Chicago-Kent Journal of Intellectual Property

Volume 20 | Issue 2 Article 1

8-26-2021

Protecting Data Privacy for Mobile Payments Under the Chinese Law: Comparative Perspectives and Reform Suggestions

Robin Hui Huang

Qiang Han

Xiuwen Zhu

Protecting Data Privacy for Mobile Payments under the Chinese Law: Comparative Perspectives and Reform Suggestions

BY ROBIN HUI HUANG*, QIANG HAN†, & XIUWEN ZHU‡

ABSTRACT

China has become one of the largest mobile payment markets in the world. While mobile payments bring great benefits such as convenience, flexibility, and efficiency, they are not without risks. This article focuses on one of the major risks, namely the data privacy risk, which is in large part caused and exacerbated by the involvement of multiple players and the extensive collection of personal information. There were some difficulties in protecting data privacy under the traditional legal framework, which was developed in a piecemeal manner with relevant provisions scattered around many different laws. In response, China has been trying to consolidate and modernise its regulatory regime for data privacy to suit the needs of the new digital era. Over the past few years, China has made great efforts to enact new laws and regulations to delineate the scope of personal information,

* Professor, Faculty of Law, Chinese University of Hong Kong; Adjunct Professor, University of New South Wales, Sydney, Australia; Li Kashing Visiting Professor, McGill law School, Montreal, Canada; Honorary Professor, East China University of Political Science and Law, Shanghai, China. This research project (Project Number: 14613219) is funded by the Hong Kong Research Grants Council's General Research Fund project, "The Regulation of Fintech in China." Thanks to Zhirong Gu and Warwick Wang Lik Chan for their excsellent research assistance.
† Professor, East China University of Political Science and Law.
‡ Faculty of Law, Chinese University of Hong Kong.

introduce the obligations for data controllers and processors, and incorporate the principles of the Fair Information Practices. However, there are some remaining concerns, including the ineffective requirements of consent and disclosure, the ambiguous principle of purpose limitation, and the limited applicability of the principle of data minimisation. In a quest for a more effective solution to meet the regulatory challenge and strike a proper balance between privacy protection and technological innovation, a comparative analysis is conducted with several other major jurisdictions in this area, including the United States, the European Union, Singapore and Hong Kong. This article proposes that China should 1) improve the requirements of consent and disclosure; 2) strengthen the application of the principles of purpose limitation and data minimization; 3) enact a specific law for data protection; 4) establish a unified law enforcement agency, and 5) enhance private and public enforcement.

Keywords: data privacy, data protection, mobile payment, China, comparative study

TABLE OF CONTENTS

1. INTRODUCTION

While there is no universal definition of mobile payments, they can be generally understood as payments "for which the payment data and the payment instruction are initiated, transmitted or confirmed via a mobile phone or device."[1] As a key component of Fintech, mobile payments offer a much more convenient means of payment than the traditional means, and can be classified into different types depending on the technologies used.[2] China's mobile payment industry has experienced explosive growth since 2013 and has played a significant role in the Chinese economy while increasing its influence in many overseas markets.

Mobile payments bring various benefits to consumers, such as flexibility, convenience, and a well-integrated purchase experience. It is also beneficial to merchants in terms of its lower cost of record-keeping and accounting, higher operational efficiency, and stronger digitising marketing capacity.[3] Nevertheless, mobile payments are not without risks.[4] First, mobile payments are plagued by data privacy and security risks. Data privacy issues concern primarily unauthorized processing of data for commercial purposes, such as targeted advertisements. The data may also leak out mainly through an illegal data transaction or as a cybersecurity issue. Mobile devices are susceptible to viruses, worms and other malicious applications that could illegally track, steal and misuse users' sensitive financial information and pose a grave threat to the safety of their funds. Secondly, mobile payment users could be exposed to the risk of deceptive commercial practices linked with inadequate or misleading disclosure. For example, consumers can be overcharged when the essential information about the actual cost of a

1. EUROPEAN COMMISSION, GREEN PAPER: TOWARDS AN INTEGRATED EUROPEAN MARKET FOR CARD, INTERNET AND MOBILE PAYMENTS 5 ((2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0941&from=EN (last visited June 13, 2021).

2. For a more detailed discussion of the typology of mobile payments in China, see Robin Hui Huang, et al., *The Development and Regulation of Mobile Payment: Chinese Experiences and Comparative Perspectives*, 20(1) WASH. U. GLOB. STUD. L. REV. 1 (forthcoming n.d.).

3. ASIA PACIFIC FOUNDATION OF CANADA (hereinafter "APFoC"), THE MOBILE PAYMENT REVOLUTION IN CHINA 4 (2019), https://www.asiapacific.ca/sites/default/files/publication-pdf/mobile_payment_report.pdf

4. For a comprehensive discussion of the risks of mobile payment in China, see HUANG ET AL., *supra* n. 2; OECD, REPORT ON CONSUMER PROTECTION IN ONLINE AND MOBILE PAYMENTS 22 (2012), https://www.oecd-ilibrary.org/docserver/5k9490gwp7f3-en.pdf?expires=1623728336&id=id&accname=guest&checksum=9BE6F1AC10DFEDAAA40E2CDD1E194E9D (last accessed June 14, 2021). ; ANDREW JAMES LAKE, RISK MANAGEMENT IN MOBILE MONEY: OBSERVED RISKS AND PROPOSED MITIGANTS FOR MOBILE MONEY OPERATORS (2013), https://www.ifc.org/wps/wcm/connect/e6ae6dd9-ad8c-4663-9c38-832c1d46a9f0/Tool+7.1.+Risk+Management.pdf?MOD=AJPERES&CVID=khAOg2B;

transaction is hidden in the terms and conditions of the transaction.[5] Thirdly, the liquidity risk of mobile payment may occur when a third-party payment service provider does not have sufficient liquid assets to meet its debts. Due to reasons such as space constraints, this paper will focus on the important issue of protecting data privacy.[6] Cybersecurity presents a big issue that would warrant the separate treatment of another full paper, but will be mentioned in this paper where necessary due to its close connection with the issue of data privacy.

The objective of this paper is to critically evaluate the efficiency of data privacy protection in the context of mobile payments in China and, based on this evaluation, to suggest improvements. Part 2 delineates the development of mobile payment in China and the privacy risks specific to the mobile payment business. Part 3 discusses China's regulatory framework for protecting data privacy, including its historical evolution and key elements of the current regime. Part 4 conducts a comparative study of relevant experiences from other jurisdictions, including the United States, the European Union, Singapore, and Hong Kong. Part 5 evaluates the Chinese regulatory regime from a comparative perspective, identifying its strengths and weaknesses, and makes relevant proposals for improvement. The last part concludes that despite the great improvement in the area of data privacy protection, China should 1) improve the requirements of consent and disclosure; 2) strengthen the application of the principles of purpose limitation and data minimization; 3) enact a specific law for data protection; 4) establish a unified law enforcement agency, and 5) enhance private and public enforcement..

2. MOBILE PAYMENT DEVELOPMENTS AND DATA PROTECTION ISSUES IN CHINA

2.1 Overview

The development of the mobile payment market in China has not been a smooth curve. Before 2010, telecommunication operators, commercial

5. OECD, REPORT ON CONSUMER PROTECTION IN ONLINE AND MOBILE PAYMENTS, 22 (2012), https://www.oecd-ilibrary.org/docserver/5k9490gwp7f3-en.pdf?expires=1623728336&id=id&accname=guest&checksum=9BE6F1AC10DFEDAAA40E2CDD1E194E9D (last accessed June 26, 2021)

6. On Nov. 2, 2020, Mr Gang Yi (易刚), the President of the Chinese central bank, People's Bank of China, attended a conference during the Hong Kong Fintech Week, stating that Fintech is a rule-changer in the financial markets and consumer privacy protection presents a huge challenge. SINA, *Yi Gang: Big technology companies are game changers in finance, consumer privacy protection is a great challenge*, 21ST CENTURY BUSINESS HERALD (Nov. 2, 2020, 2:37pm), https://finance.sina.com.cn/china/gncj/2020-11-02/doc-iiznezxr9459573.shtml.

banks, UnionPay (a Chinese bank payment association), and third-party payment service providers attempted to expand their market shares in mobile payments.[7] Nevertheless, the development of mobile payments at that time was limited by the lack of clear market regulations, the incompatibility of mobile payment technology standards, the low penetration rate of smart mobile devices, and poor mobile internet coverage.[8]

To better regulate the mobile payment market, the People's Bank of China ("PBOC"), China's central bank, issued "The Measures of Administration of Payment Services by Non-financial Institutions"[9] in 2010, defining the entry barrier for non-financial institutions to engage in mobile payment services.[10] In 2011, the PBOC issued the first batch of licences to twenty-seven third-party payment service providers.[11] The two giant payment service providers, Alipay and WeChat Pay, which were among the first group of licensed third-party mobile payment service providers, started to provide cheap payment services allowing merchants to make use of a simple printout of a QR code rather than an expensive card reader.[12] At the same time, the rapid growth of the Online-To-Offline market in ride-hailing and food delivery created abundant small-ticket payment scenarios and further advanced the wide application of mobile payments.[13]

Against this backdrop, China's mobile payment market has skyrocketed since2013. By the end of June 2018, China had roughly 890 million mobile payment users, and 2018's total value of mobile payment transactions reached 277.39 trillion yuan.[14]

7. Guojia xinxi zhongxin (国家信息中心) [St. Info. Ctr.], "Zhongguo yidong zhifu fazhan baogao" (中国移动支付发展报告) [CHINA MOBILE PAYMENT Dev. REP.] (2019), http://upload.xinhua08.com/2019/0508/1557302957552.pdf.

8. APFOC, *supra* Note 2, at 9.

9. PEOPLE'S BANK OF CHINA, "Feijinrong jigou zhifu fuwu guanli banfa" (非金融机**构**支付服务管理办法) [THE MEASURES OF ADMIN. of Payment Servs. by NON-FIN. INSTS.] (, June 14, 2010) (effective September 1, 2010), http://www.gov.cn/flfg/2010-06/21/content_1632796.htm (last accessed June 15, 2021).

10. *Id.*, Articles 8-10; APFOC, *supra* note 2, at 9.

11. APFOC, *supra* note 2, at 9.

12. *Id.*

13. APFOC, *supra* note 2, AT 9–10.;.

14. Guojia, *supra* note 6, at 8.

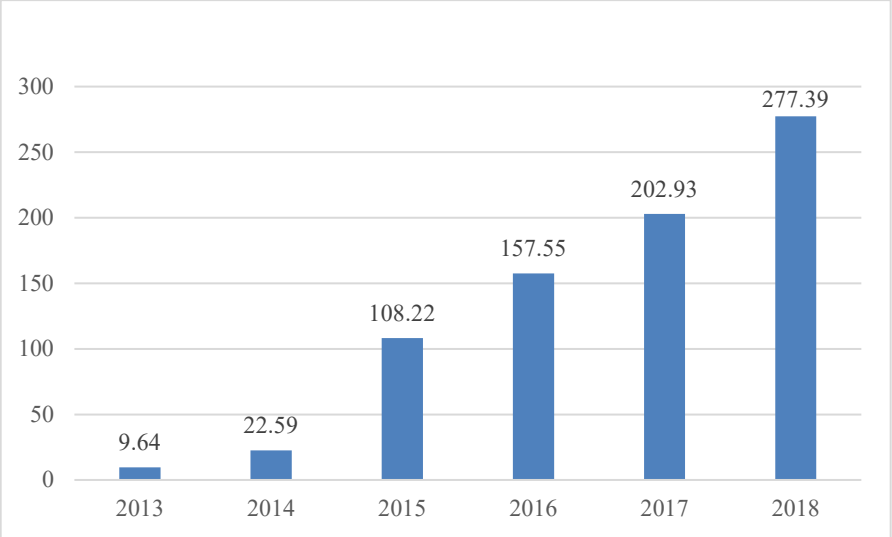

Figure 1: Total Value of Mobile Payment Transaction Processed by Banking Institutions in China, 2013-2018 (trillion yuan)
Source: State Information Centre, "China Mobile Payment Development Report" (2019).[15]

While mobile payments bring significant benefits to society, they are not without risks. In 2018, the Jiangsu Provincial Committee for the Protection of Consumers' Rights and Interests filed an action on behalf of consumers against Beijing Baidu Netcom Science Technology Co. Ltd on the basis that the mobile applications breached the users' data privacy.[16] The committee believed that the two mobile applications developed by Baidu, "Mobile Baidu" and "Baidu Browser" hoovered up various types of personal information, including sensitive information such as users' location, their MMS messages and contact lists, from users without informing them of the privacy policy or obtaining their consent. [17] Later on, Baidu approached the committee and offered to rectify the privacy issues of their mobile applications.[18]

15. *Id.*
16. SINA, *Baidu was sued for breach of privacy right* (Jan. 06, 2018, 01:20 am), http://tech.sina.com.cn/roll/2018-01-06/doc-ifyqiwuw7106698.shtml.
17. *Id.*
18. THE PAPER, Jiangsu Consumer Protection Commission withdrew the lawsuit against Baidu for breaching of consumer privacy: APP rectification and reform in place (Mar. 13, 2018, 10:28 am), https://www.thepaper.cn/newsDetail_forward_2028107.

