THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF RISK MANAGEMENT

ANALYZING THE EXTANT DIFFERENCES BETWEEN THE DATA-TRANSACTION AND PRIVACY REGULATIONS OF CHINA AND THE UNITED STATES

JIANGYINGLUN (ALAN) YUE
SPRING 2022

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Finance and International Politics
with honors in Legal Environment of Business

Reviewed and approved* by the following:

Daniel R. Cahoy
Professor of Business Law
Thesis Supervisor

Fiona Greaves
Clinical Assistant Professor of Business Law
Honors Advisor

* Signatures are on file in the Schreyer Honors College.

Abstract

This thesis provides an in-depth review of the concept of data regulation and privacy. These have become matters of pressing concern in the context of rapid, global technological change. The thesis commences by giving an overview of the data-protection policies applicable in the United States and those currently used in China. As Chapter 2 of this thesis demonstrates that data-protection policies are, at present, more effective in the US than in China. The US considers the implementation of data-transaction regulations as a key measure in promoting the economy of data. The Chinese state should learn (i.e., copy and adapt) certain techniques that are integral to the promotion of data privacy and the enhancement of the privacy of personal data. In Chapter 3, the thesis continues by providing examples of critical concepts adopted in US data regulation. These practices are recommended for adoption in China in Chapter 4 of the thesis. The paper concludes by indicating that, if these measures are incorporated within China, it is likely that China's data policy will match the efficacy of the United States of America. Indeed, Chinese rules, regulations and policies for data protection may become benchmarks in their own right.

Table of Contents

ACKNOWLEDGEMENTS

First, I would like to thank everyone who helped me throughout my thesis writing.

In particular, I would like to express my appreciation to Professor Daniel Cahoy for his support and assistance throughout my research and editing. His encouragement and dedication have been my biggest motivation to keep on track with my thesis, from selecting the topic and locating resources to finishing the final draft. Without his guidance, this thesis would not be possible.

I would also like to thank Professor Fiona Greaves for her time, and Professor Gregory Pierce with his inspiration. In addition, I would like to thank my mom for all the Chinese legal resources provided me to fulfill my thesis with contexts.

Finally, I would like to express my love and appreciation to The Pennsylvania State University and Schreyer Honors College for all the academic pursuits and opportunities it provided me.

Introduction

Rapid technological advances, on a global scale, have made privacy and data regulation matters of urgent concern. Ongoing technical advancement, indeed, has generated enormous progress regarding the precision and scale of the consumer data collected by firms. Notably, developments in machine learning, as well as other technologies of data processing linked to information technology, now offer companies the opportunity to transform retrievable data into successful outcomes in the form of business services.[1]

Indeed, such transformative change will, in various ways, contribute to the generation of vast economic returns in the years ahead. In business, however, most positive phenomena come with limitations, and in this case, the negative aspect is that consumers associated with these technological processes lack proper control over them; they also face issues related to an, "increasing number of high-profile data breaches and a growing feeling of despondency."[2] This pertains to the wider framework of data governance, which concerns not merely the facilitating of data sharing, but also the protection and preservation of data privacy. Data governance also takes into consideration the mechanisms of data transactions, as well as general questions of regulatory compliance, data privacy, data security, and legal norms - among other factors.

Contextually, a holistic approach must be implemented in the process of data protection, as well as in system design,[3] and any effective approach should consider the integration of legal,

---

[1] LEO BESEMER, TITLE PRIVACY AND DATA PROTECTION BASED ON THE GDPR (2020).
[2] Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Economic Consequences Of Data Privacy Regulation: Empirical Evidence From GDPR.* NBER WORKING PAPER SERIES. Retrieved from https://www.nber.org/system/files/working_papers/w26900/revisions/w26900.rev0.pdf?sy=900 (2020).
[3] World Bank Group. *Data protection and privacy laws.* Retrieved from https://id4d.worldbank.org/guide/data-protection-and-privacy-laws (2021).

technical, and administrative protections.[4] This thesis, therefore, aims to help the reader understand the different techniques used for regulating data transactions, and maintaining consumer privacy, in the US and China. More specifically, the thesis seeks to document such practices so that the most effective may be identified, allowing successful initiatives to be employed as regulatory benchmarks for other regions in future.

Data protection takes into consideration the regulation of trade in goods and services within the digital economy. This thesis also considers the negative effects, market related and otherwise, of insufficient data rights and data protection. In this context, it has been found that both a decline in confidence levels among consumers, and *excessively* rigorous protection that imposes undue restrictions on businesses, will generate adverse economic impacts. A form of "golden mean" is thus required.

Alongside a description of the data-transaction and privacy regulations deployed by the United States and China, this thesis also compares the regulatory techniques used by both nations, while further considering the techniques used by the United States as a potential example for the Chinese market. Based on the US template, indeed, the thesis offers practical suggestions for China.

Thesis Statement. As of 2022, China has produced a data-protection framework, but this is not comprehensive enough. The Chinese state should take lessons from the United States, which has a relatively better framework for data protection and safeguards for personal privacy, as indicated in the examples from current practice that will be explored below.

---

[4] DANIEL LE MÉTAYER, GEORGE DANEZIS, MARIT HANSEN, JAAP-HENK HOEPMAN, RODICA TIRTEA, STEFAN SCHIFFNER & JOSEP DOMINGO-FERRER. PRIVACY AND DATA PROTECTION BY DESIGN - FROM POLICY TO ENGINEERING (2014).

I. Chapter 1: Data-Transaction Regulations and Privacy

In the United States, the advent of the digital economy exposed the vulnerability of electronic data, and this generated demands for more effective protection at national level.[5] This was driven by privacy violations and high-profile data breaches that repeatedly came to light in the last two decades. On the one hand, issues related to data protection were seen as rooted in the government's methods of data utilization, and this increased tensions over control mechanisms around the private sector and digital information.[6] On the other hand, "inadequate corporate privacy practices and intentional intrusions into private computer networks have exposed the personal information of millions of Americans."[7] Data security, in other words, was a matter that involved both government and the private sector.

Risks were significantly increased by improved Internet connectivity over the years, along with the expanded use of electronic gadgets, especially mobile phones and personal computers. The problem was further exacerbated, moreover, by the inclusion of digital connectivity in a range of everyday objects, from cars to home appliances, "smart" speakers, and a host of objects linked to the Internet.[8]

Privacy International has defined "data protection" in legal terms: for that organization, the term references *laws* to protect individual privacy.[9] In terms of contemporary society, it is

---

[5] MICHAEL E. MILAKOVICH, DIGITAL GOVERNANCE: APPLYING ADVANCED TECHNOLOGIES TO IMPROVE PUBLIC SERVICE (2021).
[6] Macmillan Keck, Seharish Gillani, Ahmed Dermish, And Jeremiah Grossman, *The Role Of Data Protection In The Digital Economy.* UNCDF. Retrieved from https://policyaccelerator.uncdf.org/policy-tools/brief-data-protection-digital-economy (2021).
[7] *Supra* note 5, at 1.
[8] *Id.*
[9] Privacy International, *The Keys To Data Protection. A Guide For Policy Engagement On Data Protection*, p.4-98 (2021).

possible not only to control data, but also to protect individuals from abuses. One must ensure, at the same time, that laws for data protection restrain and shape the conduct of private companies as well as state organs. Notably, it has been found that, "institutions have shown repeatedly that unless rules restricting their actions are in place, they will endeavor to collect it all, mine it all, keep it all, share it with others while telling us nothing at all."[10] It is therefore obvious that data protection is, or should be, a key aspect of data transactions. Both data protection *and* data transactions may harness the immense potential of information technology. The ever-increasing sophistication of IT, nonetheless, allows the harvesting and storage of vast quantities of personal information in the databases of both governments and commercial enterprises.

Article 4 of the GDPR defines "personal data" as any information pertaining to "an identified or identifiable natural person."[11] A natural person can be seen as a data subject, whose presence in a database may be accompanied by names, location data, and identification numbers. Article 4 further addresses the recognition of living individuals as the subjects of their respective personal data, also due diligence in the sense that measures of data protection need to be effectively imposed.[12] For example, the procedures and policies of entities must clearly conform to data-protection laws.[13] Due diligence regarding data transactions also implicates various techniques for decreasing risks of many kinds, such as risks concerning data from employees, suppliers, and customers, and the retrieval of sensitive information. Examples might include

---

[10] Cameron F. Kerry, *Why protecting privacy is a losing game today and how to change the game.* BROOKINGS INSTITUTE. Retrieved from https://www.brookings.edu/research/why-protecting-pravacy-is-a-loosing-game-today-and-how-to-change-the-game. (2018).

[11] Rachelle Sellek, *Data Protection Considerations In Corporate Transactions And The Due Diligence Process.* Retrieved from https://acuitylaw.com/data-protection-considerations-in-corporate-transactions-and-the-due-diligence-process/ (2019).

[12] Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation Of Personal Data Retention And Erasure*, 90 U. COLO. L. REV. 593, 612 (2019).

[13] *Supra* note 11.

addresses, names, and sample signatures.[14] Techniques used by some companies include, "using samples of contracts rather than copies of signed contracts, and providing template employment contracts for non-key employees where the terms of employment are identical." Other techniques, meanwhile, include the aggregation of the identifiable salary data of individuals, and the compilation of summary-related information concerning commercial, personal and disputes-related data.[15] Regulations regarding personal-data transactions must address these phenomena, as well as any associated legal norms and policies, and they must incorporate realistic measures for prevention, protection, and compliance.

Furthermore, legal paradigms are highly significant in maintaining personal data privacy and security governance, irrespective of competing interests around the protection of data.[16] The technicalities and complexities of those legal paradigms are also reflected in a lack of regulatory uniformity at federal level. For example, in the US, individual's privacy rights are not safeguarded by the Constitution but rather the statues and state laws. However, the privacy should be restraining government intervention and overreach, also preventing private actors from abusing personal data on online platforms.[17] Statutes associated with data protection does not exist at the federal statutory level, comprising regulation not only regarding various data subcategories but also the operations of industries.

