch, 2011, p. 467; Kaminski, 2019, pp. 1559-1563). In a nutshell, it is more effective to adopt this new method.

For regulators, a contextual approach to regulation is also the common practice under such ambiguous rules for the EU and the US.

With regard to specific measures, in the EU regulation system, the European Data Protection Board (EDPB) as the EU level data protection institution continues to release interpretative documents based on different data processing scenarios, to guide data rights and responsibilities in the GDPR, such as *Guidelines on Consent under Regulation*, *Guidelines on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR* and *Guidelines on the Processing of Personal Data through Video Devices*. Especially, during the pandemic of Covid-19, the EDPB has issued *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak* and *Guidelines 03/2020 on the Processing of Data concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak*.[②] The idea of the

① For the analysis of the code of conduct and certification, see the first part.
② See https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

EDPB was to form such guidelines by simplified case law based on the enforcement actions of data protection authorities of the member states. For example, in guidelines on consent, the EDPB has delineated the elements of the valid consent by a list of concrete and detailed examples of collection activities taking into consideration of different methods that may be applied by data controllers.①

In the US, regulation practices of the FTC are highly context-oriented as well. From the evolution of substantive rules concerning information privacy, the FTC is continuing to expand the implication of "deceptive and unfair practice." With a focus on consumer privacy expectations, the FTC has embraced the empirical evidence about consumer assumptions and behavior in regard to what is a deceptive and unfair practice. Besides, with a willingness to look beyond privacy policies to the entire architecture and design of websites, software, and devices, the different privacy practice context is also taken into consideration by the FTC. There is no doubt that the FTC is poised to take even bolder steps toward developing a thick, meaningful, and broad approach to regulating privacy in the US (Solove & Hartzog, 2013, pp. 627-676).

The Second Wave of Privacy Law and Its Pitfalls

The regulatory approaches of the EU and US are in an ongoing process of change while sharing common principles. As noted by Waldman, "Privacy law is transitioning from a first wave focused on notice to a second wave focused on internal procedures" (Waldman, 2021). These new regulatory ideas envision a new underlying regulatory logic. As has been articulated, this logic abandoned the previous "lassie faire" policy and turn to the "co-regulation" ideal. Though the catalyzing force is to overcome the intrinsic defects of the original mode, these regulatory approaches also face their dilemma. Whether the regulatory approach can evolve according to its design requires more considerations.

This part serves to map the regulatory template of the EU and US onto the regulatory spectrum by introducing Waldman's descriptive theory and point out the pitfalls that it may fall into.

The Second Wave of Privacy Law

Waldman aptly observed that "in the last three years, nine proposals for comprehensive privacy legislation have been introduced in the US Congress and 42 have been introduced in the states." And these proposals are roughly the same. According to his taxonomy, this phenomenon is termed as the "second wave of privacy law." Unlike the self-regulatory approach of the "first wave of privacy law," which puts emphasis on the "notice-and-consent" requirement (Solove & Hartzog, 2013, pp. 600-606) and follows the underlying ideology of classical liberalism (Waldman, 2021), the "second wave of privacy law" is neoliberal, which incorporates liberal

① Guidelines 05/2020 on Consent under Regulation 2016/679.

beliefs into regulations by infusing marketing thinking, such as "efficiency," "maximization of profit," and "minimization of cost" (Peck & Tickell, 2007, p. 33). Formally, this approach relies heavily on the ongoing internal company compliance system. In this way, the regulatory goal is to avoid the pitfalls of the market while keeping the market function well. The second wave is also sophisticatedly described as representing a choice to filter privacy law through corporate compliance and to manage data collection and processing from within (Waldman, 2021).

It is decided that the "second wave of privacy law" is not only a US inclination but also a global trend. Waldman's observation is from the perspective of American privacy practices. However, admittedly, from the above analysis, it can be seen that the regulatory strategies applied by the EU and the US have shown more in common. With a shift of regulatory focus into internal protection system and a deliberate collaborative governance mechanism, the EU is also dedicated to the common narrative of neoliberal approach (Solove & Hartzog, 2013, pp. 617-618; Kaminski, 2019; Citron, 2016).①

The Pitfalls

As schemed by scholars, with corporative internal compliance and collaborative governance, vague standards of privacy law may finally evolve into specific rules. For the EU, these seemingly vague terms in the GDPR become clear when we combine the GDPR with interpretive tools, including reports from the European Data Protection Board. For the US, Daniel Solove and Woodrow Hartzog argue that lawyers and privacy professionals may be able to piece together what does and does not constitute "adequate" notice from the total of the FTC consent decrees.