The Security Research Institute of China Academy of Information and Communications, an affiliate of the Ministry of Industry and Information Technology (MIIT), investigated more than 200 mobile applications in 2019 and found a massive prevalence of data privacy issues – 67% of mobile applications in the market contain no less than 5 data privacy risks, and 18.5% of the mobile applications in the market carry at least 10 data privacy risks.[19] Resulting problems include non-transparent data privacy policies, unauthorised collection and sharing of personal information, and extensive harvesting of personal information.[20] Some mobile applications offering financial services collect more than 14 types of personal information, which far exceeds the scope of data collection necessary to provide services.[21] These problems could cause identity theft, cyber fraud, price discrimination, target advertising, and pervasive monitoring.[22] In summary, China must urgently address how to protect data privacy for mobile payments.

2.2 Factors behind the Heightened Privacy Risk

The following section will discuss the main factors that contribute to the data privacy risk faced by the mobile payment users. Particularly, the new and heightened privacy risks are mostly caused by the involvement of multiple players and their extensive collection of personal information used in the course of mobile payments.

2.2.1 More Players in Mobile Payments

First, there are more players involved in mobile payments than in traditional payment services. In general, the players of traditional payments include banks (including, in the case of card payments, the issuing bank, which provides the card to the consumer, and the acquiring bank, which is used by the merchant or seller) and payment processors who process payments by acting on behalf of acquiring or issuing banks.[23] Customers can use their individual bank accounts through electronic channels by swiping their cards, which usually involves "account-based electronic payment

19. Zhongguo xinxi tongxin yanjiuyuan anquan yanjiusuo (中国信息通信研究院安全研究所) [SEC.RES. INST. CHINA ACAD. OF INFO. COMMC'NS.], "Yidong yingyong shuju anquan yu geren xinxi baohu baipishu" (移动应用数据安全与个人信息保护白皮书) [WHITE PAPER ON MOBILE APPLICATION DATA SECURITY AND PERSONAL INFORMATION PROTECTION] 10 (December, 2019), http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191230332039577332.pdf.

20. *Id.*

21. *Id.* at 14.

22. *Id.*

23. OECD, *supra* note 5, at 9.

services".[24] There is only one simple and direct contractual relationship between licensed banks and customers under the traditional bank payment system.

By comparison, mobile payments use mobile devices instead of physical plastic cards in a transaction, and thus many more actors are involved, including "consumer facing" actors and "behind the scenes" actors.[25] In addition to banks and payment processors, mobile payment services often involve new actors such as mobile payment service providers, mobile application developers, data analytics companies, e-commerce platform operators, hardware manufacturers, and mobile network operators.[26] For example, in the case of the mobile payment platform, the mobile payment platform will act as a middleman to transfer money from the customer's account to the merchant's account provided that both sides have registered their bank cards in the platform.[27] From a legal perspective, there could be two separate contractual relationships, one between customers and mobile payment service providers,[28] , the other between banks and the mobile payment service providers. With so many parties involved in processing mobile payments, the risk of data leakage and abuse becomes significantly higher.

2.2.2 More Extensive Collection of Data

The privacy risk is further amplified by the extensive collection of personal data. In a typical credit card transaction, the parties to the transaction have a limited understanding of the sales.[29] Merchants may know the names of customers and the products that the customers purchase.[30]The traditional payment networks receive limited information from transactions, such as the account numbers, the amounts of fees and the identities of

24. Khiaonarong Tanai, *Oversight Issues in Mobile Payments* 6 (Int'l Monetary Fund, Working Paper No. 14, 123).

25. Edith Ramirez, *Opening Remarks at FTC Privacy Conference* (2017), FTC PRIVACY CONFERENCE 2–3, https://www.ftc.gov/system/files/documents/public_statements/1049653/ramirez_-_privacycon_remarks_1-12-17.pdf.

26. OECD, CONSUMER POLICY GUIDANCE ON MOBILE AND ONLINE PAYMENTS 10 (2014), https://www.caa.go.jp/policies/policy/consumer_policy/international_affairs/pdf/150415adjustments_2.pdf.

27. YONG WANG, CHRISTEN HAHN AND KRUTTIKA SUTRAVE, "MOBILE PAYMENT SECURITY, THREATS, AND CHALLENGES" 3, https://par.nsf.gov/servlets/purl/10042755.

28. Congdon Stephen, *What's in Your Wallet: Addressing the Regulatory Grey Area Surrounding Mobile Payments*, 7 CASE W. RES. J.L. TECH. & INTERNET 95, 99 (2016).

29. CHRIS JAY HOOFNAGLE, JENNIFER M URBAN, AND SU LI, MOBILE PAYMENTS: CONSUMER BENEFITS & NEW PRIVACY CONCERNS 5 (April 24, 2012), https://ssrn.com/abstract=2045580.

30. *Id.* at 5-6.

merchants.[31] The banks usually only receive information on the total amount of purchases and the places of purchase. The issuing banks will also know the identities of consumers.[32]

However, the nature of mobile devices makes mobile payment users susceptible to data harvesting;as mobile devices contain multiple sensors (such as cameras, microphones, movement sensors, GPS, and Wi-Fi capabilities), they can generate various sensitive personal data, such as facial images, voices, and information of geographical locations.[33] Mobile devices can also be "physically tracked via their wireless interfaces by third-parties" or "tracked by third-parties on the Internet,"[34] and data brokers could easily track our IP address, location, behavioural habits, purchase habits, and other online activities. Moreover, as mobile devices are always turned on, connected to the internet and carried around by the users, it means that data brokers could continuously and pervasively monitor users.[35]

Extensive data harvesting is one of the key defining features of Big Data, a powerful technique "that aids in the collection and mathematical analysis of data, using traditional statistical methods as well as more innovative analytical tools."[36] Many internet companies, such as Google, Facebook, and Amazon, have monetised Big Data. They harvest large amounts of personal data, exploiting them for target advertising and training "its search algorithms, and develop new data-intensive services such as voice recognition, translation, and location-based services."[37] These services can generate new revenue.[38] Big Data also intensifies the issue of profiling.[39] For instance, it allows advertisers to use the information to create detailed profiles of individual consumers and direct tailored advertisements to consumers based on the data collected.[40]

31. *Id.* at 6.

32. *Id*.

33. EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), PRIVACY AND DATA PROTECTION IN MOBILE APPLICATIONS: A STUDY ON THE APP DEVELOPMENT ECOSYSTEM AND THE TECHNICAL IMPLEMENTATION OF GDPR 11 (2017).

34. *Id.* at 12.

35. *Id.* at 11.

36. Viktor Mayer-Schonberger & Yann Padova, *Regime Change: Enabling Big Data through Europe's New Data Protection Regulation*, 17 COLUMBIA SCI. & TECH. L. REV. 315, 318 (2016); as to the feature of Big Data, see Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?,* 3(2) INT'L DATA PRIV. L., 74, 77 (2013).

37. Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3(2) INT'L DATA PRIV. L., 74, 76 (2013). .

38. *Id.* at 76.

39. *Id.* at 77.

40. CHARLES GIBNEY, et al., INTERNATIONAL REVIEW: MOBILE PAYMENTS AND CONSUMER PROTECTION iv (2015), https://www.canada.ca/content/dam/canada/financial-consumer-

Although providing consumers with advertisements customised to their taste and preference, profiling has caused a series of significant problems. First, data profiling often takes the form of "pervasive and non-transparent commercial observation" of consumer online behaviour.[41] Profiling directly interferes with consumers' rights to personal data protection, such as the right to notice and right to give consent before data collection[42]

Second, by aggregating discrete or de-identified data sets, data profiling can generate personally identifiable information that is ultimately linked to individual users.[43] One possibility is that profiling can "generate a predictive model of what has a high probability of being [personally identifiable information]."[44] For example, in 2012, a New York Times articlecriticised Target for using data mining techniques to analyse their customers' purchase history and to predict which female customers were pregnant.[45] After inferential analysis, Target disclosed the relevant information to marketers who then directed relevant advertisements to those pregnant women.[46] The data analytics thus resulted in the unauthorised disclosure of sensitive personal information and the direct invasion of consumers' privacy.[47]

Third, by aggregating data of consumers' purchase histories, profiling enables merchants to use unfair commercial practices, such as price discrimination between different groups of consumers.[48]

Fourth, target advertising may infringe consumers' liberty and autonomy as marketers may likely manipulate the consumers unaware of the profiling activities.[49] This risk acutely affects vulnerable people targeted by promotions of unhealthy food, medication, or high-interest consumer loans.[50] Profiling can even be used in politics to manipulate voters. In March 2018, Cambridge Analytica collected data from more than 50 million Facebook users without their consent to build their profiles and tailor

agency/migration/eng/resources/researchsurveys/documents/internationalreviewmobilepaymentsandconsumerprotection.pdf.

41. NJ King and P.W. Jessen, *Profiling the Mobile Customer – Privacy Concerns When Behavioural Advertisers Target Mobile Phones Part I*" 26 COMP. L. & SEC.REV. 455, 459 (2010).

42. *Id.* at 459.

43. Paul Schwartz and Dan Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. REV. 1814, 1841-42 (2001).

44. Kate Crawford and Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms* 55 BOSTON COLLEGE L. REV. 93, 98 (2014).

45. Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, February 19, 2012.

46. *Id.*

47. *Id.*

48. King & Jessen, *supra* note 29, at 459.

49. Karen Yeung, *Five Fears About Mass Predictive Personalization in An Age of Surveillance Capitalism* 8(3) INT'L DATA PROT. L. 258, 262–63 (2018).

50. King & Jessen, *supra* note 29, at 461.; for a comprehensive discussion, see Ryan Calo, *Digital Market Manipulation* 82 GEORGE WASHINGTON L. REV. 996 (2014).

political advertisements to potential voters so as to influence their voting.[51] This infringement quickly aroused worldwide outrage.[52] The FTC eventually settled with Facebook and imposed a record-breaking US$5 billion penalty on Facebook.[53]

In summary, the data-driven economy incentivises extensive data harvesting and relentless data profiling against mobile payment consumers. Balancing the need to protect consumer privacy with supporting financial and technological innovation has become extremely challenging.

3. CHINA'S REGULATORY FRAMEWORK OF DATA PROTECTION

3.1 The Historical Progression

In China, data privacy of mobile payments generally is regulated under a broad framework of data protection. This framework has undergone a structural evolution from a traditional and piecemeal approach to a principle-based approach by consolidating the fragmented data protection-related provisions and systematising the data protection regime.