Contextually, it should be noted that, "the Federal Trade Commission (FTC) fills in some of the statutory gaps by enforcing the federal prohibition against unfair and deceptive data

---

[14] Elizabeth H. Johnson, *Data Protection Law in the European Union*, FED. LAW., 44, 44–45 (2009).
[15] *Supra* note 11.
[16] *Supra* note 5, at 2.
[17] *Supra* note 12, at 593, 598.

protection practices."[18] Various commentators have highlighted the need to include provisions for data protection within corporate transactions.[19] Indeed, it is important to ascertain the precise point or stage of illicit data processing, as perceived by a buyer, and to provide an assurance that data is processed merely to ensure the effective management of transactions, as and when required.[20] The importance of the assurance of the safe data is not only guarding the fundamental rights and freedoms of natural persons, but also protection for the society in general.[21] The issue is complicated, however, by a multiplicity of national and international jurisdictions.[22] International jurisdictions have variously re-examined data-protection approaches to accommodate a significant increase in the capacity, as well as the speed, of computing - an increase that also facilitates innovation in services and/or products.[23] Regulators must further address the economic value of personal data when determining whether current practices can safeguard privacy, in light of the communications technologies and information of the 21st century; they must balance the interests of the consumer with the overall development of commerce.[24]

---

[18] *Supra* note 5, at 2.
[19] IAN G. DIBERNARDO, JASON M. SOBEL. BEST PRACTICES FOR DATA PROTECTION AND PRIVACY LEADING LAWYERS ON CREATING A DATA PROTECTION STRATEGY, DEALING WITH SECURITY BREACHES, AND ANALYZING RECENT TRENDS IN LEGISLATION (2009).
[20] *Id.*
[21] Julie E Cohan. *Examined Lives: Informational Privacy And The Subject As Object.* 52 STNLR 1373, p.10 (2000).
[22] OECD. THE OECD PRIVACY FRAMEWORK, p.1-154 (2013).
[23] *Ibid, p.69.*
[24] *Supra* note 22.

II. Chapter 2: Extant Techniques for Data-Transaction Regulation

2.1. Techniques Used in the United States

Data privacy is central to the maintenance of security, the organizational protection of personal data, and the legal and ethical processing of the latter.[25] In the business environment of the US, "managing" data too often means attacking customers with unwanted marketing messages, while failing to obtain customers' consent in the sharing of their personal information with third parties.[26] Data-privacy laws, conversely, can empower individuals and offer them much greater control over their own personal data. Most relevant legal models involve the introduction of data-subject rights for safeguarding the personal data of individuals.[27] As long ago as 1973, a report was published by the US Department of Health, Education, and Welfare (HEW), entitled *Computers and the Rights of Citizens*. [28] This proposed a complex range of legal instruments to safeguard citizens from the adverse effects of automated personal-data processing.[29] The report also referred to techniques of data protection and transaction in the US, citing case law, statutory laws and constitutional rights, among other factors. It highlighted the application of the first directly relevant US legislation, i.e., the Fair Credit Reporting Act (1970), which contributed, in particular, to dealing with the negative impact of personal data being used, or abused, within computerized databases.[30] In fact, US legislation and legal norms address a

---

[25] Matthew White, Phil Mennie & Richard Chudzynski, *Data Privacy Handbook. A Starter Guide To Data Privacy Compliance*, p.3-30 (2019).
[26] *Id.*
[27] Matt Burgess, *Ignore China's New Data Privacy Law at Your Peril.* Retrieved from *https://www.wired.co.uk/article/china-personal-data-law#intcid=_wired-uk-bottom-recirc_5ea39050-b02b-4564-a325-6e10f42de841_text2vec1* (2021).
[28] Stephen Cobb, *Data Privacy And Data Protection: Us Law And Legislation.* ESET WHITE PAPER, pp.1-15 (2016).
[29] *Id.*
[30] *Id.*

range of techniques, in the context of organizational operations, for managing data transactions efficiently, while also maintaining data privacy and data protection.[31]

First, the US Network Advertising Initiative (NAI) is a template for managing data transactions while adhering to regulatory and protection requirements, especially within the geographical boundaries of the US.[32] This instrument was established in 1999 as the basis of a robust self-regulation framework, which was primarily concerned with the activities of third-party digital-advertising bodies. Moreover, it depended on thorough review procedures for each new member, along with analysis of consumer concerns, and the deployment of technical monitoring tools. The resulting "set of self-regulatory principles that require NAI member companies to provide notice and choice with respect" can be used to support organizational compliance.[33] Meanwhile, the Fair and Accurate Credit Transactions Act (FACTA) is another example of data-transaction regulation, implemented in 2003 to safeguard the interests of consumers from identify theft; it obliged actors to ascertain the accuracy of consumers' credit information to the utmost possible level.[34] Meanwhile, a further, state-level initiative[35] is the California Consumer Protection Act (CCPA), which regulates for-profit entities in their performance of business activities throughout the US, but especially in California. This instrument was enacted on January 1st 2020. The Act reflected the fact that, "to ensure

---

31 *Supra* note 28.
32 Shawn Marie Boyne, *Data Protection In The United States*, 66 AM. J. COMP. L. 299, 343 (2018).
33 Saranga Komanduri, Richard Shay, Greg Norcie, Blase Ur, Lorrie Faith Cranor, *Adchoices Compliance with Online Behavioral Advertising Notice and Choice Requirements,* 7 I/S: J.L. & POL'Y FOR INFO. Soc'y 603, 604 (2012).
34 *Ibid.*
35 Capgemini Research Institute, *Championing Data Protection and Privacy: A Source of Competitive Advantage in the Digital Century*, p.1-33 (2019).

compliance with existing data-protection regulations - and lay the foundation for those to come - organizations are making significant investments in advice and technology upgrades."[36]

Indeed, a coordinated and coherent legislative and regulatory approach to data security does not merely help the consumer, but helps private companies to overcome data-related challenges around privacy. The importance of having a rational regulatory framework also allows businesses to make use of the immense potential that personal data affords, without compromising privacy. Thus, the reconciliation and rationalization of conflicting regulatory requirements makes it much easier to address data issues, thereby averting problems of duplication and gaps.[37]

Nonetheless, in the US context, an analysis of data-protection legislation requires the consideration of an assortment of varied legal norms, not only at the state but also at the federal level. Such norms do, collectively, help to protect the data of US citizens, especially on financial data protection.[38] The US Federal Trade Commission (FTC) is empowered, by specific legislation, not only to safeguard consumers against deceptive and unfair practices, but also to enforce regulations on data protection and privacy (ex. Federal Trade Commission Act, §§ 5(a), 5(n), 15 U.S.C.A. §§ 45(a), 45(n)). Meanwhile, "other federal statutes primarily address specific sectors, such as financial services or healthcare. In parallel to the federal regime, state-level statutes protect a wide range of privacy rights of the individual residents."[39] The template for FACTA was amended by the FCRA to restrict information about the creditworthiness and credit

---

[36] *Ibid.*
[37] JAY COHEN, TIM CERCELLE, & NIELS AAFJES, DATA PRIVACY AS A STRATEGIC PRIORITY, PP.3-11(2019).
[38] Paul F. Pittman & Kyle Levenberg, *USA: Data Protection Laws and Regulations 2021*. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (2021)
[39] *Ibid.*

standing of individuals, as well as data regarding "character," personal traits, capacity, mode of living, the general reputation of the individual and his/her respective credit patterns.[40] Data of this kind can be critical in determining employment, as well as eligibility for credit or insurance. Regulation of such data implicates the information stored in relation to credit cards, and even the figures on printed receipts. Moreover, FACTA and the FCRA address the requirement to destroy personal information, while controlling the use of information retrieved from affiliated companies, including data used in marketing operations.[41]

In addition to the measures cited above, the Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Telephone Consumer Protection Act (TCPA), and the Family Educational Rights and Privacy Act (FERPA), among others, are all significant in terms of data protection of 15 U.S.C.A. §§ 1681c(g), 1681n.[42] Meanwhile, it may be said that the US has done much to implement data-transaction regulation to confront issues such as registration formalities, the recruitment of data-protection processors and officers, key principles of data security, the creation of competent authorities, individual rights, and the implications of technical change.

---

[40] Golden Data Law, *What is a 'consumer report'?* Retrieved from https://medium.com/golden-data/what-is-a-consumer-report-61d7ba149673 (2019)

[41] JAY M. ZITTER, *Validity, Construction, and Application of Credit Card Number and Expiration Date Truncation Requirement, and Related Provisions, of Fair and Accurate Credit Transactions Act (FACTA),* A.L.R. FED. 2D 273 (2010).

[42] UPMC, HIPAA PRIVACY & SECURITY AWARENESS. TRAINING FOR STUDENTS, pp.1-16 (2010).

2.2. Techniques used in China

Privacy is a fundamental human right, and it is recognized as such in the western societies.[43] Privacy regulation emphasizes the safeguarding of human dignity, and it is thus central to democratic societies. Such regulation also involves the reinforcement and support of other rights, such as those of freedom of expression, association and information.[44] Indeed, the right to privacy presupposes that individual also possess the right to autonomous development, liberty, and free interaction with others.[45] Admittedly, many actors in the private sphere (both businesses and individuals) are eager to minimize state intervention, seeking to develop their own ways to manage the uninvited intrusion of third-parties into the sphere of private data.[46] In any case, the "activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued."[47]

In a Chinese context, interference by businesses in personal data is most closely associated with financing instruments, such as letters of credit and bank transfers.[48] The data localization is

---

[43] Privacy International. *What Is Privacy?* Retrieved from https://privacyinternational.org/explainer/56/what-privacy (2017).
[44] Teresa Thorp, *The Right to Know and the Duty to Disclose: Pathways to Effective Monitoring, Reporting, and Verification Within the Constitutionalism of Climate Justice*, 30 PACE ENVTL. L. REV. 140, 143 (2012).
[45] Andrew W. Torrance & Eric von Hippel, *The Right to Innovate*, 2015 MICH. ST. L. REV. 793, 795–96 (2015).
[46] Doug Barry, *A Basic Guide To Exporting*, US DEPARTMENT OF COMMERCE (2015).
[47] Privacy International and the Law and Technology Center. *The Right to Privacy in China.* UNIVERSAL PERIODIC REVIEW, Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwji1MC03O32AhXQQc0KHXMmAKcQFnoECAYQAQ&url=https%3A%2F%2Fuprdoc.ohchr.org%2Fuprweb%2Fdownloadfile.aspx%3Ffilename%3D142%26file%3DEnglishTranslation&usg=AOvVaw2LC1t-jAKwjTEa5R_NCrZf p.1-10 (2013).
[48] James E. Byrne, *Contracting Out of Revised Ucc Article 5 (Letters of Credit)*, 40 LOY. L.A. L. REV. 297, 303 (2006).

a significant outcome of data-transaction regulation in China, the impact of which can be seen in the development of remittances, which are facilitated with the support of so-called "mobile money."[49] Especially within emerging markets, services associated with mobile platforms seem set to become the primary model for domestic payments. It has also been found that the expansion of the (numerous) mobile-money services has contributed to increasing cross-border transfers. According to the document, a total of 184 unique corridors have been established globally, which may be used not only for sending, but also for receiving international remittances.[50] More sophisticated connections will likely be established between the 35 "sending" and the 40 "receiving" nations. Meanwhile, it should be noted that, "data localization requirements may directly conflict with AML/CFT requirements around international remittances, making it impossible for providers to comply with both regulatory frameworks."[51] Currently, nonetheless, the implementation of data-transaction regulations, and their associated techniques, have made a major contribution to addressing localization requirements, which are "a government's legal criteria on foreign and private companies to either build and use local storage and processing infrastructure, or stop data collection and transfer altogether. This implies building domestic data centers and indigenous data processing staff."[52]

---

[49] Colin C. Richard & Dodd-Frank, *International Remittances, and Mobile Banking: The Federal Reserve's Role in Enabling International Economic Development*, 105 NW. U.L. REV. COLLOQUY 248 (2011).