This is normally how the institutional design functions. However, whether these approaches can be effective is contestable.

On the one hand, the effectiveness of the current approach may be constrained by a powerful regulatory authority. Margot Kaminski worries that "how the softer and harder aspects of the GDPR play out and interact in practice will do a great deal to determine whether its attempts at collaborative governance are effective." She further explains that "authorities will need to show enough strength to incentivize companies to meaningfully participate but enough gentleness to discourage adversarial posturing" (Kaminski, 2019, p. 1598).

On the other hand, it is also admitted that paper compliance ignoring the essence of data protection may still haunt user's privacy. According to Waldman's empirical research on on-the-ground practices of privacy law in the US, privacy practices under the current approach "open the door for companies to frame the law in ways that serve corporate, rather than consumer interests" (Waldman, 2020, p. 792). For one thing, ambiguous privacy law provides more possibilities for better regulation but also a leeway to build a shield for liability. In addition to

① Scholars have gradually noticed this shift of regulatory approach.

this, the current process-oriented compliance system may offer sufficient exemption because the company may defend itself against the privacy violation as it has provided due care.

For another, the current privacy ecosystem is dominated by compliance professionals. They, rather than legislators or regulators, incorporate practice and technology design with specific meaning. Before the concrete rules of privacy law come out, these company professionals predominantly have a say on the framing of law. Legal perception of judges and regulators would definitely be influenced. Finally, it causes legal deference to what professional compliance creates (Waldman, 2020, pp. 815-819). The whole process is what Edelman deftly observed in the workplace anti-discrimination law and termed as legal endogeneity (Edelman, 2016).

As it can be seen, the two sides, proponents and opponents, have shown great concern with the effectiveness of the new regulatory approach. Data protection is basically a structural problem (Solove, 2013, pp. 1888-1893), more precisely, a structural asymmetry of power. An effective approach will need to be able to adjust this extraordinary power imbalance. The current approach is nevertheless to be improved for its risks to become too harsh or, as empirical experience shows, too weak, either of which would tilt the intended balance.

Conclusion

Although the EU and the US have adopted similar approaches to regulating corporations in terms of data protection, these approaches are far from perfect. Either way, we must take potential pitfalls into consideration.

China has recently published the second draft of its most comprehensive data protection law.[①] It is clear that these regulatory elements include internal compliance and collaborative governance. In the meantime, it is hard to predict which direction China's regulatory approach will turn to, even though facial resemblances appear, because they may not share the same understanding. However, it needs to keep in mind that an effective regulatory approach requires constraint of regulatory power and being on guard against legal endogeneity.

① *Personal Information Protection Law (Bill for Second Deliberation).*

REFERENCES

A brief overview of the Federal Trade Commission's Investigative and Law Enforcement Authority. (2008). Retrieved from http:// www.ftc.gov/about-ftc/what-we-do/enforcement-authority

Albrecht, J.P., & Jotzo, F. (2017). Das neue Datenschutzrecht der EU: Grundlagen, Gesetzgebungsverfahren, Synopse, 126–129.

Alhadeff, J., Alsenoy, Brendan, A., & Dumortier, J. (2012). The accountability principle in data protection regulation: origin, development and future directions. *D. Guagnin, L. Hempel, C. Ilten a.o. (eds.)*, 49-82.

Bamberger, K. A., & Mulligan, D. K. (2011). Privacy on the books and on the ground, *Stanford Law Review*, 63.

Borgesius, F. Z. (2015). Informed consent: We can do better to defend privacy, *13 IEEE COMPUTER & RELIABILITY SOC'YS*, 103–107.

Charter of Fundamental Rights of the European Union, O.J C 364/10 (2000).

Citron, D. K. (2016). The privacy policy-making of State Attorneys General, *92 NOTRE DAME L. REV.* 747, 760.

Cohen, J. E. (2008). Privacy, Visibility, Transparency, and Exposure, *75 U. CHI. L. REv.* 181, 201.