3.1.1 Before 2016: A Traditional and Piecemeal Approach

Before 2016, there was no general data protection law but traces of data protection could be found in different laws. The Constitution of the People's Republic of China makes reference to privacy once, stating that citizens' private correspondence is protected, and no organisation or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence, except in cases to meet the needs of the state security or of the investigation into criminal offences, public security and so forth.[54] Article 38 also states that citizens' personal dignity is inviolable.[55] However,

51. Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*", N.Y. TIMES, March 17 2018.

52. The Federal Trade Commission (FTC) filed a complaint against Facebook, alleging that Facebook violated the FTC's 2012 order by misrepresenting the control that the users had over their personal information, failing to institute and maintain a reasonable program to ensure consumers' privacy, and deceptively failing to disclose that it would use the users' phone numbers for target advertising, see U.S. v. Facebook, 456 F. Supp. 3d 115 (D.D.C. 2020).

53. FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

54. Zhonghua renmin gongheguo xianfa (中华人民共和国宪法) [Constitution of the People's Republic of China] (promulgated by the National People's Congress on 4 December 1982, effective from 4 December 1982; amended in 1988, 1993, 1999, 2004 and 2018) (hereinafter *China Constitution*), Article 40.

55. *China Constitution*, Article 38.

these constitutional rights may not directly relate to data protection since they cannot directly serve as the legal ground for a judicial decision.[56]

China's civil and criminal laws protect individuals' right to privacy. The Tort Liability Law of the People's Republic of China[57] ("Tort Liability Law"), which came into effect in July 2010, recognises the right to privacy as an independent civil right.[58] Article 36 protects individuals' civil rights and interests from online infringement.[59] Individuals thus have a cause of action in tort against tortfeasors if their right to privacy is infringed. The Ninth adopted version of Amendments to the Criminal Law of the People's Republic of China (Criminal Law) contains several important severe prohibitions relating to data protection.[60] It imposes severe punishment for the illegal activities of (i) selling or providing citizens' personal information to third parties, and (ii) selling or providing to third parties citizens' personal information obtained during the course of performing duties or providing services.[61] Network service providers may face criminal liability if they fail to fulfill "information network security administration duties prescribed by laws or administrative regulations" or take remedial action.[62]

In December 2012, the Standing Committee of the National People's Congress (NPCSC) promulgated "The Decision on Strengthening Online Information Protection" (2012 NPSCS Decision).[63] 2012 NPSCS Decision sets out several basic principles on data protection and acts as the primary baseline for the subsequent privacy regulation in China.[64] Article 2 specifies that network service providers shall "abide by the principles of legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain consent from the person

56. Tong Zhiwei, *A comment on the rise and fall of the Supreme People's Court's reply to Qi Yuling's case* 43 SUFFOLK *U. L. Rev.* 669, 677–78 (2010) (pointing out that "China is a state of statutory laws and any provision of constitutional rights must be implemented through laws made by legislative bodies; otherwise, the constitutionally recognized rights cannot be practically protected.")

57. Zhonghua renmin gongheguo qinquan zerenfa (中华人民共和国侵权责任法) [Tort Liability Law of the People's Republic of China] (promulgated by the Standing Committee of the National People's Congress on 26 December 2009, effective from 1 July 2010) (hereinafter *Tort Liability Law*).

58. *Tort Liability Law*, Article 2.

59. *Tort Liability Law*, Article 36.

60. Zhonghua Renmin Gongheguo Xingfa Xiuzhengan (9) (中华人民共和国刑法修正案九) [The Ninth Amendment to the Criminal Law of the PRC] (promulgated by the Standing Committee of the National People's Congress on 29 August 2015, effective from 1 November 2015) (hereinafter *Criminal Law*).

61. *Criminal Law*, Article 17.

62. *Criminal Law*, Article 28.

63. "Guanyu jiaqiang wangluo xinxi baohu de guiding" (关于加强网络信息保护的决定) [The Decision on Strengthening Online Information Protection] (promulgated by the NPSCS on 28 December 2012, effective from 28 December 2012) (hereinafter 2012 *NPSCS Decision*).

64. GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE & HUMAN RIGHTS PERSPECTIVES 204 (Oxford University Press, 2014).

whose data is collected."[65] Following this decision, China continuously develops the regime of personal data protection by making and amending laws and regulations in various economic sectors.[66]

In addition to the general laws, the PBOC paid close attention to the issue of data privacy in the financial industry. In 2011, the PBOC issued a circular to the banking industry on the issue of protecting personal financial information.[67] This circular laid down a foundation for the PBOC's future regulation of data privacy protection. For example, the circular requires that banks must establish internal control systems to ensure the confidentiality of personal financial information, and banks should not collect information irrelevant to their service.[68] In March 2012, the PBOC issued another circular requiring banks to strengthen the protection of data privacy in accordance with laws and regulations.[69]

The above circulars were only applicable to banks. In December 2015, the PBOC issued another regulation to rein in the rapid growth of mobile payments.[70] First, non-bank payment institutions must establish an internal data management and risk control system.[71] Second, the payment institutions must not store certain sensitive information, such as magnetic track information and chip information of bank cards, account passwords, and card verification codes.[72] Third, without consent of clients and banks, payment institutions must not store the expiration date of bank cards.[73] They also must not provide other organisations with clients' information unless otherwise authorised by law or approved by the clients.[74] Last but not least, they should

65. *2012 NPSCS Decision*, Article 2.

66. China also updated the Law on the Protection of Consumer Rights and Interests (Consumer Protection Law) in 2013: Zhonghua renmin gongheguo xiaofeizhe quanyibaohufa (中华人民共和国消费者权益保护法) [Consumer Rights Protection Law of the People's Republic of China] (promulgated by the NPCSC on 31 October 1993, effective from 1 January 1994; amended in 2009 and 2013).

67. Guanyu yinhangye jinrong jigou zuohao geren jinrong xinxi baohu gongzuo de tongzhi" (**关**于银行业金融机**构**做好个人金融信息保护工作的通知) [Circular of the People's Bank of China on the Protection of personal Financial Information by Bank and Financial Institutions] (issued by the People's Bank of China on 21 January 2011, effective from 1 May 2011).

68. *Id.*

69. Guanyu yinhangye jinrong jigou jinyibu zuohao geren jinrong xinxi baohu gongzuo de tongzhi (**关**于银行业金融机**构**进一步做好个人金融信息保护工作的通知) [Circular of the People's Bank of China on the Further Protection of personal Financial Information by Bank and Financial Institutions] (issued by the People's Bank of China on 27 March 2012, effective from 27 March 2012).

70. "Feiyinhang Zhifu Jigou Wangluo zhifu yewu guanli banfa" (非银行支付机构网络支付业务管理办法) [The Management Measures of the Mobile Payment Business of the Non-bank Payment Institutions] (issued by the People's Bank of China on 28 December 2015, effective from 28 December 2015) (hereinafter *Mgmt. Measures*).

71. *Mgmt. Measures*, Article 20.

72. *Mgmt. Measures*, Article 20.

73. *Mgmt. Measures*, Article 20.

74. *Mgmt. Measures*, Article 20.

comply with the principles of minimisation when collecting and processing the clients' information and should also inform clients of the scope and purpose of data collection and processing.[75]

3.1.2 After 2016: A Comprehensive and Proactive Regime

The Cybersecurity Law of the People's Republic of China (Cybersecurity Law), enacted in November 2016, is thus far the most important and comprehensive law relating to data protection.[76] Although the major purpose of this law is to reduce the risk of cyberattacks and safeguard national security, it reiterates the basic requirements in the 2012 NPSCS Decision, articulates a set of data protection principles, specifies the data subject's rights, and stipulates penalties for violations of the law.[77]

The Cybersecurity Law is accompanied by the Personal Information Security Specification (2018 SAMR Specification (2020 Revision)), a comprehensive guide setting out the compliance requirements of data protection.[78] The 2018 SAMR Specification (2020 Revision) is a nationally recommended standard. Under Article 2 of the Standardisation Law of the People's Republic of China, the national standards are divided into mandatory standards and recommended standards; while mandatory standards must be implemented, recommended standards are simply recommended for implementation.[79] As such, the 2018 SAMR Specification (2020 Revision) is not mandatory. However, it can act as a regulatory baseline for judicial and law enforcement authorities as well as companies to determine compliance with the requirements of data protection.[80] In addition, we believe that it may reflect the direction of future legislation on data protection.

Following the enactment of the Cybersecurity Law, the PBOC issued an implementing rule for the financial industry, titled "Measures for the

75. *Mgmt. Measures*, Article 20.

76. Zhonghua renmin gongheguo wangluo anquan fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the NPCSC on 7 November 2016, effective from 1 June 2017) (hereinafter *Cybersecurity Law*).

77. *Cybersecurity Law*, Article 41.

78. Xinxi anquan jishu – Geren xinxi anquan guifan (信息安全技术 —— 个人信息安全规范) [Information Security Technology – Personal Information Security Specification] (issued by State Administration of Market Supervision and Administration and National Standardisation Management Committee on 29 December 2017, effective from 1 May 2018; amended in 2019 and 2020) (hereinafter *2018 SAMR Specification (2020 Revision)*).

79. Zhonghua renmin gongheguo biaozhunhua fa (中华人民共和国标准化法) [Standardisation Law of the People's Republic of China] (promulgated by the NPCSC on 29 December 1988, effective from 1 April 1989; amended in 2017), Article 2.

80. *2018 SAMR Specification (2020 Revision)*, Section 1.

Protection of the Rights and Interests of Financial Consumers".[81] It imposes the obligations of data privacy protection on financial institutions. According to Article 2, financial institutions include banks and other financial institutions providing cross-market and cross-industry financial products and services, as well as non-bank payment institutions.[82] Chapter 3, on data privacy protection, defines "personal financial information" as "the personal information obtained, processed and preserved by financial institutions in the course of ordinary business or through other channels, which includes the information of personal identity, asset, account, credit, transaction and other information that can reflect certain situations of individuals."[83] It reiterates the key principles for data protection laid out in the Cybersecurity Law. For instance, Article 28 states that when collecting personal financial information, financial institutions shall follow the principles of legality, reasonableness and necessity, collect personal financial information in accordance with the requirements of laws and regulations and business needs, and not collect information which is irrelevant to business, collect information in an improper manner, or illegally store personal financial information.[84]

In line with the 2018 SAMR Specification (2020 Revision), the PBOC issued "Personal Financial Information Protection Technical Specification" (2020 PBOC Specification) in February 2020.[85] Similar to the role of the 2018 SAMR Specification (2020 Revision), the 2020 PBOC Specification sets out the best practice for data privacy protection. It classifies personal financial information and sets forth various requirements governing the different categories of the data. As the 2020 PBOC Specification basically incorporates the framework of the 2018 SAMR Specification (2020 Revision), the 2020 PBOC Specification will be discussed only to the extent necessary to avoid repetition.

In September 2020, the PBOC also updated "Measures for the Protection of the Rights and Interests of Financial Consumers" in accordance

81. Zhongguo renmin yinhang jinrong xiaofeizhe quanyi baohu shishi banfa (中国人民银行金融消费者权益保护实施办法) [Measures of the People's Bank of China for the Protection of the Rights and Interests of Financial Consumers] (issued by the People's Bank of China on 14 December 2016, effective from 14 December 2016) (hereinafter *PBC Protection*).

82. *PBC Protection*, Article 2.

83. *PBC Protection*, Article 27.

84. *PBC Protection*, Article 28.

85. Geren jinrong xinxi baohu jishu guifan (个人金融信息保护技术规范) [Personal Financial Information Protection Technical Specification] (issued by the People's Bank of China on 13 February 2020).

with the Cybersecurity Law and the 2020 PBOC Specification.[86] It adds the requirements of disclosure, data breach notification and data classification.