[50] *Id.*

[51] Claire Scharwatt, *The impact of data localisation requirements on the growth of mobile money-enabled remittances.* GSMA MOBILE MONEY. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf (2019).

[52] Akın Ünever & Grace Kim, *Cross-Border. Data Transfers and Data Localization.* EDAM CYBER POLICY PAPER SERIES. Retrieved from https://edam.org.tr/wp-content/uploads/2017/03/data_transfers_en.pdf (2016).

Personal Financial Information (PFI) is a significant factor in this area, although it actually comprises both personal and non-personal data.[53] PFI is affected by the collection, generation, and security of data, along with their processing, especially in association with financial products or services. In the Chinese business environment, PFI is retained by businesses until the business operation in question is completed, but explicit consent must be obtained from data subjects.[54] To ascertain the security and integrity of recipients and/or data processors, appropriate measures must be taken, such as maintaining on-site diligence and the use of explicit processing agreements.[55] To the extent that PFI principles are properly followed, "the regulatory environment concerning data protection in China continues to evolve rapidly, so it remains crucial to monitor developments and react accordingly."[56] In fact, China has made significant progress in terms of data-transaction regulation, including the maintenance of security and the prevention of fraud. Nonetheless, existing regulations should be supplemented with those from the US because of the comprehensiveness of the existing establishment such as Federal Trade Commission Act, so that existing gaps can be identified and addressed at the earliest opportunity.

---

[53] Jacques de Werra, *Using Arbitration and Adr for Disputes About Personal and Non-Personal Data: What Lessons from Recent Developments in Europe?*, 30 AM. REV. INTL. ARB. 195, 197–98 (2019).

[54] Scott Thiel, Carolyn Bigg, Venus Cheung & Fangfang Song, *Section 10: Stricter data localization and security rules for financial and insurance data in China.* Retrieved from https://www.dlapiper.com/en/china/insights/publications/2020/03/navigating-china-episode-10/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration (2020).

[55] Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight-What the Proposed Eu Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 835–45 (2012).

[56] *Supra* note 54.

A general data-protection statute was originally absent in China, although certain "traces" of data protection existed within the vast collection of sector-specific legal instruments.[57] Finally, however, 2021 saw the passage of the Personal Information Protection Law (PIPL), which came into effect on November 1, 2021.[58] The law created a template to allow all security agencies dealing with personal information to work together, thus ensuring (theoretically) that personal information is protected. This initiative runs in parallel with China's existing Cybersecurity Law (CSL) and Data Security Law (DSL).[59] These legal initiatives will affect every company, domestic and foreign, that handles data within China.

The Personal Information Protection Law gives clear guidelines regarding which information can be classified as "personal."[60] It also lays down the obligations that those who handle such information must respect, with a view to streamlining how the information is processed.[61] In the event that provisions regarding data protection are violated, stringent measures are imposed.[62]

The Personal Information Protection Law also avoids an unduly specific sectoral approach to data protection. As an instrument of "cumulative effect," it clarifies the impact of the Chinese approach as regards data protection. The law has the added advantage, or at least the added

---

[57] Paul de Hert & Vagelis Papakonstantinou, *The data protection regime in China.* DIRECTORATE GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS (2015).
[58] J. D. Supra. *China's Personal Information Protection Law (PIPL) Takes Effect on November 1, 2021.* Retrieved from https://www.jdsupra.com/legalnews/china-s-personal-information-protection-9128602/ (2021).
[59] *Id.*
[60] Interview with Dr. Lao Dongyan, Professor at Tsinghua Univeristy (translation) (2022).
[61] *Id.*
[62] The National People's Congress of the PRC. *Personal Information Protection Law: Constructing processing rules centered on 'notification-consent' (translation).* Retrieved from http://www.npc.gov.cn/npc/c30834/202108/c923fa7af84e4275bcd07ce3263ef057.shtml (2021).

characteristic, of clearly distinguishing between regulatory models in China and the others, and this lack of ambiguity will be useful in terms of data processing. On one side, it could be easier for government to control the data regulations regarding international issues; on the other hand, it gives the space for the new law tryout and expand for the future. In some scenarios, at least, robust modes of data protection (against rights violations) do currently exist in China, and they aim at safeguarding individual consumers. The Law addresses both basic and evolving technical concepts of data protection, and such a comprehensive approach is "instrumentally necessary for the development of e-commerce."[63]

In terms of financial data-transaction systems in China, research shows that the most commonly used are Interbank Clearing and Settlement Systems (ICSS), together with Post-Trade Clearing, Processing, and Securities Settlement Systems.[64] ICSS themselves comprise a range of sophisticated systems, including the High-Value Payment System (HVPS), Cheque Image System (CIS), Bulk Electronic Payment System (BEPS), China Domestic Foreign Currency Payment System (CDFCPS), and Local Clearing Systems.[65] Meanwhile, the Post-Trade Clearing, Processing, and Securities Settlement Systems encompass Central Counterparties and Clearing Systems, which can be further sub-divided into SD&C securities and SHCH clearing systems, alongside Securities Settlement Systems. Finally, the latter can also be divided into three components, namely, the SD&C Securities Settlement System, the CCDC Central Bond

---

[63] Paul de Hert & Vagelis Papakonstantinou, *The data protection regime in China: In-Depth Analysis.* POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, pp.5-32 (2015).

[64] CPSS RED BOOK, PAYMENT, CLEARING AND SETTLEMENT SYSTEMS IN CHINA, pp.23-58 (2012).

[65] László Kajdi, *A Western Diet with Chinese Spices – The Specificities of Payments in China*. FINANCIAL AND ECONOMIC REVIEW, VOL. 16, Special Issue, pp. 140–169 (2017).

Generalized System, and the SHCH Registration and Settlement system.[66] In sum, given the complexity of the structures for financial transactions within China, any deficiencies in regulation will have serious consequences, and regulations themselves must continually be revised. [67] Any regulatory "gaps" must be identified, and adequate measures for data-transaction regulation put in place.

[66] *Supra* note 64, at 62.
[67] *Ibid.*

III. Chapter 3: Data-Transaction Regulation Techniques of the US, as examples for China

The commercial-privacy regime of the US is arguably the oldest, but also one of the most robust, effective, and well-developed data-transaction regulation systems in the world.[68] The privacy system therein is also known for its relatively flexible and non-prescriptive nature. Moreover, the US privacy regime depends largely on *post-hoc* government enforcement and private litigation. [69] Indeed, although the US has sophisticated regulations regarding commercial privacy and data security, the deterrent role of litigation is a major factor in the efficacy of the model.

There are several factors that make the data-transaction approach of the US a positive example to be followed by other countries, as a reference point for attaining economic growth and development over time. Contextually, it should be noted that "with certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy,[70] but rather, allows injured parties (and government agencies) to bring legal action to recover damages for […]'unfair or deceptive' business practices."[71]

While with high requirement of initial data protection, the California Consumer Protection Act and the US Federal Trade Commission (FTC) are useful examples of the techniques used by US administrators in managing data-transaction regulation. Both the Act and the Commission deal extensively with the commercial entities within their jurisdictions, with a view (for

---

[68] Vivek Mohan, *The Strength of the U.S. Commercial Privacy Regime.* HARVARD KENNEDY SCHOOL OF GOVERNMENT OFFICE OF SCIENCE AND TECHNOLOGY POLICY (2014).
[69] ALAN CHARLES RAUL, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW (2014).
[70] *Id.*
[71] MARCO MARTUZZI & JOEL A. TICKNER, THE PRECAUTIONARY PRINCIPLE: PROTECTING PUBLIC HEALTH, THE ENVIRONMENT AND THE FUTURE OF OUR CHILDREN, p.208 (2004).

example) to protecting consumers against unfair business practices. Such work obviously encompasses issues of data security and privacy. The United States applies various regulations across its 50 states, and dependent territories, for the appropriate management and safeguarding of data, such as Commission Rule 1.98, 16 C.F.R. Sec. 1.98; Consumer Protection. Section 5(a), etc.[72] There are also regulatory mechanisms to govern (e.g.) the appropriate utilization of social-security numbers, adherence to privacy policies, and notifications associated with data breaches.[73] No system is perfect, but given their comprehensiveness, and the fact that relatively long usage has provided opportunities for refinement and the detection of lacunae, the data-transaction regulatory regime of the US serves as a benchmark for data security and the protection of privacy.

Nonetheless, if one seeks to treat US legislation as an exemplar, one must consider the variation in federal law as it pertains to different fields. This includes the area of 'affirmative prohibitions,' as well as restrictions imposed on the different commercial sectors.[74] These nuances can be seen in the restrictions concerning the accessibility of financial and medical data, alongside the regulation of electronic communications in the context of children's privacy, 'consumer reports' in credit and employment, background investigations, and various other areas. Moreover, numerous privacy regulations have accrued at the state-legislative level, over time.[75] In the words of one commentator, "The United States has some of the strictest data-breach notification standards in the world and these standards have been in place far longer than

---

[72] Federal Trade Commision, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority.* Retrieved from https://www.ftc.gov/about-ftc/mission/enforcement-authority (2017).
[73] DLA Piper, DATA PROTECTION LAWS OF THE WORLD, pp.2-9 (2021).
[74] Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 175 (1999)
[75] *Id*.

most other countries."[76] Both state governments and the federal government have been active in enacting laws and designing regulation. One consequence of this is that US data-transactional rules have become something of a mosaic.

State law is generally preempted by federal law on given subjects, even though in certain instances, state law may not be subjected to any form of federal preemption.[77] In this case, some laws and regulations concern the application of varied forms of information, such as those used in the financial or health sectors, while others address the use of more homogeneous types of information, as in commercial emails or telemarketing. The application of financial-transaction regulation at the national level takes into account its role in combating "unfair and deceptive trade practices."[78] National regulation thereby plays the leading role in the development, as well as the enforcement of privacy-related protections. Nonetheless, it is not unusual for *state-level* attorneys-general to take initiatives of their own regarding privacy and cybersecurity standards.[79] Thus, US data-transaction regulation offers a wealth of examples that may, in due course, be transposed to other countries as a foundation for nascent regulatory templates.