Digital Rights Ir. Ltd v. Minister for Commc'ns, Marine and Nat. Res. (Apr. 8, 2014). Retrieved from http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

Edelman, L.B. (2016). Working Law: Courts, corporations, and symbolic civil rights.

Edwards, L., & Veale, M. (2018). Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"?, *16 IEEE SECURITY & PRIVACY*, 46, 52.

Federal Trade Commission Act, 15 U.S.C. § 45(1914).

FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook". Retrieved from https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook". Retrieved from https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

FTC policy statement on unfairness. (1980). Retrieved from http://www.ftc.gov/bcp/policystmt/ad-unfair.htm

FTC's new 20-year settlement order. Retrieved from https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf

Google Spain SL v. Agencia Española de Protección de Datos (May 13,2014). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

Greenleaf, G. (2011) The influence of European data privacy standards outside Europe: Implications for the globalization of Convention 108, *2 Int'l Data Privacy Law 2*, 13. DOI: 10.1093/idpl/ips006

Greenleaf, G. (2018, June). Global convergence of data privacy standards and laws: Speaking notes for the European Commission Events on the launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018. *UNSW L. RES. PAPER*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184548.

Hartzog, W., & Solove, D. J. (2015). The scope and potential of FTC data protection, *83 George Washington Law Review*.

Haynes, A. W. (2007). Online privacy policies: Contracting away control over personal information?, *111 Penn St. L. Rev.* 587, 594.

Hirsch, D. D. (2011). The Law and Policy of Online Privacy: Regulation Self-Regulation, or Co-Regulation?. *34 SEATTLE U. L. REV.* 439, 465–467.

Julie E. Cohen, Privacy, Visibility, Transparency, and Exposure, 75 U. CHI. L. REv. 181, 201 (2008)., F. H. (2006). The failure of fair information practice principles, in Consumer Protection in The Age of the 'Information Economy' 341. *J. K. Winn (eds.)*.

Kaminski, M.E. (2019). Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. *Southern California Law Review, 92*(6), 1529-1616.

Koops. B. J. (2014). The trouble with European Data Protection Law. *4 International Data Privacy Law 250*.

Law of the People's Republic of China on the Protection of Personal Information (Draft II)

Lynskey, O. (2015). The foundations of EU Data Protection Law, *Oregon*, 228.

Neil Robinson et Al., Rand Eur., Review of The European Data Protection Directive 39 (2009).

Peck, J., & Tickell, A. (2007). Conceptualizing neoliberalism, thinking thatcherism. Contesting Neoliberalism: Urban Frontiers. *H. Leitner, et al. (eds.)*, 26, 33.

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016) General Data Protection Regulation (GDPR).

Schwartz, P. M., & Peifer, K. N. (2010). Prosser's privacy and the German Right of Personality, 98 CALIF. L. REV. 1925, 1953–1954.

Schwartz, P. M., & Solove, D. J. (2013). Reconciling personal information in the United States and European Union, *86 SSRN ELECTRONIC JOURNAL* 1814, 880.

Scott, M. D. (2008). The FTC, the unfairness doctrine, and data security breach litigation: Has the commission gone too far?, *60 Admin. L. Rev. 127*, 130–131.

Solove, D. J. (2013). Privacy self-management and the consent dilemma, *126 HARVARD LAW REVIEW*, 1880, 1902.

Solove, D. J., & Hartzog, W. (2013). The FTC and the new Common Law of Privacy, *SSRN Electronic Journal*, 600-676.

Stephanie W. Kanwit, Federal Trade Commission §12:1 (2013).

Taylor, R. (2017). No Privacy Without Transparency. In R. Leenes, R. V. Brakel, S. Gutwirth, & P. D. Hert (Eds), *Data protection and privacy 63*, 74–76.

The United States v. Godwin (Skidekids), No. 1:11-cv-03846-JOF, at 14-15 (N.D. Ga. Feb. 1, 2012).

Waldman, A. E. (2020). Privacy Law's False Promise, *97 Wash. U. L. Rev*, 792-819.

Waldman, A. E. (2021). The New Privacy Law, *UC Davis Law Review*, 55. Retrieved from https://ssrn.com/abstract=3856598

Zakharov v. Russia, App. No. 47143/06 (Dec. 4, 2015). Retrieved from http:// hudoc.echr.coe.int/eng?i=001-159324.

(Editor: Zeng Yueying)