In addition to the various rule-making efforts, the PBOC also endeavoured to improve the financial infrastructure to provide adequate technical support for data protection. In 2017, the PBOC instructed the Payment and Clearing Association of China to establish a unified payment clearing platform for non-bank payment institutions.[87] By doing so, the PBOC can monitor information on mobile payment transactions, regulate relevant financial activities, and deal with the risks of money-laundering.

3.2 Main Elements of Current Regulatory Regime

3.2.1 Concept of Personal Information

In general, there are two groups of payment data collected and processed in mobile payments: Essential payment data and ancillary data.[88] Essential payment data includes payer personal, account, and transaction data.[89]

Therefore, the starting point of considering China's current regulatory regime in the area of mobile payment is the concept of personal information. In other words, the first question is which kinds of personal information are protected under the regulatory regime. The 2018 SAMR Specification (2020 Revision) expressly expands the scope of personal information, referring to "any information that is recorded, electronically or otherwise, can be used solely or in combination with other information to identify the identity of a natural person or reflect the activities of a natural person."[90] Arguably, this definition may extend to cover "the information that may reflect a specific person (without necessarily identifying them)."[91] If this is the case, the 2018

86. Zhongguo renmin yinhang jinrong xiaofeizhe quanyi baohu shishi banfa" (中国人民银行金融消费者权益保护实施办法) [Measures for the Protection of the Rights and Interests of Financial Consumers of the People's Bank of China] (issued by the People's Bank of China on 15 September 2020, effective from 1 November 2020).

87. "Zhongguo renmin yinhang zhifujiesuan si guanyu jiang feiyinhang zhifu jigou wangluo zhifu yewu you zhilian moshi qianyi zhi wanglian pingtai chuli de tongzhi" 中国人民银行支付结算司关于将非银行支付机构网络支付业务由直连模式迁移至网联平台处理的通知 [Notice on Migrating the Online Payment Business of Non-bank Payment Institutions from Direct Connection Mode to Network Platform Processing] (issued by the People's Bank of China on 4 Aug 2017).

88. PAYMENT SYSTEM REGULATOR (UK), DATA IN THE PAYMENTS INDUSTRY 17 (2018), https://www.psr.org.uk/publications/consultations/discussion-paper-data-in-the-payments-industry/ (last visited June 15, 2021).

89. *Id.*

90. *2018 SAMR Specification (2020 Revision)*, Section 3.1.

91. Greenleaf Graham and Livingston Scott, *China's Personal Information Standard: The Long March to a Privacy Law*, 150 PRIV. L. & BUS. Int'l REP. 25, 26 (2017).

SAMR Specification (2020 Revision) would apply not only to the personally identifiable information but also to information "which gives an organisation the capacity to interact with a person on an individuated basis (such as behavioural target marketing using data) which does not enable the [data controller] to identify the data subject."[92]

The 2020 PBOC Specification applies to the personal financial information, which is defined as "personal information collected, processed and stored through the financial products and services by the financial institutions."[93] This essentially incorporates the concept of personal information set out in the 2018 SAMR Specification (2020 Revision). Additionally, the 2020 PBOC Specification grades the personal financial information into three categories, namely C1, C2 and C3, according to the nature and level of sensitivity of the information.

The 2018 SAMR Specification (2020 Revision) distinguishes general personal data from sensitive personal data. Sensitive personal data is defined as "personal data that, if disclosed or illegally processed, might endanger personal and property security, damage personal reputation, or physical or psychological health, or lead to discriminatory treatment and so forth."[94] In this respect, C2 and C3 fall within the category of sensitive personal data. Accordingly, the enhanced protective mechanisms for sensitive information under the 2018 SAMR Specification (2020 Revision) should also be applied, such as explicit consent from data subjects before collection,[95] encryption storage and transmission of sensitive information,[96] and special controls of accessing sensitive information.[97]

3.2.2 Data Controllers and Data Processors

As discussed above, the 2020 PBOC Specification imposes upon financial institutions the obligations of protecting data privacy and cybersecurity. The term "financial industry institutions (jin rong ye ji gou)" refers to licensed financial institutions regulated by the authorities and the relevant institutions involved in the processing of personal financial information.[98] The licensed financial institutions include banks, non-bank payment institutions, and licensed financial service companies. The relevant

92. *Id.*
93. *2020 PBOC Specification*, Section 3.2
94. *2018 SAMR Specification (2020 Revision)*, Section 3.2.
95. *2018 SAMR Specification (2020 Revision)*, Section 5.4(b).
96. *2018 SAMR Specification (2020 Revision)*, Section 6.3(a).
97. *2018 SAMR Specification (2020 Revision)*, Section 7.1(e).
98. *2020 PBOC Specification*, Section 3.1

institutions involved in the processing of financial information may include telecommunication service providers, information technology providers and marketing service providers. In fact, these entities, according to the 2018 SAMR Specification (2020 Revision) which will be discussed below, can be categorised into two types: data controllers and data processors.

The Cybersecurity Law imposes upon the network operators the legal responsibility for complying with the respective data protection obligations. Network operators refer to the owners and administrators of networks as well as network service providers.[99] This loosely-defined term would encompass almost all the business that owns or administrates networks. The 2018 SAMR Specification (2020 Revision) provides a more specific concept "data controller." Data controller means "any organization or person that has the power to decide the purpose and method of processing personal information."[100] It is the data controller that has the obligation to comply with the respective requirements. In light of the increasingly important role of the data outsourcing services, the 2018 SAMR Specification (2020 Revision) also makes a distinction between a data controller and a third-party data processor. The delegation of data processing by the data controller to the data processor should be within the data subject's authorisation.[101] The data processor should strictly follow the data controller's instructions.[102]

In the context of mobile payment, a merchant can be seen as a data controller of the purchase data that he processes for a sales agreement.[103] A bank is also a data controller of its customers' financial information.[104] A payment processor is likely to be a processor as it operates on behalf of the issuing or acquiring bank to evaluate whether transactions are valid. A mobile payment application developer can act in both capacities. It can be a processor if the mobile application is developed at the request and on behalf of a bank or financial institution to facilitate contactless payments.[105] On the other hand, if the developer retains access to personal data to provide additional services, such as tailored advertisements, it qualifies as a controller as well.[106] Both e-commerce platform providers and mobile payment service providers are, by definition, data controllers, and a third-

99. *Cybersecurity Law*, Article 76(3).

100. *2018 SAMR Specification (2020 Revision)*, Section 3.4.

101. *2018 SAMR Specification (2020 Revision)*, Section 9.1(a).

102. *2018 SAMR Specification (2020 Revision)*, Section 9.1(c).

103. SIMONT BRAUN, "MOBILE WALLETS AND MOBILE CONTACTLESS PAYMENTS – A CLOSER LOOK AT DATA PROTECTION", https://www.simontbraun.eu/images/pdf/News/NFC_News_II_versie_21mei_2015_2_2.pdf

104. *Id.*

105. *Id.*

106. *Id.*

party service provider for authentication of users or personalised advertisement is a data processor dealing with data on behalf of the data controller. Therefore, in mobile payments, data controllers may include merchants, banks and non-bank payment service providers, mobile payment application developers and e-commerce platform providers. Data processors may include payment processors, mobile payment application developers, third-party service providers.

Before engaging a third party as the data processor, the data controller should carry out a personal information security impact assessment, ensuring that the data processor has sufficient data security capabilities and provides sufficient security safeguards.[107] The data controller should also supervise the data processor and record the processor's activities.[108] In addition to the general requirements, the financial institutions are not allowed to authorise a non-financial institution to collect C2 or C3-level personal financial information.[109] They may not authorise a third-party to process any C2 or C3-level personal financial information that supports user authentication (e.g. one-time password or a SMS code).[110] The information to be outsourced should be de-identified.[111] The data processor has a number of direct obligations, including strictly following the data controller's instructions, obtaining its authorisation before engaging a sub-processor and deleting all personal data at the end of the engagement.[112]

3.2.3 Principles of Fair Information Practices

The fundamental principles of data protection under the Cybersecurity Law and the 2018 SAMR Specification (2020 Revision) are based on the Fair Information Practices (FIPs). The 2020 PBOC Specification reiterates these principles. The FIPs originated from a 1973 report by the United States Department of Health, Education, and Welfare, and it became extremely influential in shaping privacy law in the United States and around the world.[113] The Cybersecurity Law incorporated several key principles of the FIPs, including the principles of lawfulness, fairness and transparency, integrity and confidentiality, data minimisation and data subjects'

107. *2018 SAMR Specification (2020 Revision)*, Section 9.1(b).
108. *2018 SAMR Specification (2020 Revision)*, Section 9.1(d).
109. *2020 PBOC Specification*, Section 6.1.1(a).
110. *2020 PBOC Specification*, Section 6.1.4.4 (b).
111. *2020 PBOC Specification*, Section 6.1.4.4 (c).
112. *2018 SAMR Specification (2020 Revision)*, Section 9.1(c).
113. For a history of the FIPs, see, ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (October 7, 2019), https://ssrn.com/abstract=2415020; Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* 126 HARVARD L. REV. 1966 (2013).

participation. The 2018 SAMR Specification (2020 Revision) further introduces the principles of purpose limitation, accuracy, and storage limitation.

The Cybersecurity Law states that the network operators should abide by the principles of lawfulness, fairness, and necessity.[114] Under the 2018 SAMR Specification (2020 Revision), the principle of lawfulness means that data controllers shall not deceive, trick, or coerce data subjects to provide personal information, or conceal the data collection functions of their products or services, or obtain data from illegal channels.[115] The principle of necessity is closely connected with the principle of data minimisation. Under the Cybersecurity Law, "network operators must not collect personal information unrelated to the services they provide."[116] The 2018 SAMR Specification (2020 Revision) modifies this with a stricter approach, requiring that "the type of personal information collected should be directly related to the business function of the product or service; it means that the function of the product or service cannot be realized without the participation of the above personal information."[117] In addition, "the frequency of automatic collection of personal information should be the minimum frequency necessary to realize the business function of the product or service,"[118] and "the amount of indirect acquisition of personal information should be the minimum necessary to realize the business function of the product or service."[119]

Furthermore, the Cybersecurity Law requires network operators to "make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is gathered."[120] This principle of transparency aims to keep data subjects informed about how their data are being used and offset the asymmetry of information between the data controllers and data subjects. The 2018 SAMR Specification (2020 Revision) further requires that the scope, purposes, and rules of data processing should be open to the public in an explicit, intelligible, reasonable and accessible manner.[121] The 2018 SAMR Specification (2020 Revision) also spreads out the particular consent requirements. It prohibits the seeking

114. *Cybersecurity Law*, Article 41.
115. *2018 SAMR Specification (2020 Revision)*, Section 5.1.
116. *Cybersecurity Law*, Article 41.
117. *2018 SAMR Specification (2020 Revision)*, Section 5.2(a).
118. *2018 SAMR Specification (2020 Revision)*, Section 5.2(b).
119. *2018 SAMR Specification (2020 Revision)*, Section 5.2(c).
120. *Cybersecurity Law*, Article 41.
121. *2018 SAMR Specification (2020 Revision)*, Sections 5.5(b)-(d).

of bundle consent and forced consent.[122] An individual's express consent through opt-in or other affirmative action is required to collect sensitive personal data, and such consent must be fully informed and involve a clear and definitive expression of intent.[123]

The Cybersecurity Law does not contain the principle of purpose limitation. The 2018 SAMR Specification (2020 Revision) introduces this principle, stipulating that "the use of personal information should not exceed the scope that is directly or reasonably related to the purpose claimed at the time of the collection of personal information."[124] The 2018 SAMR Specification (2020 Revision) also introduces the requirement of storage limitation, stating that "the storage period of personal information should be the minimum time necessary to achieve the purpose authorized by the data subject,"[125] and the data must be erased or anonymised when those purposes have been served.[126]