3.1. Personal Information Protection Law in China

The People's Republic of China was obliged to establish a right to privacy before promulgating data-protection rules. The recognition of this right was a necessary first step in the

---

[76] Michelle A. Reed, *A Guide to US Data Protection.* TRADE SECURITY JOURNAL, (9), pp.1-4 (2018).
[77] Hope Babcock, *Can Vermont Put the Nuclear Genie Back in the Bottle?: A Test of Congressional Preemptive Power*, 39 ECOLOGY L.Q. 691, 695 (2012).
[78] Ulrike Spangenberg, Ann Mumford & Stephen Daly, *Moving Beyond the Narrow Lens of Taxation: The Sustainable Development Goals As an Opportunity for Fair and Sustainable Taxation*, 26 COLUM. J. EUR. L. 36, 73 (2019)
[79] *Supra* note 75.

process of protecting personal information. Compared with the United States and the European Union, however, the idea of "privacy" in China was not well developed. As Western countries expanded privacy rights to encompass personal-data protection, China continued to lag behind. Nonetheless, China passed one of the world's harshest data-privacy laws in August 2021, threatening violators with fines of up to $7.8 million, or 5% of annual revenue.[80] China is building its data-protection regime on the basis of its Personal Information Protection Law (PIPL). In fact, the PIPL was the first piece of Chinese legislation to grant citizens wide-ranging protection, and rights, in terms of their personal data.[81] The comprehensive law also applies to entities conducting business within and outside China.[82] It places significant restrictions on how individuals and companies can collect and handle people's personal information.[83] It therefore helps to position China as a leading player in global data security, with robust constitutional provisions safeguarding citizens, state entities, and firms.

Although the PIPL will play a significant role in stopping theft and unauthorized trading of personal data in China, it also reflects the government's national security concerns and interests, and it builds upon recent-data security and cybersecurity regulations.[84] The PIPL ostensibly places those overseas companies not aligned with the stipulated rules on a blacklist, thus

---

[80] Alexa Lee, Mingli Shi, Qiheng Chen, Graham Webster, Jamie P. Horsley, and Kendra Schaefer, *Seven major changes in China's finalized Personal Information Protection Law*. BROOKINGS. Retrieved from https://www.brookings.edu/articles/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (2021).

[81] Interview Script from Mr. Fang Yu, Director of Internet Law Research Center at China Academy of Information and Communications Technology (translation) (2022).

[82] Steven Jiang & Jill Disis, *China passes sweeping data privacy law, stinging tech stocks again.* CNN. Retrieved from https://www.cnn.com/2021/08/20/tech/china-data-privacy-law-intl-hnk/index.html (2021).

[83] Sullivan & Cromwell LLP, Personal Information Protection Law of the People's Republic of China—Overview, pp.1-30 (2021).

[84] Matt Burgess, *Ignore China's New Data Privacy Law at Your Peril*. Retrieved from https://www.wired.com/story/china-personal-data-law-pipl/ (2021).

preventing them from processing Chinese personal data, by which "Overseas companies that don't fall into line with PIPL or harm the national security of China could effectively gets banned from processing Chinese personal data — opening the door to international tit-for-tat retaliation against businesses."[85] Two notable victims of the law were, in fact, LinkedIn and Yahoo; both companies duly withdrew from the Chinese market, claiming that the legal and business environment was too challenging.[86] Nonetheless, a closer analysis of the new law reveals two key issues. Firstly, the PIPL does not provide granular detail for most of the public-interest issues covered therein. Rather, it provides broad principles and goals, while outlining mandates of enforcement for regulators. The latter are thus empowered to draft and implement rules and standards.[87]

Meanwhile, the Personal Information Protection Law focuses on protecting individuals, communities, and Chinese national security from potential risks likely to arise from mismanagement and mishandling of personal information.[88] The promulgation of new privacy laws in China has left most tech companies confused in terms of compliance. Nonetheless, it makes China, for the first time, a credible competitor for the United States in the race to promulgate global digital standards.[89] China has enacted sweeping regulations in this regard, making it the third major international player after the US and Europe. Multiple business groups from the United States protested to the National People's Congress that the punitive monetary penalties, vague language and complex liabilities of Chinese law were unnecessary and

---

85 *Id.*
86 *Supra* note 80.
87 *Supra* note 83.
88 VICKY LIU, XU KE, YAN LUO, & ZHIJING YU. ANALYZING CHINA'S PIPL AND HOW IT COMPARES TO THE EU'S GDPR (2021).
89 Emmanuel Pernot-Leplay, China's Approach on Data Privacy Law: A Third Way Between the US and the EU? PENN ST. JL & INT'L AFF., 8, 49 (2020).

burdensome. In effect, they claimed that the prescriptive new law would limit creativity and innovation[90]. These criticisms were all the more significant, given the continuing lack of an overarching federal data-protection law in the US itself. Thus, the establishment and implementation of the PIPL may enable China to influence global data-privacy regulations and standards, but it does not follow that this influence is uniformly benign.

While the PIPL may appear to be China's version of Europe's General Data Protection Regulation, it differs from the latter and contains additional obligations. The clauses regarding "critical infrastructure information" within the Chinese legislation, for instance, are absent from the EU's GDPR.[91] The category contains provision for both personal and public-security data. Thus, companies should assess and adjust their operations, depending on the type of information they handle.

Nonetheless, the restrictive nature of the Personal Information Protection Law gives government agencies and officials "protective" power and control over private firms and individuals. As implementation of the new regulations gains momentum, a closer analysis places the new Chinese data model somewhere between the United States market-driven approach and Europe's privacy-oriented template.[92] In fact, research indicates that Chinese legislators and regulators have borrowed from *both* the American and the European models.[93] Nonetheless,

---

[90] Jake Holland, *China's privacy law adds to international compliance patchwork*. Retrieved from https://news.bloomberglaw.com/privacy-and-data-security/chinas-privacy-law-adds-to-international-compliance-patchwork (2021).

[91] Latham & Watkins Data Privacy & Security Practice, *China Introduces First Comprehensive Legislation on Personal Information Protection*. Retrieved from https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection (2021).

[92] Michael L. Rustad & Thomas H. Koenig, *A Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019).

[93] ROGIER CREEMERS, CHINA'S EMERGING DATA PROTECTION FRAMEWORK (2021)

trying to make sense of the Chinese legal order using Western legal frameworks may create blind spots, since various elements of the Chinese legal system are not captured in the West's legal theory. These elements are critical in understanding the conception, implementation and enforcement of Chinese laws. Furthermore, since legal developments take place in wider social, national and cultural contexts, exclusively legalistic comparisons may miss important details.

"Privacy" is the main foundation on which the protection of personal information, within Chinese data law, currently rests. In the United States and the European Union, there is a close connection between data protection and privacy. In these jurisdictions, privacy provides the foundation upon which constitutional framers built their respective legislative edifices.[94] Nevertheless, in the Chinese context, privacy is not merely an analytical concept, and it does not enjoy explicit constitutional like other countries as well.[95] It may be noted, for example, that privacy is not overtly recognized as a fundamental human right within the PIPL. Therefore, the latter can be considered as an *emerging* system closely related to the well-established legal frameworks in the United States and Europe.[96]

Since the Chinese political regime prioritizes secrecy and information management, information security is a key consideration for the Party leadership.[97] On the other hand, discussions related to privacy and data protection often align with liberal constitutional principles. The Constitution of the EU, for instance, specifies that both individuals and commercial entities possess a fundamental right to informational privacy and personal-data

---

[94] *Ibid.*
[95] *Supra* note 88.
[96] *Ibid.*
[97] Interview with Professor Zhou, Deputy Director and Researcher of the Institute of Law, Chinese Academy of Social Sciences (translation) (2022).

protection.[98] Thus, the European Union remains committed to the constitutional protection of personal data and private information, which is a significant issue of concern around cross-border information flows[99]. This concern often looms large in relations between Europe and the United States. Unlike the European Union, the United States does not restrict cross-border data transfer. It may thus be argued that, in order to achieve cross-border commercial and technological advantage, US administrations have made strategic use of deliberately low privacy requirements.[100]

Nonetheless, the European Union and the United States continue to share and allow free flows of information across borders, despite existing constitutional difficulties. By contrast, the Chinese constitutional structure embraces an authoritarian system that elevates government and its agencies over individuals and private companies.

National security and sovereignty are issues that often arise in discussions of data governance and privacy across jurisdictions. China's Personal Information and Protection Law, and Europe's data-protection regulations, support their respective narratives relating to national security and sovereignty. Beyond labels, however, the two models have little in common in these areas, either philosophically or conceptually.[101] Similarly, although the United States pegs its data-protection laws on liberal-democratic ideas, it increasingly enforces its regulations in a

---

[98] Daniel E. Newman, *European Union and United States Personal Information Privacy, and Human Rights Philosophy - Is There A Match?*, 22 TEMP. INT'L & COMP. L.J. 307 (2008).
[99] Alexandra Levine, *US stands pat on privacy legislation as China, others move forward.* Retrieved from https://iapp.org/news/a/us-stands-pat-on-privacy-legislation-as-china-others-move-forward/ (2021)
[100] SVETLANA YAKOVLEVA & KRISTINA IRION, PITCHING TRADE AGAINST PRIVACY: RECONCILING EU GOVERNANCE OF PERSONAL DATA FLOWS WITH EXTERNAL TRADE (2022).
[101] Wanshu Cong, *The spatial expansion of China's digital sovereignty: Extraterritoriality and geopolitics,* Retrieved from http://dx.doi.org/10.2139/ssrn.4019797 (2021).

manner that supports sovereignty and nationalism. Indeed, the US approach to national security and sovereignty, in data-regulative terms, is not far removed from that of China.

The Chinese government has adopted, implemented, and enforced the PIPL as the foundation for government control over Internet actors and digital companies. In addition to this, the law also serves as an instrument of international policy. In geopolitical terms, several of its concepts have a long history; they may be traced to the country's "Principles of Peaceful Coexistence," as developed in the 1950s.[102] As a result, the PIPL has roots in traditional notions of territorial sovereignty and security. While the PIPL resembles Europe's data-protection law in many respects, nonetheless, it often fails to address privacy concerns; in China, for reasons of culture and politics, the latter are perceived differently at the conceptual level. Nonetheless, the constitutional provisions across the three regions (US, EU and China) implicate broader policy areas beyond data protection and privacy. They concern other issues, such as cybersecurity, platform governance, telecommunications, and digital infrastructure. Concerning data governance, for instance, constitutional requirements extend to both personal and non-personal data.[103] The European Union's Data Governance Act restricts cross-border access to certain non-personal data from beyond its geographic area, which also gives the General Data Protection Regulation stronger than the PIPL.[104] In this case, the use of broader data-related conceptualizations shows that digital sovereignty is not merely a matter of fundamental rights and values; it also encompasses policies around national security, economics and industry.

---

[102] *Supra* note 100.
[103] *Id.*
[104] Jacques de Werra, *Using Arbitration and Adr for Disputes About Personal and Non-Personal Data: What Lessons from Recent Developments in Europe?*, 30 AM. REV. INT'L ARB. 195, 198 (2019).

IV. Chapter 4: Suggestions for China, considering the example of the United States

In China, because of problematic approaches to personal privacy and excessive data harvesting, data-security incidents have become a regular occurrence, and most of them affect ordinary citizens.[105] In May 2020, due to violations of laws and regulations, such as serious underreporting of capital-transaction information and the underreporting of credit-asset-transfer business (in terms of both reporting *per se* and data quality), the China Banking Regulatory Commission issued nine simultaneous fines.[106] Several major Chinese banks (including the Bank of Construction Industry and Agriculture, Communications Bank, Postal Savings Bank, CITIC, and China Everbright) were fined a total of 19.7 million yuan, which is 3.13 million US dollars.[107] This reflected a serious, ongoing pattern of data breaches. In the past two years, for example, 500 million pieces of personal information from the Huazhu Group have been leaked, and 4.7 million pieces of data from the "12306" website (a rail-ticketing platform) have been sold by criminals.[108] Meanwhile, the listed company, Datatang, has been investigated for the crime of misusing citizens' personal information, and the APP Special Governance Working Group has found a series of data-related infringements.[109]

The behavior of certain Chinese business sectors has been "challenging" for some time, even if the pattern of illicit conduct has varied throughout time. Some of these issues date back to the

---

[105] Karthi Softek, *More than 4.7 million pieces of suspected 12306 user data were trafficked. Suspects were detained*, Retrieved from https://blog.birost.com/a?ID=01500-4abb81e2-4334-4bc1-9a88-c4bb73ba8817 (2020)

[106] Emilio Demetriou-Jones, *Chinese regulator issues first fines for lax data reporting*, GLOBAL BANKING REGULATION REVIEW, pp.1-2 (2020).

[107] Interview with Professor Zhi Zhengfeng, Researcher at the Institute of Law at the Chinese Academy of Social Sciences (translation) (2022).

[108] *Id.*

[109] *Supra* note 105.

pre-reform period. It has been demonstrated that the Chinese Communist Party (CCP), in its policy decisions of the late 1970s, contributed heavily, not only to rapid economic modernization, but to the sponsoring of economic growth *without* suitable regulatory measures.[110] The modern Chinese government is broadly committed to the free market, and as it competes with the US and other countries, it welcomes commercial transactions within China. In the current scenario, however, the party (operating through national agencies) seeks to exercise its economic power not only to co-opt but also to coerce other countries.[111] The implicit aim to is to encourage foreign societies and their politics to align themselves with the goals of the CCP, or at least to accommodate those goals. The Chinese government also seeks to reform international organizations in alignment with the nation's particular brand of "market socialism."[112]

Simultaneously, the CCP is constructing a world-class military as a rival for that of the United States.[113] In fact, "these actions enable the CCP to credibly pursue the quest - proceeding outward through the Indo-Pacific region and encompassing the globe - to achieve 'national rejuvenation' culminating in the transformation of the international order."[114] It can, in this context, be stated that China-US relationships concerning the transaction and regulation of data both reflect, and comprise a portion of, a wider geopolitical competition.

---

[110] Richard Von Glahn, *The Economic History of China: From Antiquity to the Nineteenth Century*, CAMBRIDGE UNIVERSITY PRESS. doi: www.10.1017/CBO9781139343848 (2016).
[111] *Id.*
[112] *Id.*
[113] Office of Policy Planning (Office of the Secretary of State). *The Elements of the China Challenge*. p.1-72 (2020).
[114] *Id.*

Despite emphasizing data security, Chinese law puts personal data at stake. The legal framework does not focus on safeguarding individual interests. Rather, the Chinese approach tends to address the collection of significant volumes of data for specific populations, instead of specific persons.[115] China's regulatory behavior also suggests that it is restricting cross-border flows of data by exploiting narratives around sovereignty and national security. Emphasizing such national-sovereign concerns allows China to maintain a cautious approach to its global engagements.[116] PIPL, and China's other new forms of data regulation, supposedly mimic the United States style of open-ended obligations, which do not constrict international data flows. This theoretical aspiration is not, and may not be, realized in practice, however, and considerable room may remain for "authoritarian maneuvers." Like the United States and EU, China repurposes its regulatory (PIPL) threshold beyond the context of national security.[117] Nonetheless, the new law remains narrower than its European Union and the US counterparts. Therefore, China needs to (re)consider incorporating provisions that promote commerce *alongside* national security and territorial sovereignty.

4.1. Recommendations for China considering the "Data Examples" of the US

Today, vast numbers of transactions depend on Sino-American technological interdependence, as, in many ways, does the efficiency of international data regulation.[118] This leads to a series of challenges, starting from cross-border data flows, data security and data privacy. The limitations of this technological relationship can, at times, even work to overcome

---

[115] *Supra* note 89, at 10.
[116] *Supra* note 100.
[117] *Supra* note 88.
[118] Garrick Apollon, *Sino-American Contract Bargaining and Dispute Resolution*, 13 PEPP. DISP. RESOL. L.J. 385, 392 (2013).

the protection of intellectual property (IP), as well as exacerbating traditional threats of cyber-espionage.[119] Deficiencies in US-China cooperation have also generated new problems in data management, often associated with the digital technologies that have become so critical in the modern global economy.[120] In fact, "the right way to address these issues […] requires a broader approach than narrowly focusing on them within the U.S.-China technology conflict." [121] At the same time, these problems offer an opportunity for the US to propose a holistic, comprehensive approach to Internet governance, which two governments could potentially working on together to secure a safer internet environment.[122]

The conduct of the Chinese government reflects both short-term priorities and the long-term ambitions of the CCP, and it is also driven by its perceptions of current developments in the geopolitical environment.[123] The US has not understood Chinese global strategy particularly well, and "this prolonged failure in China policy could turn out to be the biggest US policy deficiency in the past seven decades, given the accumulating dangerous strategic consequences of the rise of Chinese power for world order as well as for the United States and its allies and friends."[124] Data transactions and data security comprise merely one aspect of the problematic Sino-American relationship, but a highly important one.

---

[119] Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 242 (2010).
[120] Samm Sacks, *Addressing the Data Security Risks of US-China Technology Entanglement.* YALE LAW SCHOOL, pp.1-7 (2021).
[121] Marianne Schneider-Petsinger, Jue Wang, Yu Jie & James Crabtree, *US–China Strategic Competition: The Quest for Global Technological Leadership (Asia-Pacific Programme and the US and the Americas Programme)*, p.2-43 (2019).
[122] *Id.*
[123] *Supra* note 106.
[124] Robert D. Blackwill, *Trump Deserves More Credit for His Foreign Policies.* Retrieved from https://foreignpolicy.com/2019/05/07/trump-deserves-more-credit-for-his-foreign-policies/ (2019)

It is high time that China borrowed data-protection practices from countries that have proven successful in the field. The United States offers the best comparative model, owing to the robust and practical data-protection laws that have been in existence there for some time. By contrast, China has lagged behind in designing and implementing policies for data protection - a failure all the more striking, given the country's rapid technological progress. Scholars of data-privacy law note that domestic socio-economic developments require China to produce data-protection policies and laws that match international standards.[125] In this regard, fortunately, the country need not reinvent the wheel; there is much that it can learn from foreign jurisdictions in general, and the US in particular.

Unlike the United States, China lacks an elaborate, detailed model of the necessary elements to safeguard personal data and personal privacy; this remains true, despite the much-vaunted PILP. The data-protection measures in China are piecemeal and incoherent initiatives. The country is thus in danger of falling further behind in terms of data security. Nonetheless, this narrative can be changed, if these incoherent initiatives are replaced with a more effective, national data-privacy law. If it does so, China can place itself once more on the promising data-policy trajectory that originally commenced in 2014.[126] In that year, the country attempted to introduce a data-protection law, but its approach was limited in comparison to other countries (such as the US) with longer traditions of expertise in the area.[127] In 2018, however, China's policymakers indicated their renewed interest in data policy. Specifically, they announced their intention to formulate policies to *exceed* current standards obtaining in the US, if not (yet) those

---

[125] *Supra* note 88, at 82-96.
[126] United Nations, *Data-protection regulations and international data flows: Implications for trade and development.* UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, p.1-139 (2016).
[127] MACIEJ GAWRONSKI. GUIDE TO THE GDPR, p.1-50 (2019).

of the EU.[128] However, formulating a comprehensive national privacy law especially under the CCP party control is not an easy task.

Still, unlike China, the United States has well-formulated data-protection policies *today.* The latter evince a wide application, touching on all aspects of the collection and processing of personal data.[129] Conversely, the Chinese approach deals with relatively superficial aspects of personal data. In the United States, there are numerous laws that address data protection and citizens' privacy. Data-protection laws focus, for instance, on government agencies, children's data and health data.[130] They also address data breaches at both state and federal level. Many of these policies and laws were drafted years before the Chinese government even began to consider data-protection policy. In other words, the US has established a formidable lead in data security over China, and this should serve as a "wake-up call" for the latter.[131] The National People's Congress (NPC), as the supreme law-making body in China, should move with speed to enact laws for data protection, especially at the individual level. New laws are required if China's National Data Protection Authority is ever to become a truly effective defender of privacy rights and data security, on behalf of the Chinese people.[132]

To reiterate, China began to enact data-protection laws significantly later than the United states. China might thus be expected to formulate its laws somewhat differently from the US model, since circumstances have changed in recent years. The formulation of current policy

---

128 *Id.*

129 Bracewell LLP. *China's New Data Privacy Law is Sweeping and Serious: Avoid the High Cost of Noncompliance.* Retrieved from https://www.jdsupra.com/legalnews/china-s-new-data-privacy-law-is-4552583/ (2021).

130 *Supra* note 71, at 74.

131 JACQUELINE KLOSEK. DATA PRIVACY IN THE INFORMATION AGE (2000).

132 Interview with Dr. Zhao Jingwu, Associate Professor at Beihang University School of Law, Researcher at Institute of Industrial and Information Law (translation) (2022).

should not, after all, be a matter of copying and pasting. In the formulation of data-protection policy, China should also take account of certain emerging trends.[133] Technological innovations have created new paradigms, and issues that were not formerly considered violations of privacy now fall within that category, not least because of technological innovation. Indeed, technical innovations have paved the way for changes in the very definition of "data issues." Certain aspects that were not formerly considered part of the data universe, now are.[134] Therefore, since China must formulate data-protection laws in this new and complex era, its new laws should *build upon* the existing data-protection laws in the United States. China's new legal and regulatory framework must take account of recent technological advances, and it must address conspicuous lacunae that exist within the US model. This is a matter of urgency, in a commercial environment where data protection is of unprecedented importance.

Furthermore, Western countries and China have some obvious differences in their political and social alignment. For this reason alone, it would not be possible to see US laws directly imported to the Chinese domestic context. There would be major differences in the objectives of such laws, given the profound differences between the political regimes holding sway in the two countries. Thus, the "borrowing" and application of US data-protection laws should be done by modifying certain aspects, while adopting others that seem to fit the context of contemporary China.[135] The Chinese political and economic model is nominally based on socialist philosophies, which also influence Chinese data-protection and privacy rules. Similarly, US data-

---

[133] Dan Luo & Youji Wang. *China - Data Protection Overview*. Retrieved from https://www.dataguidance.com/notes/china-data-protection-overview (2021).
[134] U.S. Embassies abroad. *Privacy Shield Framework. European Union - Data Privacy and Protection*. Retrieved from https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection (2016).
[135] *Supra* note 89.

protection templates have been designed in accordance with that country's system of governance.[136] China will doubtless evince a unique approach to data-related issues owing to the country's specific sociopolitical context and geopolitical ambitions.