The Cybersecurity Law requires that "network operators shall strictly maintain the confidentiality of user information they collect, and establish and complete user information protection systems."[127] It further requires that network operators shall adopt technical measures and other necessary measures to ensure the security of personal information.[128] In the case of data breaches, remedial measures shall be immediately taken, and the network operators shall promptly inform the users and to make a report to the competent departments in accordance with regulations.[129] The 2018 SAMR Specification (2020 Revision) also requires that an incident notification must explain the nature and impact of the incident, the measures taken or to be taken in response, the practical recommendations for data subjects to minimise the impact of the incident, and the data subjects' rights and remedies.[130]

The 2018 SAMR Specification (2020 Revision) requires organisations to employ enhanced security measures, such as de-identification of personal information and encryption of sensitive personal data.[131] Likewise, under the 2020 PBOC Specification, financial institutions should use de-identification,

122. *2018 SAMR Specification (2020 Revision)*, Section 5.3(a).
123. *2018 SAMR Specification (2020 Revision)*, Section 5.4(b).
124. *2018 SAMR Specification (2020 Revision)*, Section 7.3.
125. *2018 SAMR Specification (2020 Revision)*, Section 6.1(a).
126. *2018 SAMR Specification (2020 Revision)*, Section 6.1(b).
127. *Cybersecurity Law*, Article 40.
128. *Cybersecurity Law*, Article 42.
129. *Cybersecurity Law*, Article 42.
130. *2018 SAMR Specification (2020 Revision)*, Sections 10.1 & 10.2.
131. *2018 SAMR Specification (2020 Revision)*, Sections 6.2 & 6.3.

anonymisation or encryption where necessary to protect the personal financial information after collection.[132] The 2020 PBOC Specification further specifies that the transmission of information in C2 or C3 categories through a public network should be conducted through encrypted channels.[133]

Network operators are obligated to allocate persons responsible for network security as part of their internal security management systems.[134] The 2018 SAMR Specification (2020 Revision) and the 2020 PBOC Specification stipulate controllers' duties of responsibility and accountability.[135] Financial institutions should establish a specific unit responsible for protecting financial information,[136] and exercise necessary supervision of the responsible personnel.[137] For other entities acting as data controllers, they are expected to designate a person or agent to manage personal data.[138] If an organisation has more than 200 personnel and its main business involves processing personal data, or if the organisation is expected to handle the personal data of more than 1,000,000 people over the next 12 months, then it should establish a department with dedicated staff to handle personal data security.[139]

Under the Cybersecurity Law, data subjects can request network operators to delete their personal information if individuals discover that network operators have violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information.[140] The 2018 SAMR Specification (2020 Revision) gives more control to the data subjects; for instance, a data subject has the right to access his information collected by the data controllers[141] and the right to rectify inaccurate information.[142] Data subjects can revoke consent to data processing, after which the data controller is not allowed to further process the data.[143] The 2018 SAMR Specification (2020 Revision) also reiterates data subjects' rights to delete information if the data controller has breached its legal obligations or an agreement with the data subject. The same right

132. *2020 PBOC Specification*, Section 6.1.3.
133. *2020 PBOC Specification*, Section 6.1.3.
134. *Cybersecurity Law*, Article 21.
135. *2018 SAMR Specification (2020 Revision)*, Section 11; *2020 PBOC Specification*, Section 7.2.
136. *2020 PBOC Specification*, Section 7.2.2.
137. *2020 PBOC Specification*, Section 7.2.3.
138. *2018 SAMR Specification (2020 Revision), Section 11.1(b).*
139. *2018 SAMR Specification (2020 Revision)*, Section 11.
140. *Cybersecurity Law*, Article 43.
141. *2018 SAMR Specification (2020 Revision)*, Section 8.2.
142. *2018 SAMR Specification (2020 Revision)*, Section 8.2.
143. *2018 SAMR Specification (2020 Revision)*, Section 8.4(a).

extends to information in the possession of data processors.[144] Personal data should also be deleted or anonymised when users close down accounts.[145]

3.2.4 Enforcement Mechanisms

Under the Cybersecurity Law, the Cyberspace Administration of China is responsible for the overall planning and coordination of cybersecurity work and related supervision and management work.[146] The implementation of the Cybersecurity Law is left to the Public Security Bureau and the MIIT.[147] While the Public Security Bureau is mainly responsible for the investigation of criminal offences, the MIIT, as the chief internet and telecommunication regulator, is responsible for dealing with privacy-related complaints.

Apart from the general agencies for data protection, attention also needs to be paid to the specialist financial regulators, particularly because mobile payment represents a form of financial service. The current financial regulatory structure in China has the defining feature of being sector-based.[148] As the central bank, the PBOC assumes responsibility for monetary policies and the stability of the national financial system generally. The China Banking and Insurance Regulatory Commission (CBIRC) and the China Securities Regulatory Commission are the authorities responsible for regulating the banking and insurance sectors and the securities sector respectively. The banking sector is broadly defined to cover commercial banks, non-bank financial institutions and trust companies.[149] Hence, as non-bank financial institutions, mobile payment platforms are subject to the regulation of both the PBOC and the CBIRC.

Individuals and organizations have the right to report conducts endangering cybersecurity to relevant departments.[150] Cybersecurity refers to the "capacity for network data to be complete, confidential and usable as well as protecting them from attack."[151] The relevant competent departments may order the organisations to make corrections, and can, according to the

144. *2018 SAMR Specification (2020 Revision)*, Section 8.3.

145. *2018 SAMR Specification (2020 Revision)*, Section 8.5.

146. *Cybersecurity Law*, Article 8.

147. *Cybersecurity Law*, Article 8.

148. ROBIN HUI HUANG, SECURITIES AND CAPITAL MARKETS LAW IN CHINA 24–35 (Oxford University Press, 2014).

149. *Id.* at 27–29; Robin Hui Huang, *The Logics and Path of the Reform of China's Financial Regulatory Structure: International Experiences and Local Choice* 2019(3) FAXUE JIA 124-137 (2019) (discussing the development and function of the CBIRC).

150. *Cybersecurity Law*, Article 14.

151. *Cybersecurity Law*, Article 76(2).

circumstances, confiscate any illegal income made and impose a fine of not less than one time and not more than ten times the illegal gains. If there are no illegal gains, a fine up to 1,000,000 yuan shall be imposed, and the person in charge and other persons directly responsible shall be fined not less than 10,000 yuan but not more than 100,000 yuan. If the circumstances are serious, the relevant departments can suspend the organisations' relevant business and revoke their business licenses.[152]

In addition to administrative fines, private civil action is available for individuals whose rights have been harmed.[153] An individual may file a claim in tort if his right or interest has been infringed.[154] Network users and network service providers may be required to make apologies and restore the claimants' reputation.[155] Where their violations cause "financial loss or grave psychological harm", the claimants can request compensation.[156] Where the loss or harm is not ascertainable, the courts may order damages up to 500,000 yuan.[157]

The Cybersecurity Law states that where any breaches of the law constitute a crime, criminal responsibility will apply to the wrongdoers.[158] The Criminal Law which has been discussed above would apply.

4. INTERNATIONAL EXPERIENCES

The internet landscape has changed profoundly over the past decades. In the international arena, many jurisdictions are evaluating or reforming their regulatory frameworks to protect consumers and respond to technological innovation. In this part, we will examine the regulatory frameworks of some major jurisdictions, including the United States, the European Union, Singapore, and Hong Kong.

4.1 The United States

The United States (US) deals with data privacy on a sectoral basis. There are no omnibus records of federal privacy statutes, and the method of

152. *Cybersecurity Law*, Article 64.

153. *Cybersecurity Law*, Article 74.

154. 0137.

155. Zuigao renmin fayuan guanyu shenli liyong xinxi wangluo qinhai renshenquanyi minshi jiufen anjian shiyong falv ruogan wenti de guiding" (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定)[Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Disputes over the Use of Information Network to Infringe upon Personal Rights and Interests] (issued by Supreme People's Court on 23 June 2014, effective from 10 October 2014), Article 16 (hereinafter *China's Supreme Court Provisions*) .

156. *China's Supreme Court Provisions*, Article 17.

157. *China's Supreme Court Provisions*, Article 18.

158. *Cybersecurity Law*, Article 74.

protecting personal information depends on the specific category of the information involved.

The categories covered under federal laws include, among others, healthcare data (under the Health Insurance Portability and Accountability Act)[159], financial data (under the Gramm Leach Bliley Act)[160], children's information (under the Children's Online Privacy Protection Act)[161], consumer credit data (under the Fair Credit Reporting Act)[162], electronic communication data (under the Electronic Communications Privacy Act).[163] The FTC, which is the main regulatory body addressing privacy breaches[164], fills in some of the statutory gaps by taking actions against unfair and deceptive data protection practices.[165]

The pertinent laws for mobile payment privacy protection include the Gramm Leach Bliley Act and the FTC Act.[166] The Gramm Leach Bliley Act imposes several obligations of protecting consumers' non-public personal information from financial institutions engaging in financial activities. Financial institutions must provide consumers with "clear and conspicuous" notice describing their privacy policies.[167] Financial institutions are generally not allowed to share non-public personal information with non-affiliated third parties unless they provide consumers with notice and an option to opt-out,[168] nor can they share consumers' financial information to third parties for direct marketing.[169] Federal banking regulators are responsible for supervising depository institutions, and the FTC regulates all non-depository institutions.[170] Wrongdoers who knowingly and intentionally obtain or disclose "customer information" through false or fraudulent statements or representations will face criminal liability.[171]

The FTC Act gives the FTC authority to take actions against unfair and deceptive data protection practices. Generally speaking, an act or practice is

159. 42 U.S.C. § 1320d(9).
160. 15 U.S.C. §§ 6801–6809.
161. 15 U.S.C. §§ 6501.
162. 15 U.S.C. § 1681.
163. 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3126.
164. FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last visited June 18, 2021).
165. FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 18, 2021); Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, 587 (2014).
166. 15 U.S.C. § 41.
167. 15 U.S.C. § 6803(a); 12 C.F.R. §§ 1016.4–1016.6.
168. 15 U.S.C. § 6802(b); 12 C.F.R. § 1016.10(a).
169. 15 U.S.C. § 6802(d); 16 C.F.R. § 313.12(a).
170. 15 U.S.C. § 6805(a)(1)–(7).
171. 15 U.S.C. §§ 6821, 6823.

unfair only if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[172] As for the concept of "deceptive," the FTC has clarified that an act or practice is to be considered deceptive if it involves a material "representation, omission, or practice that is likely to mislead [a] consumer" who is "acting reasonably in the circumstances."[173]

Some scholars have pointed out that the FTC's enforcement approach is based on the principle of "common law" of privacy.[174] Crucial to this principle is the idea of "notice and choice" where companies are required to disclose their privacy policy enabling their users to make an informed choice.[175] Companies are bound against deceiving others by their data privacy and data security promises.[176] Companies act deceptively if they make false representations in order to induce disclosure of personal information,[177] or provide insufficient notice about their privacy practices.[178] The FTC can either bring administrative proceedings or civil proceedings.[179] But most actions initiated by the FTC are negotiated and settled through the consent order procedures.[180] The FTC Act does not provide a right to private action, nor does it provide a criminal sanction.

In addition, all 50 states have enacted data breach notification statutes following the California Security Breach Notification Law with effect from July 1, 2003, to establish data breach notification mechanisms.[181]

4.2 The European Union

The right to data protection is one of the fundamental rights in the European Union (EU). This right is believed to be grounded in the concept

172. 15 U.S.C. § 45(n).

173. FTC, POLICY STATEMENT ON DECEPTION 1–2 (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception (last visited June 19, 2021).

174. Daniel Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy* 114 COLUMBIA L. REV. 583, 619 (2014).

175. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 40 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf (last visited June 15, 2021).

176. *Solove and Woodrow, supra* note 181*,* at 628.

177. *Id.* at 630.

178. *Id. at 634*.

179. *Id.* at 609.

180. *Id.* at 610.

181. NATIONAL CONFERENCE OF STATE LEGISLATURES, SECURITY BREACH NOTIFICATION LAWS (2018), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last accessed June 20, 2021).

of human dignity.[182] The stand-alone right to data protection marks one of the major differences between the US and the EU in protecting personal data.[183]

The early history of the EU data protection law begins within individual European countries, such as Sweden (1973), the Federal Republic of Germany (1977), Austria (1978), Denmark (1978), France (1978), and Norway (1978).[184] In 1995, the EU started to harmonise the data privacy law and adopted the 95 Directive to protect the collection, use, process and exchange of personal data based on the recommendation proposed by the OECD.[185] The 95 Directive was replaced by the General Data Protection Regulation (GDPR) in 2018.[186]

The key principles of data protection in the GDPR are specified in Article 5, including the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. The GDPR requires data controllers and processors to have a lawful basis for processing personal data. These legal bases include consent, performance of the contracts, compliance with legal obligations, protection of the vital interests of the data subject or another individual, tasks carried out in the public interest, and legitimate interests of the controllers or a third party.[187] The individuals have the right to be informed, right of access, right to rectification, right to be forgotten, right to restrict processing, and right to data portability.[188] Data controllers are required to implement a range of measures designed to ensure the compliance with the GDPR, such as establishing GDPR-conforming contracts with data processors,[189] maintaining records of processing

182. ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 242 (Oxford University Press, 2015).

183. James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Review* 1151; Paul M. Schwartz, "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures" (2013) 126 *Harvard Law Review* 1966.

184. Colin J Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instrument in Global Perspective* (Cambridge, Massachusetts: MIT Press, 2006), 127.

185. Summaries of EU Legislation, "Protection of Personal Data", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14012

186. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 [hereinfater GDPR].

187. GDPR, Article 6.

188. GDPR, Articles 12-23.

189. GDPR, Article 28(3).

activities,[190] conducting impact assessments on personal data use,[191] and appointing a data protection officer.[192]

In the event of a personal data breach, the GDPR requires data controllers to notify the relevant authorities of any breach within 72 hours of discovering it.[193] The GDPR allows European data protection authorities to fine companies up to the higher of €20 million or 4 percent of their global turnover for the most severe category of data protection violations.[194] Individuals also have the right to lodge a complaint with regulatory authorities.[195] They can seek an effective judicial remedy against data controllers and processors, and obtain compensation for their damages suffered.[196]

The Payment Service Directive 2 (PSD2)[197] came into force on 12 January 2016, and the EU Member States were required to legislate it into national law by 13 January 2018.[198] The European Commission considered the PSD2 to be necessary to address the potential gaps in the regulatory regime for payment services. In terms of data protection, there are considerable overlaps between the PSD2 and the GDPR. The PSD2 reiterates the application of the 'principles of necessity, proportionality, purpose limitation, and proportionate data retention period' to payment service providers.[199]

It is worth noting that the PSD2 lays out stricter obligations of data protection on third-party payment providers (including payment initiation service providers and account information service providers). Under the GDPR, personal data can only be collected for "specified, explicit and legitimate purposes."[200] By comparison, the PSD2 states that third-party payment providers can only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.[201] They are not allowed to "use, access

190. GDPR, Article 30.
191. GDPR, Article 35.
192. GDPR, Article 37-39.
193. GDPR, Article 33.
194. GDPR, Article 83(5)-(6).
195. GDPR, Article 77.
196. GDPR, Articles 79 & 82.
197. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35 [hereinafter PSD2] .
198. PSD2, Article 115(2).
199. PSD2, Recital 89.
200. PSD2, Article 5(1)(b).
201. PSD2, Article 94(2).

or store any data for purposes other than for performing their service explicitly requested by the customer."[202] It essentially prohibits third-party payment providers from collecting ancillary information, which is not necessary for the service of payment or using the information for additional marketing purposes.

Under the PSD2, payment service providers are required to notify their home competent authority in the case of a "major operational or security incident."[203] Where the incident may have an impact on the financial interests of payment service users, payment service providers must also inform payment service users of the incident and requisite mitigation measures without undue delay.[204]

Additionally, the E-Privacy Directive[205] gives individuals specific protections in relation to online-tracking issues, and it can be summarised as follows. First, unsolicited marketing by phone, email, or other electronic messages may only be allowed if consumers have given their prior consent.[206] Secondly, service providers must obtain users' active and clear consent before setting cookies.[207] Thirdly, service providers must take appropriate measures to safeguard the security of their service, and they are obligated to notify the relevant authorities and consumers in the case of a data breach.[208] Fourthly, subject to several exemptions,[209] service providers are obligated to erase or anonymise the data processed when no longer needed.[210]

4.3 Singapore

Singapore's key data protection law is the Personal Data Protection Act (PDPA)[211] which is structured around the fundamental principles of FIPs.

202. PSD2, Articles 66 & 67.

203. PSD2, supra note 175 at Article 96(1).

204. PSD2, supra note 175 at Article 96(1).

205. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201/37) [hereinafter E-Privacy Directive].

206. *Id.* at Article 13.

207. *Id.* at Article 5(3) & Recital 24; European Commission, Cookie Policy,https://ec.europa.eu/info/cookies_en (explaining that Cookie is a small text file that a website stores on the user's computers or other devices when the user visits the site which allows the service providers to recognise that user's device and store some information about the user's preferences or past actions).

208. E-Privacy Directive, supra note 183 at Article 4.

209. E-Privacy Directive, supra note 183 at Article 15.

210. E-Privacy Directive, supra note at Article 6.

211. Personal Data Protection Act, 2012 (Sing.).

These principles are very similar to those in the 2018 SAMR Specification (2020 Revision) and the GDPR, and thus will not be discussed again here. The PDPA is enforced by the Personal Data Protection Commission who has the power to make orders to an organization to ensure its compliance with the PDPA and impose penalties not exceeding S$1 million.[212] Criminal penalties may also be imposed on organisations or individuals that obstruct the commission or its authorised delegate in the performance of its duties or powers under the PDPA.[213]

The PDPA provides several rights to individuals. They can give notice to the relevant organisations to withdraw their consent given or deemed to have been given in respect of collection, use, or disclosure of their personal data.[214] Individuals have rights to access personal data[215] and to make corrections.[216] Besides, the PDPA provides for the right of an individual to take civil action against an organisation if that individual suffers loss or damage as a result of a contravention of the PDPA.[217] The possible remedies include injunction, declaration, damages, or other relief as the court thinks fit. The PDPA imposes very limited obligations on data processors. These obligations are restricted to the areas of data security[218] and data retention.[219]

The PDPA also establishes the Do Not Call Registry (DNCR) scheme, which allows individuals to opt out of receiving certain direct marketing messages. Section 40 of the PDPA states that "a subscriber may apply to the Commission, in the form and manner prescribed to add his Singapore telephone number to a register."[220] The PDPA prohibits any person or organisation from sending marketing messages to a number that is listed on the DNCR.[221] Fines of up to S$10,000 may be imposed on the failure to comply with the DNCR obligations.[222]

There are a very wide range of circumstances allowing for the collection, use, or disclosure of personal information without obtaining consent from data subjects (or allowing collection from third parties).[223] Many exemptions are phrased in very broad terms, which could give rise to

212. Personal Data Protection Act § 48J.
213. Personal Data Protection Act Part X.
214. Personal Data Protection Act § 16.
215. Personal Data Protection Act §21.
216. Personal Data Protection Act § 22.
217. Personal Data Protection Act § 48O.
218. Personal Data Protection Act § 24
219. Personal Data Protection Act § 25.
220. Personal Data Protection Act § 40.
221. Personal Data Protection Act § 43.
222. Personal Data Protection Act § 51.
223. Personal Data Protection Act, § 17, Second to Fourth Schedules.

significant legal uncertainty and undermine the effectiveness of such protection.

Unlike the EU or China, Singapore does not distinguish between general personal information and sensitive personal information. Therefore, there is no enhanced protection on sensitive personal information. Currently, under the PDPA, there is no mandatory requirement for data users to notify authorities or data subjects about data breaches.

4.4 Hong Kong

The Personal Data (Privacy) Ordinance (PDPO) establishes Hong Kong's data protection legal framework.[224] All organisations that collect, hold, process or use personal data must comply with the PDPO. Similar to the EU's approach, Hong Kong basically structures the PDPO around the FIPs.

Hong Kong has strengthened its regulation on direct marketing by adding relevant provisions as such into the PDPO effective from 1 April 2013. Data users must obtain subjects' express consent before they use or transfer the data subjects' personal data for marketing purposes.[225] Non-compliance with the direct marketing provisions is an offence, and the highest penalties are a fine of HK$500,000 and imprisonment for three years.[226] Under the PDPO, there is no mandatory requirement of data breach notification or the appointment of data protection officers. The PDPO also fails to regulate data processors appointed by data users for the data process.

The sanctions under the PDPO are very limited. A contravention of the data protection principles does not in itself constitute a crime or result in any punishment. The Privacy Commissioner for Personal Data has the power to issue notices requiring data users to take steps to make corrections or prevent further violations.[227] Data users will only commit an offence if they fail to comply with the enforcement notice or violate the requirement again. In that case, the maximum fine is HK$50,000 and imprisonment for two years.[228] If a data user contravenes more than one notice, the maximum penalty is a fine of HK $500,000 and imprisonment for three years.[229]

224. Personal Data (Privacy) Ordinance (Hong Kong) (Cap. 486).
225. PDPO, § 35E.
226. PDPO, § 35E(4).
227. PDPO, § 50.
228. PDPO, § 50A.
229. PDPO, § 50B.

5. EVALUATION AND RECOMMENDATIONS

5.1 Comparative Insights and Merits of the Chinese Law

The above examination of some major jurisdictions' data protection regimes shows that both the US and the EU have well-established regulatory frameworks, but the EU's model is proven to be more influential in shaping other jurisdictions' data protection laws, such as those of Singapore and Hong Kong. We also note that the effectiveness of Singapore's data protection law is partially undermined by its wide exemptions, while the sanctions under Hong Kong's data protection law are inadequate.

In the EU, the right to data protection is a fundamental right[230] and protected by a comprehensive set of legal rules. The GDPR has a wide scope of application, covering all natural or legal persons collecting and processing personal data. By comparison, in the US, there is no unified data protection law and the respective data protection provisions are scattered among many laws that regulate different sectors. While the EU's data protection law is structured around data subjects' right to data protection, the US's philosophy of data protection is based on the idea that consumers' interests should be protected against deception or unfairness.[231] Despite their different approaches, data protection laws on both sides are informed by the FIPs and share the core principles of fairness, lawfulness, transparency, data minimisation, purpose limitation and so forth. But some principles in the US are less stringent than those in the EU. One classic example is that data subjects in the US are generally required to opt out to stop sharing their personal data with third parties rather than opt into the service. The underlying reason behind the less stringent requirements seems that the US is trying to strike a balance between Internet economy innovation and consumer protection.[232]

By comparing China's regulatory approach with other jurisdictions, we find that China started with a piecemeal approach resembling the US model but is now moving towards the EU's principle-based approach.[233] The 2018 SAMR Specification (2020 Revision), as a comprehensive guide of data protection, substantially follows the GDPR's regulatory approach. Significantly, the Cybersecurity Law and the 2018 SAMR Specification

230. The Charter of Fundamental Rights of the European Union, Article 8.

231. Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law* (2017) 106 GEORGETOWN L. J. 115, 119 (2017).

232. Gina Stevens, *Privacy Protections for Personal Information Online*" 2 Cong. Res. Serv. 2 (2011).

233. For a comprehensive discussion, see Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?* 8 PENN ST. *J. L.* & *INT'L* AFFS. 49 (2020).

(2020 Revision) widen the application scope, covering all organizations that collect and process personal data, and impose strict obligations of data protection on them.