Nonetheless, given the expansion of China's economy, the latter will continue to process vast quantities of data, and the country must explore any potential techniques for managing that data effectively. Specifically, it might borrow from the Network Advertising Initiative (NAI) of the United States, which manages data transactions while adhering to regulatory and protection requirements.[137] Policymakers should focus on how the data stored within the frontiers of China should be regulated and protected. Third-party digital organizations should, of course, be bound by any such regulations that are made. Naturally, the main concerns of consumers regarding privacy and security must be accommodated within the model that China finally constructs. This can be facilitated by putting in place a Code of Conduct to bind all organizations involved with the collection, gathering and analysis of personal data. Furthermore, China should produce legislation broadly similar to the Fair and Accurate Credit Transactions Act (FACTA). Such an Act should be framed in a manner that safeguards the interests of consumers against identify theft, while ensuring the accuracy of consumers' credit information to the highest possible degree. [138]

China should also "borrow" the provisions of the California Consumer Protection Act (CCPA). This law does a great deal to protect individual data from theft and misuse, and the

---

[136] PYMNTS, *Deep Dive: How US Data Regulation Fragmentation Is Affecting Merchants, Consumers*. Retrieved from https://www.pymnts.com/news/regulation/2020/deep-dive-how-us-data-regulation-fragmentation-is-affecting-merchants-consumers/ (2020).
[137] *Supra* note 32.
[138] *Supra* note 33.

Chinese National People's Congress could draft similar legislation without undue difficulty. Such an Act should put in place *enforcement mechanisms* to ensure that profit-making organizations that rely on personal data comply with existing regulations and laws. This can be done by establishing a body that *checks* how commercial enterprises utilize the data at their disposal.[139] California's CCPA, being relatively recent, could be accommodated fairly easily in China, since it takes due account of technological innovations and advances not merely in the US, but globally. A coordinated approach to data protection, meanwhile, will be a significant asset not only to Chinese data consumers, but also to organizations that deal with data as one of their trading assets. Data security will be greatly enhanced if the inconsistencies between regulatory regimes can be overcome through coordination, and such coordination can also minimize problems of lacunae and overlap. A more rational, uniform and coordinated regulatory system will also reduce the risks of costly litigation for businesses.

The National Data Protection Authority in China, which names Cyberspace Administration of China (CAC) that controls everything relates to information and protection like PIPL, should also use the US Federal Trade Commission (FTC) as a benchmark; the latter has a general mandate for regulating the business environment in the United States. Indeed, China's CAC should be at the forefront in advocating regulation to protect consumers, organizations and individuals involved in data-related transactions. If the CAC can formulate such policies, both the Chinese consumer and the wider Chinese economy will benefit. The Cyberspace Administration of China should also gather comprehensive information from agencies that deal with the analysis and collection of data. Of particular interest here are insurance agencies,

---

[139] DANIEL. J. SOLOVE & PAUL M. SCHWARTZ. CONSUMER PRIVACY AND DATA PROTECTION (2020).

educational and training institutions, political-party affiliates, and so on, since these are some of the entities most highly involved in transactions associated with personal data.[140] Any future regulatory system must be rigorous, comprehensive and lucid, but it should also be constructed in a manner that will nurture, and not inhibit, the growth of data-related industries. Nonetheless, regulations should properly address the requirement to destroy personal information after use, while controlling the utilization of information obtained from different sources.

There are certain universally accepted principles regarding data-protection law, and China must integrate these into any future framework, if China wants to build a comprehensive data transaction protection law. Among the most common of these legal principles are the following: (a) data must be processed fairly and lawfully (the "fairness and lawfulness" principle); (b) data should only be processed pursuant to the purpose specified by the individual (purpose specification); (c) only the personal information necessary for that purpose should be collected and processed, and it should then be deleted (data minimization); (d) such data should be relevant, accurate and current (data quality); (e) individuals should be made aware of such processing and of their rights (transparency); (f) these rights should allow individuals to exercise control over data processing, i.e. by modifying, rectifying or deleting the data, or objecting to the processing (data-subject participation); (g) additional safeguards should be provided for special categories of data (sensitivity); (h) all data should be appropriately protected against risks such as loss, unauthorized access, destruction, misuse, modification or illicit disclosure (security and

[140] FAYE FANGFEI WANG. LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS: CONTEMPORARY ISSUES IN THE EU, US AND CHINA (2020).

confidentiality); and finally (i), data controllers should be held accountable for compliance with suitable measures giving effect to these principles (accountability).[141]

Crucially, any future Chinese model should address the need for *the public themselves to be involved in data protection.* The laws enacted must make it mandatory for data-related companies to obtain informed consent from the owners of data. Before the data of individual citizens are used, those citizens must be informed of the rationale - i.e., why the data are needed. In addition, they must be informed of the *extent* to which their information will be used, and what redress will be available if their data are used in a manner they did not anticipate. China's future laws on data protection should enshrine the right to *withdraw* one's consent at any time. Indeed, there should be a streamlined process to make it easier for members of the public to withdraw their consent, should they feel that the handling of their data does not conform to the expectations they had when that consent was given. The privacy law should provide granular detail regarding the concrete applications of necessary minimum standards. In sum, tech companies must operate with the explicit agreement of the individuals whose data they use.

In terms of the current Personal Information Protection Law (PIPL) in China, one of the most notable innovations is the declared intention to "empower individuals with full rights."[142] According to Yang Heqing, the current Deputy Director of the Economic Law Office of the Legal Affairs Committee of the Standing Committee of the National People's Congress , "The Personal Information Protection Law elevates the rights of individuals in personal-information

---

[141] Anneliese Roos, *Core Principles Of Data Protection Law.* 39 COMP. AND INT'L L. J. OF S. AFRICA, p.102 (2006). (Here, Roos compares several sources in Europe and the US to identify a set of core data-protection principles used in these legal instruments.)

[142] Interview Script from Yang Heqing, the Deputy Director of the Economic Law Office of the Legal Affairs Committee of the Standing Committee of the National People's Congress (translation) (2022).

processing activities, including knowledge of personal information processing rules and matters, consent and withdrawal of consent, as well as personal information inquiry, copying, correction, deletion, etc., [and also] the right to know, the right to decide, clarifying that individuals have the right to restrict the processing of personal information."[143] He continued by observing that, "The Personal Information Protection Law stipulates in principle the right to portability of personal information, requiring that personal information processors should provide individuals with a way to transfer their personal information under the conditions specified by the national cybersecurity and information department." [144]

At least the above represents a notable advance from the previous state of minimal protection. The legal clause "under the proper supervision" nonetheless, underlines the fact that, in China, the individual's "full rights" are only enforceable at the discretion of the government. This is conceptually different from the United States legal template, which regards data rights as inherent and inalienable.

Both in the EU and the US model, the right to personal information is a cluster of rights, and the scope is defined by legislation. National discrepancies notwithstanding, the core of the matter lies with the information subject's right to control his or her information, to "know," and to modify. Also critical are the right to erasure, the right to portability, the right to be forgotten, etc. The right to privacy in different jurisdictions must first be confirmed as a basic right, and then formulated in terms of civil tort law.[145] Also, China's privacy-protection law evinces its own independent sources, programmatic design, system configuration, law-enforcement mechanisms

---

143 *Id.*
144 *Id.*
145 Interview with Honorary Professor Wang Zejian, the National University of Taiwan (translation) (2022).

and communication platform.[146] Chinese model now comprises a professional, independent legal system, which surpasses traditional privacy protection via its deployment of complex, specialist knowledge.[147]

Against international trends, China's civil-law specialists have promoted the inclusion of personal-information protection within the field of personality rights, alongside the right to privacy. The same experts have argued that laws regarding the protection of personal information should be treated as a special branch of civil law, thus (unlike the US) mandating the fusion of two essentially different paradigms. The positioning of personal-information protection within civil legislation strikes Professor Zhou as problematic and logically confusing.[148] The root cause of the problem is the qualitative dislocation of rights. The attempt merely to reclassify a new form of public law within the sphere of traditional civil rights means ignoring the distinguishing qualities of personality rights, on the one hand, and the right to the protection of personal information on the other. This kind of mismatch will not only lead to repetition and confusion in legislation; it will also generate huge uncertainty regarding the (unclear) ownership of personal information, the nature of protection, and ambiguous legal relationships. Far better to maintain a clear distinction, as with the US CCPA, with its rights-specific goals, criteria and modes of implementation.

The Chinese government should take reasonable efforts to enhance data protection wherever possible. Chinese data-protection law should incorporate a data-user policy to detail forms of compensation for those who have their data used (or misused). Such compensation should be

---

[146] Quote from Professor Zhou Zhenghua, Deputy Director and Researcher of the Institute of Law, Chinese Academy of Social Sciences (translation) (2022).
[147] *Id.*
[148] *Id.*

structured in such a way as to encourage, not hinder, data transactions. The modern world has embraced the data economy, and personal information, when used ethically and rationally, can be an instrument for generating income. Thus, future data laws should provide payment formulae for data use. To reiterate, meanwhile, mechanisms should be put in place to deter the use of data for any other purpose than those sanctioned by the owner. In sum, if these measures are adopted in China, it is likely that China's data policies will match, or even surpass, those of the United States.

V. Conclusion

The discussion above demonstrates that data-transaction regulation is central to organizational management and performance, and even the overall economic and social development of particular countries. Advances in technology and consumer data must be measured within the contexts of security, privacy and protection, however. Different nations evince varied patterns of data-transaction regulations, with the best regulatory examples being those adhered to by businesses and governmental bodies in the US. The US techniques associated with data-transaction regulation, at federal and state level, are distinctive; they have also provided the basis of the regulatory frameworks for many other countries. The present thesis has compared the data-transaction regulations obtaining in the US and China. It has also explored some of the regulations pertaining to financial transactions in those jurisdictions, while considering factors relevant to the long-term protection of privacy and personal data. Of course, data-transaction regulations, and their associated methods, pertain directly to the ethical and legal processing of personal data by organizations, be they in the private or government domain.

Data protection implicates a wide range of rules and legislation. In the US, this includes the Fair Credit Reporting Act, the Network Advertising Initiative (NAI), the Fair and Accurate Credit Transactions Act (FACTA), and the California Consumer Protection Act (CCPA). These are benchmarks of their kind, but they achieve maximum efficacy when deployed in parallel with a self-regulatory code of conduct for data-utilizing organizations. The ethical use of data is a central pillar of a democratic society. This in turn has various dimensions, such as “liberty,” autonomous development, interaction, censorship, surveillance, and prohibition. The future development of individual nations, economically and socially, requires them to strike the right balance between ease of data usage and the protection of privacy.

This developmental process should streamline, or even render obsolete, numerous restrictions and prohibitions, by improved regulation around issues of privacy, security, protection, and potential data breaches. Future regulations should address business proceedings and the management of data transaction both online and offline. With continuous technological advances and the increasing global use of the Internet, compliance with data-transaction regulation in both the US and China will be of critical importance.