For mobile payment, the laws and regulations address the privacy risks of mobile payment, such as target advertising. For instance, "the information that may reflect a specific person (without necessarily identifying) them"[234] now falls within personal information so that the collection and processing of personal data will be subject to the data protection requirements under the 2018 SAMR Specification (2020 Revision). It would help to deal with target marketing, one of the major threats to the data privacy of mobile payments, particularly in the case where target marketing does not directly use personally identifiable information but often uses software to build personal profiles excluding the necessary identifiable information.[235]

The 2018 SAMR Specification (2020 Revision) deals with online tracking problems that are often considered intrusive and threatening to personal data privacy. Many online platform service providers would place cookies or similar tracking devices on users' equipment without their knowledge to track their online behaviour and usage patterns in order to develop a specific profile and provide consumers with tailored advertisements.[236] The 2018 SAMR Specification (2020 Revision) regards the information of online activities as sensitive information and requires service providers to obtain the users' opt-in consent before collecting such information.[237]

The 2018 SAMR Specification (2020 Revision) also makes a distinction between anonymized data and de-identified data.[238] It does not exclude the de-identified data from the scope of personal information as this type of data may still be identified with the help of additional information.[239] The special mechanisms of protecting sensitive personal information are introduced, such as explicit consent from data subjects before collection,[240] encryption storage and transmission of sensitive information,[241] as well as

234. Greenleaf Graham and Livingston Scott, *China's Personal Information Standard: The Long March to a Privacy Law* 150 PRIV. *L.* & BUS. INT'L REP. 25, 26 (2017).

235. Paul M.Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information* 86 N.Y.Univ. L. REV. 1814, 1854–55 (2011).

236. Ira S. Rubinstein, Ronald D. Lee, and Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches* 75 UNIV. CHI. L. REV. 261, 271 (2008).

237. 2018 SAMR Specification (2020 Revision), §5.4(b).

238. 2018 SAMR Specification (2020 Revision), supra note 58 at §§3.14 - 3.15.

239. Paul Ohm, Broken Promise of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA L. REV.*, 1701, 1716-27 (2010).

240. 2018 SAMR Specification (2020 Revision), supra note 58 at § 5.5.

241. 2018 SAMR Specification (2020 Revision), supra note 58 at §6.2.

special controls of accessing sensitive information.[242] Likewise, under the 2020 PBOC Specification, financial institutions should use de-identification, anonymisation or encryption where necessary to protect the personal financial information after collection.[243]

In relation to the consent requirement, the 2018 SAMR Specification (2020 Revision) prohibits the bundle or forced consent.[244] Opt-in consent is required before the collection of sensitive information is allowed.[245] The principle of transparency is also strengthened. The disclosure statements are required to be presented in a concise, meaningful, timely and accessible manner.[246] A standardised short-form notice is introduced to allow users to digest privacy policies more easily.[247]

As discussed before, the PBOC has played a proactive role in strengthening data privacy protection for the financial industry. The 2020 PBOC Specification represents the PBOC's more recent effort in this regard. It adds some industry-specific parameters by grading the personal financial information into three categories, which in turn require different protective measures. By doing so, it provides clearer guidance on data protection for the relevant institutions, including banks and non-bank payment institutions. In general, the 2020 PBOC Specification largely aligns with the 2018 SAMR Specification (2020 Revision) on the FIPs and specific technical requirements, such as de-identification, anonymisation and encryption.

Overall, in relation to data privacy protection, the rules issued by the PBOC[248] are essentially intended to embody and specify the general regulatory requirements of data protection for the financial markets, and do not really introduce many new regulations. While the general regulatory regime can be used to deal with many privacy risks in mobile payment, some risks are much more acute for mobile payment users. Accordingly, it is important for the regulators to make specific rules to facilitate compliance and enforcement regarding the privacy issue in mobile payment.

242. 2018 SAMR Specification (2020 Revision), supra note 58 at §7.1(e).

243. 2020 PBOC Specification, supra note 65 at § 6.1.

244. 2018 SAMR Specification (2020 Revision), supra note 58 at §5.3(a).

245. 2018 SAMR Specification (2020 Revision), supra note 58 at §5.5.

246. 2018 SAMR Specification (2020 Revision), supra note 58 at §§5.5(b) - (c).

247. 2018 SAMR Specification (2020 Revision), supra note 58 at Appendix D.

248. For example, "Feiyinhang Zhifu Jigou Wangluo zhifu yewu guanli banfa" (非银行支付机构网络支付业务管理办法) [The Management Measures of the Mobile Payment Business of the Non-bank Payment Institutions] (issued by the People's Bank of China on 28 December 2015, effective from 28 December 2015); Zhongguo renmin yinhang jinrong xiaofeizhe quanyi baohu shishi banfa" (中国人民银行金融消费者权益保护实施办法) [Measures for the Protection of the Rights and Interests of Financial Consumers of the People's Bank of China] (issued by the People's Bank of China on 15 September 2020, effective from 1 November 2020).

5.2 Remaining Problems and Recommendations

5.2.1 Improving Certain Regulatory Requirements and Principles

For mobile payment, there are some remaining problems with the regulation, the chief among which is the ineffective requirements of consent and disclosure, the ambiguous principle of purpose limitation, and the limited applicability of the principle of data minimisation. These problems need to be addressed in order to improve the efficacy of the regulation.

To begin with, while the disclosure requirement is crucial to data protection, the effectiveness of disclosure is undermined in the context of mobile payment. One major reason is that the privacy policies are often provided in scrolling text boxes present on mobile phones' small screens.[249] They are often several pages long, and users usually would not spend considerable time reading the policies which are full of complex and technical terms before using a particular service. The inefficiency of the disclosure requirement further undermines the effectiveness of the consent requirement.[250] Although the 2018 SAMR Specification (2020 Revision) requires consumers' affirmative consent, many consumers may simply tick consent boxes without reading or understanding the policies.[251] The prohibition on bundle consent is mainly theoretical with little practical meaning, as a single collection request for its major mobile payment service will allow the mobile payment service providers to collect all the necessary information. If consumers refuse to accept the privacy policy, their access to the platform will be denied.

Inspired by the EU's approach, this article makes two recommendations to solve this issue. First, a multi-layered notice mechanism can be used. Specifically speaking, the essential information in relation to the data collection and processing should be presented in the initial notice to the consumers in a concise and readable manner.[252] It can be combined with the use of icons, images or videos. Further detailed information can be made available through hyperlinks.[253] The primary purpose of this approach is to

249. Marla Blow, Statement for the Record of Marla Blow before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit, House Financial Services Subcommittee, 2, (2012), https://financialservices.house.gov/uploadedfiles/hhrg-112-ba15-wstate-cfpb-20120629.pdf

250. Bert-Jaap Koops, The Trouble with European Data Protection Law 4(4) *International Data Protection Law* 250, 251 (2014).

251. Marla Blow, supra note 227.

252. Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices, 24, a https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

253. Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices"24, (Feb. 27, 2013) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (hereinafter Data Protection Working Party).

allow consumers to quickly grasp the key information on the privacy policies. Second, we note that the mobile payment service providers usually make their service contingent upon consumers' acceptance of their privacy policy practices of extensively collecting their personal information (both financial and ancillary information). The problem with this "take-it-or-leave-it" approach is, however, particularly unfair to the consumers in China where the mobile payment market is dominated by two giants – Alipay and WeChat Pay, and consumers do not have much choice but to accept their privacy policies. Therefore, like the requirement of the PSD2 in the EU, the data controllers should only collect and process personal data necessary for the provision of their payment services. Even if they intend to collect ancillary data for additional purposes (such as marketing purpose), a separate consent from consumers must be obtained.

Further, the Cybersecurity Law does not contain the principle of purpose limitation. The 2018 SAMR Specification (2020 Revision) also fails to give a detailed definition of this principle except a simple statement that "the use of personal information should not exceed the scope that is directly or reasonably related to the purpose claimed at the time of the collection of personal information."[254] The issue is how to determine whether the purpose for which the data is originally collected and processed is directly or reasonably related to the purpose of further processing. For example, one privacy concern arising in mobile payment is target advertising. If we booked a flight on an online platform, we may find that this platform will keep recommending advertisements on hotels after the booking. Would we say that this advertising is directly or reasonably relevant to the original purpose of collecting information, which is supposed to be the execution of payment?

The EU's Article 29 Data Protection Working Party has provided a systematic approach to deal with this issue. When examining whether the additional purpose of processing data is directly or reasonably related to the original purpose, the following factors could be taken into consideration: whether the new purpose was already implied or a logical next step in the processing, whether the consumers expressly consented to the further processing, whether the processing involved sensitive personal information, and whether the controllers have adopted safeguards "to ensure fair processing and to prevent any undue impact on the data subjects (e.g., anonymisation, increased transparency, a possibility to object)."[255] Another practical approach to deal with this problem is that a data controller could

254. 2018 SAMR Specification (2020 Revision), Section 7.3.
255. Data Protection Working Party at 3.

list the original purpose and the additional purposes of collecting and processing data, allowing consumers to opt-in for the acceptable ones.

Last but not least, under the 2018 SAMR Specification (2020 Revision), the principle of data minimisation only applies to the stage of data collection.[256] By comparison, under the GDPR, the principle of data minimization does not only apply to data collection but applies to all types of data processing.[257] It is possible for information that is initially collected in a lawful manner under this principle to be illegally processed later. Therefore, it is important to ensure that all stages of data processing should comply with the principle of data minimisation.

5.2.2 Establishing A Unified Data Protection Law and A Unified Enforcement Agency

Although China is moving toward a coherent legal structure on data protection, the relevant laws and regulations are still broad-brush and repetitive. The 2018 SAMR Specification (2020 Revision) and the 2020 PBOC Specification are not mandatory, but rather serve as voluntary industry standards. No direct penalties would be applied for contravention of these two specifications. Although they can act as reference for law enforcement authorities to decide compliance with various data protection rules, the authorities have latitude in their enforcement and this can create significant legal uncertainty. We can find that a unified data protection law is a global common practice. It is submitted that China should incorporate the basic principles and specific requirements of data protection into one unified law to reduce fragmentation of laws, strengthen consistency in enforcement, simplify the regulatory environment, and reduce unnecessary costs and administrative burden. In light of our analysis on the efficiency of China's current data privacy protection regime, it is recommended that future legislation could be structured around two well-recognised axes.[258] The first one is privacy by design, where companies are obligated to comply with the data protection requirements at every stage of the development of products and services. The second axis is privacy by default where the data controllers make pre-existing choices on behalf of the data subjects regarding the data processing option, and in doing so, they must ensure that only the personal data that is necessary to achieve the purpose of the processing is enabled.

256. 2018 SAMR Specification (2020 Revision), Section 5.2.

257. GDPR, Article 5.

258. GDPR, Article 25;but see Ira S. Rubinstein and Nathaniel Good, "The Trouble with Article 25 (and How to Fix It): the Future of Data Protection by Design and Default" (2020) 10(1) *International Data Privacy Law*, 37.

Apart from a unified data protection law, there is also a need for a unified enforcement agency, which is more efficiently structured to facilitate the enforcement of the law. Under China's current regulatory regime, there are multiple enforcement agencies responsible for enforcing the myriad statutory protections, including but not limited to the Cyberspace Administration of China, the Public Security Bureau, and the MIIT. In addition, as non-bank financial institutions, mobile payment service providers are also subject to the regulation of both the PBOC and the CBIRC. The SAMR has the general responsibility to protect consumers' rights, including the right to data protection.

By examining the experiences of those overseas jurisdictions, we note that a unified law enforcement agency is a common practice in data privacy protection. However, in China, the enforcement could be hampered by the existence of multiple enforcement agencies authorized by different laws. This is illustrated by the Alipay case. At the end of 2017, Ant Financial (an affiliate of Alibaba Group Holding Limited operating the Alipay mobile payment services of Alibaba's shopping platform) launched its Alipay Annual User Footprint Report within its Alipay mobile wallet application, allowing users to look how they had spent their money over the year.[259] However, the landing page of the report had a small box that was checked by default, which provided that "I consent to the 'Sesame Credit Service Agreement'". Users who did not notice the checked box would have agreed by default to opt into this agreement under which Ant Financial can direct users' information to the third party Sesame Credit, and the users were not allowed to revoke their consent.[260] When Alipay's grasping terms of service came into light, many users expressed their grave concerns over their data privacy.[261]

As Ant Financial is subject to the regulation of multiple authorities, including the Cyberspace Administration of China, the MIIT and the PBOC, these authorities have taken different actions against the company. On 6 January 2018, the Security and Coordination Office of the Cyberspace Administration of China made inquiries into Ant Financial and Sesame Credit, concluding that Ant Financial failed to meet the data protection

259. SOUTH CHINA MORNING POST, *Alibaba's payments affiliate apologises for opting in users for credit scoring system*, (Jan. 4, 2018, 11:09 am), https://www.scmp.com/tech/china-tech/article/2126772/chinas-ant-financial-apologises-over-alipay-user-data-gaffe.

260. *Id.*

261. *Id.*

requirements set out in the 2018 SAMR Specification (2020 Revision).[262] On 11 January 2018, the Communication Management Office of the MIIT inquired into three technology companies – Alibaba Group, Baidu and ByteDance and reprimanded these companies for not giving sufficient notification to users on their privacy policies.[263] These companies were requested to immediately rectify and improve their privacy policy to protect the users' rights and interests.[264] On 22 March 2018, the Hangzhou Central Branch of the PBOC imposed an administrative fine of 180,000 yuan on Ant Financial on the basis that the data practice of Ant Financial failed to provide adequate protection for financial consumers' right to know and right to choose.[265]

In summary, the lack of a single privacy law enforcement agency has caused conflict and friction between different authorities, leading to fragmented and incoherent decision-making. Different authorities may also bring actions for the same violation, which will not only result in a waste of regulatory and judicial resources but will also give rise to the issue of inconsistent judgments. Therefore, China should consider establishing a unified agency responsible for the enforcement of a unified data protection law.

5.2.3 Enhancing both Public and Private Enforcement

As with any other areas of law, the effectiveness of the data protection regime depends on both substantive rules and enforcement strategies. In general, law enforcement strategies can be broadly divided into two modes – public enforcement and private enforcement. Public enforcement is initiated by a state official such as a regulator or a prosecutor, while private enforcement is done so by a private party in the form of civil actions for compensation or rescission. These two modes of law enforcement have their own strengths and weaknesses. For instance, public enforcement has advantages *vis-à-vis* private enforcement in terms of the power to investigate and impose severe penalties. Private enforcement, however, has its own strengths. First, while the function of deterring misconduct is common to both public and private enforcement, private enforcement also has the

262. XINHUA NET, "Ant Financial Services Group reflects on 'Alipay Annual Billing Incident': Platform Governance Will be Improved" (Jan. 10, 2018, 13:12 pm), http://www.xinhuanet.com/fortune/2018-01/10/c_1122238416.htm.

263. SINA, "MIIT reprimanded Alipay, ByteDance and Baidu to rectify" (Jan. 13, 2018, 01:37 am), http://tech.sina.com.cn/i/2018-01-13/doc-ifyqqciz6242328.shtml.

264. *Id.*

265. PEOPLE'S NET, "Alipay was fined 180,000 yuan for multiple violations" (Apr. 09, 2018), http://it.people.com.cn/n1/2018/0409/c1009-29913402.html.

important function of compensating victims which public enforcement usually cannot perform. Second, the efficacy of public enforcement depends very much on the organizational capacity and resources of the regulator. As discussed above, there is a need for China to establish a uniform regulator for data protection. Hence, China is advised to pursue both enforcement strategies in relation to the data protection law.

On the one hand, private enforcement in the form of civil litigation is often sought on the basis of tort law, but a claimant may face many difficulties in pursuing the action. First, there can be an enormous imbalance of economic power and information asymmetry between the aggrieved individuals and the organizational data controllers, which makes it difficult for the claimants to produce evidence and prove the tortious act. This problem may become particularly acute where the data controllers exclusively possess the impugned information. For instance, in the case of *Lin Nianping v. Sichuan Airlines Co., Ltd,*[266] a passenger named Lin Nianping sued Sichuan Airlines for disclosing his personal information (including his name, phone number, and flight information) to a third party who subsequently misled Lin Nianping to buy another air ticket. The court found that Lin Nianping was an ordinary consumer who did not possess material evidence to prove the respondent's actual negligence of failing to protect personal data, whereas Sichuan Airlines Co Ltd was in a favourable position to provide the necessary evidence to prove otherwise. Lin Nianping had already proven a strong likelihood that the company disclosed its passenger's information, and it would be unfair to require him to further prove that Sichuan Airline Co Ltd was actually negligent. The reversal of the evidential burden has also been confirmed in *Pang Lipeng v. China Eastern Airlines Co., Ltd. and Beijing Qunar Information Technology Co., Ltd*[267] which was later compiled by the Supreme People's Court into the list "The First Batch of Typical Cases Related to the Internet."[268] The Supreme Court remarked that the claimant as an ordinary passenger did not have the ability to prove the respondents' negligence of failing to protect personal data, and

266. Lin Nianping yu Sichuan hangkong gufen youxian gongsi qinquan zeren jiufenan (林念平与四川航空股份有限公司侵权责任纠纷案)[*Lin Nianping v. Sichuan Airlines Co., Ltd* (regarding the dispute on tort liabilities)] (Chengdu Intermediate People's Court of Sichuan Province, civil (1634) 2015).

267. Pang Lipeng su zhongguo dongfang hangkong gufen youxian gongsi, Beijing quna xinxi jishu youxian gongsi yinsiquan jiufenan (庞理鹏诉中国东方航空股份有限公司、北京趣拿信息技术有限公司隐私权纠纷案) [*Pang Lipeng v. China Eastern Airlines Co., Ltd. and Beijing Qunar Information Technology Co., Ltd* (regarding the dispute on right of privacy)] (The First Intermediate People's Court of Beijing, civil (509) 2017).

268. "Diyipi she hulianwang dianxing anli" (第一批涉互联网典型案例) [The First Batch of Typical Cases Related to the Internet] (issued by the Supreme People's Court of the PRC on 16 August 2018).

the court cannot and should not require the claimant to prove that the respondent must have leaked the passenger's personal information. It was for the respondent to prove otherwise.

The second difficulty lies in the problem of proving concrete harm or loss suffered by the aggrieved party as "the risk accompanying the collection, use, and dissemination of personal data is accumulative."[269] Thirdly, even though the claimants could succeed in their claims, the courts may only award a small amount of damages. For example, in *Lin Nianping*, the court eventually ordered Sichuan Airline Co Ltd to make an apology and compensate Lin Nanping with 5,648 yuan (about US$806).[270] In *Pang Lipeng*, the court only ordered an apology to be made.[271] It may discourage the aggrieved party from bringing private actions. Fourthly, many data practices, such as data harvesting and profiling, often take place in a non-transparent manner. Without the knowledge of how their data are misused, individuals cannot effectively protect their personal data on their own.

On the other hand, under the mode of public enforcement, the relevant competent departments may order the organisations to make corrections, and can, according to the circumstances, confiscate any illegal income, and impose a fine of not less than one time and not more than ten times the illegal gains. If there are no illegal gains, a fine of not more than 1,000,000 yuan shall be imposed, and the person in charge and other persons directly responsible shall be fined not less than 10,000 yuan but not more than 100,000 yuan.[272] However, there are two issues with administrative fines. First, it may be easy to calculate the gains from the illegal trade in data but it would prove difficult to assess the unlawful gains made by internet companies. As discussed above, many internet companies, like Google and Facebook, do not trade in the personal data but use the data for target advertising and supply the data to develop their artificial-intelligence services, which can in turn generate new sources of profits. Assuming the data used in the development of artificial-intelligence services is illegally collected or processed, should we take into account the remote gains derived from the development of new technology? Secondly, the current level of fines in China is inadequate to act as a deterrent. In the Alipay Case, Alipay was only fined 180,000 yuan (about US$25,700) by the PBOC, which was negligible compared with this technology giant's annual revenue. By

269. Ding Xiaodong, "Personal Data Protection: Rethinking the Reasons, Nature, and Legal Framework" (2018) 13 *Frontiers of Law in China* 380, 387.

270. Supra n.237.

271. Supra n.238.

272. Cybersecurity Law, Article 64.

comparison, the GDPR allows European data protection authorities to fine companies up to the higher of €20 million or 4 percent of their global turnover for the most serious category of data protection violations.[273]

With the above observations, this article makes the following suggestions. First, given the massive asymmetry of information and evidential difficulties which limit the utility of private enforcement, this article suggests that a "piggyback" mechanism be introduced whereby the private action follows and thus can piggyback on the public enforcement in relation to threshold questions, such as the occurrence of infringements and the guilt of relevant people.[274] Second, as most data privacy infringements are motivated by the pursuit of profits, substantial fines can be introduced to deter illegal use of personal data.[275] To incentivise data controllers and data processors to comply with the requirements of data protection, future legislation should develop a system of determining fines for wrongdoers by taking into consideration economic and informational power of data controllers and processors, past acts of non-compliance, and the risks to which personal data is exposed as a result of their illegal practices. Similarly, in the private enforcement, the compensation awarded to the victims could be calculated by reference to the extent to which the personal data is illegally collected and the risk to which the personal data is exposed in the illegal data practices.

6. CONCLUSION

Mobile payment has transformed the Chinese economy. While consumers are enjoying the great benefits provided by mobile payment, they are also plagued by the serious issue of data privacy risks. This article first examined the development of mobile payment in China, and the factors responsible for the heightened privacy risks of mobile payment. It found that the involvement of multiple players in mobile payment and extensive data harvesting contribute to these privacy risks. This article then discussed the transformation process of China's data protection regime, under which China started with a piecemeal approach and is now moving towards a principle-based framework. At present, China's data protection regime is mainly comprised of the Cybersecurity Law and relevant regulatory rules

273. GDPR, Article 83(5)-(6).

274. A piggyback mechanism of this kind has been employed for the bringing of private securities litigation in China. For a detailed discussed of this mechanism, see Robin Hui Huang, "Private Enforcement of Securities Law in China: A Ten-year Retrospective and Empirical Assessment" (2013) 61 *American Journal of Comparative Law* 757.

275. Paul Nemitz, "Fines under the GDPR" (2017), *CPDP 2017 Conference Book*,https://ssrn.com/abstract=3270535

such as the 2020 PBOC Specification, which together set out the key regulatory elements such as the concept of personal information, the obligations for data controllers and processors, as well as the principles of the FIPs.

By examining the experiences of some overseas jurisdictions, including the US, the EU, Singapore and Hong Kong, this article found that China's current regulatory approach bears more resemblance to that of the EU. The 2018 SAMR Specification (2020 Revision), as a comprehensive guide to personal data security and privacy, substantially follows the GDPR's regulatory structure. China's current regulatory regime strengthens the standard of privacy protection and addresses a series of privacy issues arising in mobile payment, such as target advertising and online tracking. Despite China's efforts to enhance data privacy protection in the digital age, more needs to be done. This article made the following observations and suggestions. Firstly, there are some remaining issues, including, among others, the ineffective requirements of consent and disclosure, the ambiguous principle of purpose limitation, and the limited applicability of the principle of data minimisation. Secondly, a unified law and a unified enforcement agency should be established to reduce the fragmentation of laws, strengthen consistency in enforcement, simplify the regulatory environment, and reduce unnecessary costs and administrative burden. Finally, both private enforcement and public enforcement should be strengthened to compel data controllers to comply with the regulatory requirements.