The ways that data may be collected, processed and used under US legislation underscore numerous differences *vis-à-vis* Chinese data-transaction regulations. The "techniques" and instruments associated with the US privacy regime are robust, effective and sufficiently flexible. In the US, the precautionary principle is central, and this contributes to guarding the privacy of individuals, while allowing injured parties, with the support of governmental agencies, to take legal action to redress any harm arising from illicit business practices.

Data privacy, of course, implies strict adherence to laws around data protection. It also requires the establishment of access controls for safeguarding the information retrieved by unauthorized parties, thereby maintaining data integrity and prioritizing consent from data subjects, as and when required. Data-protection laws are useless unless supplemented by effective mechanisms of enforcement; but rational, transparent regulations, properly implemented, will radically increase compliance, to the advantage of all concerned. There are certain overlapping obligations that reflect similarities between data privacy and data security. These include data integrity, access control, and accountability. If cybersecurity measures are designed and implemented with the active support of security professionals, meanwhile, both data availability and data confidentiality will be improved. Future regulatory frameworks must address the tasks of data encryption and authorization, both of which contribute to preventing

data breaches, and both of which are crucial in defending transactional data from malicious attacks.

Bibliography

Aridor, G., Che, Y.K Che & Salz, T., *The Economic Consequences Of Data Privacy Regulation: Empirical Evidence From GDPR.* NBER WORKING PAPER SERIES. Retrieved from https://www.nber.org/system/files/working_papers/w26900/revisions/w26900.rev0.pdf?sy=900 (2020).

Apollon, G., *Sino-American Contract Bargaining and Dispute Resolution*, 13 PEPP. DISP. RESOL. L.J. 385, 392 (2013).

Babcock, H., *Can Vermont Put the Nuclear Genie Back in the Bottle?: A Test of Congressional Preemptive Power*, 39 ECOLOGY L.Q. 691, 695 (2012).

Burgess, M., *Ignore China's New Data Privacy Law at Your Peril.* Retrieved from *https://www.wired.co.uk/article/china-personal-data-law#intcid=_wired-uk-bottom-recirc_5ea39050-b02b-4564-a325-6e10f42de841_text2vec1* (2021).

Blackwill, R. D., *Trump Deserves More Credit for His Foreign Policies.* Retrieved from https://foreignpolicy.com/2019/05/07/trump-deserves-more-credit-for-his-foreign-policies/ (2019)

Byrne, J.E., *Contracting Out of Revised Ucc Article 5 (Letters of Credit)*, 40 LOY. L.A. L. REV. 297, 303 (2006).

Boyne, S.M., *Data Protection In The United States*, 66 AM. J. COMP. L. 299, 343 (2018).

Cate, F.H., *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 175 (1999)

Capgemini Research Institute, *Championing Data Protection and Privacy: A Source of Competitive Advantage in the Digital Century*, p.1-33 (2019).

CPSS RED BOOK, PAYMENT, CLEARING AND SETTLEMENT SYSTEMS IN CHINA, pp.23-58 (2012).

COHEN, J., CERCELLE, T., & AAFJES, N., DATA PRIVACY AS A STRATEGIC PRIORITY, PP.3-11(2019).

Cohan, J.E. *Examined Lives: Informational Privacy And The Subject As Object.* 52 STNLR 1373, p.10 (2000).

Cobb, S., *Data Privacy And Data Protection: Us Law And Legislation.* ESET WHITE PAPER, pp.1-15 (2016).

Cong, W., *The spatial expansion of China's digital sovereignty: Extraterritoriality and geopolitics*, Retrieved from http://dx.doi.org/10.2139/ssrn.4019797 (2021).

Barry, D., *A Basic Guide To Exporting*, US DEPARTMENT OF COMMERCE (2015).

Bracewell LLP. *China's New Data Privacy Law is Sweeping and Serious: Avoid the High Cost of Noncompliance.* Retrieved from https://www.jdsupra.com/legalnews/china-s-new-data-privacy-law-is-4552583/ (2021).

BESEMER, L., TITLE PRIVACY AND DATA PROTECTION BASED ON THE GDPR (2020).

Cate, F.H., *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 175 (1999)

CREEMERS, R., CHINA'S EMERGING DATA PROTECTION FRAMEWORK (2021)

Demetriou-Jones, E., *Chinese regulator issues first fines for lax data reporting,* GLOBAL BANKING REGULATION REVIEW, pp.1-2 (2020).

DIBERNARDO, I.G., SOBEL, J.M. BEST PRACTICES FOR DATA PROTECTION AND PRIVACY LEADING LAWYERS ON CREATING A DATA PROTECTION STRATEGY, DEALING WITH SECURITY BREACHES, AND ANALYZING RECENT TRENDS IN LEGISLATION (2009).

DLA Piper, DATA PROTECTION LAWS OF THE WORLD, pp.2-9 (2021).

Federal Trade Commision, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority.* Retrieved from https://www.ftc.gov/about-ftc/mission/enforcement-authority (2017).

GAWRONSKI, M.. GUIDE TO THE GDPR, p.1-50 (2019).

Gilbert, F., *European Data Protection 2.0: New Compliance Requirements in Sight-What the Proposed Eu Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 835–45 (2012).

Glahn, R.V., *The Economic History of China: From Antiquity to the Nineteenth Century,* CAMBRIDGE UNIVERSITY PRESS. doi: www.10.1017/CBO9781139343848 (2016).

Golden Data Law, *What is a 'consumer report'?* Retrieved from https://medium.com/golden-data/what-is-a-consumer-report-61d7ba149673 (2019)

Holland, J., *China's privacy law adds to international compliance patchwork*. Retrieved from https://news.bloomberglaw.com/privacy-and-data-security/chinas-privacy-law-adds-to-international-compliance-patchwork (2021).

Hert, d.P. & Papakonstantinou, V., *The data protection regime in China.* DIRECTORATE GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS (2015).

Interview with Dr. Lao Dongyan, Professor at Tsinghua Univeristy (translation) (2022).

Interview Script from Mr. Fang Yu, Director of Internet Law Research Center at China Academy of Information and Communications Technology (translation) (2022).

Interview with Dr. Zhao Jingwu, Associate Professor at Beihang University School of Law, Researcher at Institute of Industrial and Information Law (translation) (2022).

Interview with Honorary Professor Wang Zejian, the National University of Taiwan (translation) (2022).

Interview with Professor Zhou, Deputy Director and Researcher of the Institute of Law, Chinese Academy of Social Sciences (translation) (2022).

Interview Script from Yang Heqing, the Deputy Director of the Economic Law Office of the Legal Affairs Committee of the Standing Committee of the National People's Congress (translation) (2022).

Interview with Professor Zhi Zhengfeng, Researcher at the Institute of Law at the Chinese Academy of Social Sciences (translation) (2022).

Interview from Professor Zhou Zhenghua, Deputy Director and Researcher of the Institute of Law, Chinese Academy of Social Sciences (translation) (2022).

Johnson E.H., *Data Protection Law in the European Union*, FED. LAW., 44, 44–45 (2009).

J. D. Supra. *China's Personal Information Protection Law (PIPL) Takes Effect on November 1, 2021*. Retrieved from https://www.jdsupra.com/legalnews/china-s-personal-information-protection-9128602/ (2021).

Jiang, S. & Disis, J., *China passes sweeping data privacy law, stinging tech stocks again.* CNN. Retrieved from https://www.cnn.com/2021/08/20/tech/china-data-privacy-law-intl-hnk/index.html (2021).

Kerry, C.F., *Why protecting privacy is a losing game today and how to change the game.* BROOKINGS INSTITUTE. Retrieved from https://www.brookings.edu/research/why-protecting-pravacy-is-a-loosing-game-today-and-how-to-change-the-game. (2018).

Keck, M., Gillani, S., Dermish, A., & Grossman, J., *The Role Of Data Protection In The Digital Economy.* UNCDF. Retrieved from https://policyaccelerator.uncdf.org/policy-tools/brief-data-protection-digital-economy (2021).

Komanduri, S., Shay, R., Norcie, G., Ur, B., Cranor, L. F., *Adchoices Compliance with Online Behavioral Advertising Notice and Choice Requirements,* 7 I/S: J.L. & POL'Y FOR INFO. Soc'y 603, 604 (2012).

Kajdi, L., *A Western Diet with Chinese Spices – The Specificities of Payments in China*. FINANCIAL AND ECONOMIC REVIEW, VOL. 16, Special Issue, pp. 140–169 (2017).

KLOSEK, J. DATA PRIVACY IN THE INFORMATION AGE (2000).

Lee A., Shi M., Chen Q., Webster G., Horsley J.P., and Schaefer K., *Seven major changes in China's finalized Personal Information Protection Law*. BROOKINGS. Retrieved from https://www.brookings.edu/articles/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (2021).

Latham & Watkins Data Privacy & Security Practice, *China Introduces First Comprehensive Legislation on Personal Information Protection.* Retrieved from https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection (2021).

Levine A., *US stands pat on privacy legislation as China, others move forward.* Retrieved from https://iapp.org/news/a/us-stands-pat-on-privacy-legislation-as-china-others-move-forward/ (2021)

LIU, X., KE, X., LUO, L., & YU, Z. ANALYZING CHINA'S PIPL AND HOW IT COMPARES TO THE EU'S GDPR (2021).

Luo, D. & Wang, Y.. *China - Data Protection Overview*. Retrieved from https://www.dataguidance.com/notes/china-data-protection-overview (2021).

MARTUZZI, M. & TICKNER, J.A., THE PRECAUTIONARY PRINCIPLE: PROTECTING PUBLIC HEALTH, THE ENVIRONMENT AND THE FUTURE OF OUR CHILDREN, p.208 (2004).

MÉTAYER D.L., GEORGE DANEZIS, MARIT HANSEN, JAAP-HENK HOEPMAN, RODICA TIRTEA, STEFAN SCHIFFNER & JOSEP DOMINGO-FERRER. PRIVACY AND DATA PROTECTION BY DESIGN - FROM POLICY TO ENGINEERING (2014).

MILAKOVICH, M.E., DIGITAL GOVERNANCE: APPLYING ADVANCED TECHNOLOGIES TO IMPROVE PUBLIC SERVICE (2021).

Mohan, V., *The Strength of the U.S. Commercial Privacy Regime.* HARVARD KENNEDY SCHOOL OF GOVERNMENT OFFICE OF SCIENCE AND TECHNOLOGY POLICY (2014).

Newman, D.E., *European Union and United States Personal Information Privacy, and Human Rights Philosophy - Is There A Match?*, 22 TEMP. INT'L & COMP. L.J. 307 (2008).

O'Hara, G., *Cyber-Espionage: A Growing Threat to the American Economy,* 19 COMMLAW CONSPECTUS 241, 242 (2010).

OECD. THE OECD PRIVACY FRAMEWORK, p.1-154 (2013).

Office of Policy Planning (Office of the Secretary of State). *The Elements of the China Challenge*. p.1-72 (2020).

Pernot-Leplay, E., China's Approach on Data Privacy Law: A Third Way Between the US and the EU? PENN ST. JL & INT'L AFF., 8, 49 (2020).

Pittman, P.F. & Levenberg, K., *USA: Data Protection Laws and Regulations 2021.* Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (2021)

Privacy International, *The Keys To Data Protection. A Guide For Policy Engagement On Data Protection*, p.4-98 (2021).

Privacy International. *What Is Privacy?* Retrieved from https://privacyinternational.org/explainer/56/what-privacy (2017).

Privacy International and the Law and Technology Center. *The Right to Privacy in China.* UNIVERSAL PERIODIC REVIEW, Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwji1MC03O32AhXQQc0KHXMmAKcQFnoECAYQAQ&url=https%3A%2F%2Fuprdoc.ohchr.org%2Fuprweb%2Fdownloadfile.aspx%3Ffilename%3D142%26file%3DEnglishTranslation&usg=AOvVaw2LC1t-jAKwjTEa5R_NCrZf p.1-10 (2013).

PYMNTS, *Deep Dive: How US Data Regulation Fragmentation Is Affecting Merchants, Consumers.* Retrieved from https://www.pymnts.com/news/regulation/2020/deep-dive-how-us-data-regulation-fragmentation-is-affecting-merchants-consumers/ (2020).

RAUL A.R., THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW (2014).

Richard, C.C. & Frank, D., *International Remittances, and Mobile Banking: The Federal Reserve's Role in Enabling International Economic Development*, 105 NW. U.L. REV. COLLOQUY 248 (2011).

Reed, M.A, *A Guide to US Data Protection.* TRADE SECURITY JOURNAL, (9), pp.1-4 (2018).

Rustad, M.L. & Koenig, T.H., *A Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019).

Roos A., *Core Principles Of Data Protection Law.* 39 COMP. AND INT'L L. J. OF S. AFRICA, p.102 (2006). (Here, Roos compares several sources in Europe and the US to identify a set of core data-protection principles used in these legal instruments.)

Sacks, S., *Addressing the Data Security Risks of US-China Technology Entanglement.* YALE LAW SCHOOL, pp.1-7 (2021).

Sellek, R., *Data Protection Considerations In Corporate Transactions And The Due Diligence Process.* Retrieved from https://acuitylaw.com/data-protection-considerations-in-corporate-transactions-and-the-due-diligence-process/ (2019).

Scharwatt, C., *The impact of data localisation requirements on the growth of mobile money-enabled remittances.* GSMA MOBILE MONEY. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf (2019).

Schneider-Petsinger, M., Wang, J., Jie, Y. & Crabtree, J., *US–China Strategic Competition: The Quest for Global Technological Leadership (Asia-Pacific Programme and the US and the Americas Programme)*, p.2-43 (2019).

SOLOVE D.J. & SCHWARTZ, P.M. CONSUMER PRIVACY AND DATA PROTECTION (2020).

Softek, K., *More than 4.7 million pieces of suspected 12306 user data were trafficked. Suspects were detained,* Retrieved from https://blog.birost.com/a?ID=01500-4abb81e2-4334-4bc1-9a88-c4bb73ba8817 (2020)

Spangenberg, U., Mumford, A. & Daly, S., *Moving Beyond the Narrow Lens of Taxation: The Sustainable Development Goals As an Opportunity for Fair and Sustainable Taxation*, 26 COLUM. J. EUR. L. 36, 73 (2019).

Sullivan & Cromwell LLP, Personal Information Protection Law of the People's Republic of China—Overview, pp.1-30 (2021).

Torrance, A. & Hippel, E., *The Right to Innovate,* 2015 MICH. ST. L. REV. 793, 795–96 (2015).

Thiel, S., Bigg, C., Cheung, V. & Song, F., *Section 10: Stricter data localization and security rules for financial and insurance data in China.* Retrieved from https://www.dlapiper.com/en/china/insights/publications/2020/03/navigating-china-episode-10/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration (2020).

Tsesis A., *Data Subjects' Privacy Rights: Regulation Of Personal Data Retention And Erasure*, 90 U. COLO. L. REV. 593, 612 (2019).

Thorp, T., *The Right to Know and the Duty to Disclose: Pathways to Effective Monitoring, Reporting, and Verification Within the Constitutionalism of Climate Justice*, 30 PACE ENVTL. L. REV. 140, 143 (2012).

The National People's Congress of the PRC. *Personal Information Protection Law: Constructing processing rules centered on 'notification-consent' (translation).* Retrieved from http://www.npc.gov.cn/npc/c30834/202108/c923fa7af84e4275bcd07ce3263ef057.shtml (2021).

Ünever A. & Kim G., *Cross-Border. Data Transfers and Data Localization.* EDAM CYBER POLICY PAPER SERIES. Retrieved from https://edam.org.tr/wp-content/uploads/2017/03/data_transfers_en.pdf (2016).

UPMC, HIPAA PRIVACY & SECURITY AWARENESS. TRAINING FOR STUDENTS, pp.1-16 (2010).

U.S. Embassies abroad. *Privacy Shield Framework. European Union - Data Privacy and Protection*. Retrieved from https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection (2016).

United Nations, *Data-protection regulations and international data flows: Implications for trade and development.* UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, p.1-139 (2016).

WANG F.F.. LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS: CONTEMPORARY ISSUES IN THE EU, US AND CHINA (2020).

Werra, J., *Using Arbitration and Adr for Disputes About Personal and Non-Personal Data: What Lessons from Recent Developments in Europe?*, 30 AM. REV. INTL. ARB. 195, 197–98 (2019).

White, M., Mennie, P. & Chudzynski, R., *Data Privacy Handbook. A Starter Guide To Data Privacy Compliance*, p.3-30 (2019).

World Bank Group. *Data protection and privacy laws.* Retrieved from https://id4d.worldbank.org/guide/data-protection-and-privacy-laws (2021).

YAKOVLEVA, S. & IRION, K., PITCHING TRADE AGAINST PRIVACY: RECONCILING EU GOVERNANCE OF PERSONAL DATA FLOWS WITH EXTERNAL TRADE (2022).

ZITTER, J., *Validity, Construction, and Application of Credit Card Number and Expiration Date Truncation Requirement, and Related Provisions, of Fair and Accurate Credit Transactions Act (FACTA)*, A.L.R. FED. 2D 273 (2010).

ACADEMIC VITA
JIANGYINGLUN (ALAN) YUE

EDUCATION

The Pennsylvania State University — **University Park, PA**
Schreyer Honors College, Smeal College of Business, College of Liberal Arts — *August 2018 – May 2022*
B.S. Finance (H), B.A. International Politics (H), *Minors in Legal Environment of Business*
Honors: Robert A. Scholar, Paterno Fellowship, Phi Beta Kappa (ΦBK), ΠΣA Honor, ΦHΣ Honor, ΦAΔ Honor, Dean's List 7/7

PROFESSIONAL EXPERIENCE

Mars Wrigley US — Newark, NJ
Finance Associate Intern, S&F Supply Chain Finance — *May 2021 – August 2021*
- Pinpointed $50m disconnections between Unconstrained Demand and Constrained Production Planning during S&OP cycles
- Developed 3 Visio workflows and E2E processes to mitigate 11 bridges by networking with 47 cross-functional stakeholders
- Proposed and presented redundant packaging problems of Twix and M&M with 4 interns during Mars Innovation Initiative

Argolytics, LLC — State College, PA
Business Analyst (Project), Executive Office — *Jan 2020 – May 2020*
- Created a comprehensive 5-year, 127-page business plan for the start-up, including structuring current and projected financial statements, researching markets, analyzing P&L, and intergrading products into the only SPC software solution in the U.S
- Collaborated with 11 peers on creating and delivering presentations; presented to the CEO of the company, the Business School Boards, and Ben Franklin Technology Partners to earn funding

China Development Bank (Headquarters) — Beijing, China
Summer Researcher, Treasury & Financial Market Department — *July 2019 – Aug 2019*
- Generated 63-page reports on LIBOR reform implementations, focusing on the impact of syndicated loans and derivatives
- Executed 3 presentations to Executive Board on how China banks could adjust to amendments

Summer Analyst (FOREX), Global Markets Department — *July 2019 – Aug 2019*
- Accomplished valuation training using Bloomberg, Reuters, and Wind to report business information every morning
- Practiced and learned FOREX trading with Excel under instructions of dealers who had 100b RMB trading access daily

Tarriff Center for Business Ethics and Social Responsibility — State College, PA
Researcher (Tarriff Scholar), Smeal College of Business — *Jul 2020 – Sep 2020*
- Completed a 56-page research project on Ethics and CSR to establish the fundamental database for the newly endowed center

DHH Law Firm — Washington, D.C.
Summer Legal Assistant, Washington, D.C. Branch — *May 2019 – Jun 2019*
- Compiled, analyzed, and translated 38 documents about China-US Trade War, e.g. FIRRMA Act and memorandum of CGCC
- Performed and translated legal research on antitrust jurisdictions, export control, and duty-free zone controversies in the U.S.
- Coordinated 8 meetings for clients with agents such as mediation agencies and asset recovery personnel
- Represented the firm to attend Dept. of Commerce's Select USA Investment Summit to network with 80+ people from different state governments, bureaus, technology companies, and foreign investors

Ministry of Justice of P.R.C (Pro Bono Legal Aid Center) — Guangxi, China
Summer Volunteer, National Poverty-Stricken County Legal Aid Center in Tiandeng County — *May 2019 – August 2019*
- Assisted 2 aid lawyers on 5 cases preparation, including community correction, divorce and contract dispute, and labor ADR

LEADERSHIP EXPERIENCE

Phi Eta Sigma (ΦHΣ) Honor Society — University Park, PA
Treasurer, Executive Board — *May 2020 – Present*
- Manage 8 fiscal issues, such as collecting and refunding dues, reporting to the national chapter, and cooperating with the ASB

Zeta Beta Tau (ZBT) Fraternity — University Park, PA
Apparel Committee Chair & Alumni Relation Director, Alpha Psi (AΨ) Chapter at Penn State — *March 2019 – Present*
- Designed over 30 apparel and accessories from shirts to phone cases to brand ZBT across schools and communities
- Organized 2 seasons of homecoming events and over 10 philanthropy events with 2 sororities, THON partners, and alumni

Chinese Students and Scholars Association (CSSA) — University Park, PA
Vice Director, Public Relation Department (PR) — *February 2019 – Present*
- Sign and execute cumulatively over $50k ad. contracts with 20 midsize companies and maintain the relationship for 2 years
- Coordinate with 30 representatives in 8 departments to promote 2 Chinese galas via 3 social media platforms annually

SKILLS & INTERESTS

Languages: Mandarin (Native), English (Native), and Cantonese (Fluent)
Computer: R, Agile, Python, and Java; Proficient in Word, PowerPoint, Excel, Team; Adobe Ps, Ae, Pr; and Apple Keynote, FCP;
Interests: Multimedia Producing, Photography, Culinary Commentary, Football, Weightlifting, Game of "Go", Boxing, Dressage