COMMODIFYING DATA: Analyzing Legal Regulations on Foreign Digital Payment Systems

A Comparative Analysis Between the United States and the People's Republic of China

Emmeline Nettles

International Affairs Program

University of Colorado, Boulder

Defense Date: October 27, 2023

COMMITTEE

Thesis Advisor: Dr. Lauren Collins, Center for Asian Studies

Honors Council Representative: Dr. Rob Wyrod, Department of Women and Gender Studies; International Affairs Program

Outside Reader: Dr. Svet Derderyan, Department of Political Science

Dedication & Acknowledgements

The author would like to dedicate this paper to Cody Wren Morang and his mom, Dr. Lauren Collins, without whose passion and expertise in the subject matter this research likely would not exist. This paper is also dedicated to the memory of Colonel Albert A. Nettles, whose enormous collection of National Geographic magazines instilled in me the love of cultural research and exploration.

I am extremely grateful to the staff at Cyber Statecraft Initiative, and the Young Global Professionals Program. The research skills and policy knowledge I gained were integral in the formation of this paper. Many thanks to Dr. Doug Snyder, who supported this paper in its developing stages. Finally, I would be remiss to not mention my parents. Their support throughout my college career has enabled me to explore and develop my passion for research.

Table of Contents

List of Acronyms

California Consumer Privacy Act – CCPA

Council on Foreign Investment in the United States – CFIUS

End User Licensing Agreement – EULA

European Union - EU

Federal Trade Commission – FTC

General Data Protection Regulation – GDPR

Gramm-Leach-Bliley Act – GLBA

Nonpublic Personal Information – NPI

People's Republic of China – PRC

Personal Information Protection Law – PIPL

Personally Identifiable Information – PII

United States – US[1]

[1] Following Chicago's Manual of Style, United States will be abbreviated in this paper as US, not U.S.

List of Figures

Charts

Tables

Diagrams

Introduction

"*Amy shows her unique Alipay code and has it scanned. More than 60% of the transactions processed by Alipay are done on mobile devices.*"[2]

Digital payment platforms are increasing in popularity around the world[3]. Globally, 2/3rd of adults made or received a digital payment in 2022 alone[4]. In the People's Republic of China (PRC)[5], e-commerce transactions account for "more than 38% of the country's GDP" in 2022[6]. Digital payments come with many conveniences and their growing popularity has facilitated an increasing integration of various sectors of production and consumption, resulting in the growing necessity for people worldwide to make use of one or several of the existing digital payment platforms. To use these platforms, however, users must give up personally identifiable data. Akin to a pay-to-play system[7], users "pay" with their personal data to gain access to digital payment platforms to "play" various transactions. This data includes linking banking information, contacts, and consumer practices and behaviors, as well as noting the geographic sphere in which the consumer operates [8].

---

[2] *Daily Life with Alipay*, 2016, https://www.youtube.com/watch?v=QlW60frlH6w.
[3] Marina Pasquali, "Topic: E-Commerce Worldwide," Statista, November 28, 2022, https://www.statista.com/topics/871/online-shopping/.
[4] World Bank, "COVID 19 Drives Global Surge in use of Digital Payments", June 22, 2022., https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments
[5] Throughout this paper, the People's Republic of China will serve as the term for China's government. In cases where political party doctrine is necessary to differentiate, the Chinese Communist Party (CCP) will be used to specify.
[6] Yihan Ma, "Topic: E-Commerce in China," Statista, November 17, 2022, https://www.statista.com/topics/1007/e-commerce-in-china/.
[7] Sean Herman, "Council Post: Should Tech Companies Be Paying Us For Our Data?," Forbes, accessed January 22, 2023, https://www.forbes.com/sites/forbestechcouncil/2020/10/30/should-tech-companies-be-paying-us-for-our-data/.
[8] Holly Stanley, "What Is Customer Data? Definition, Collection Methods, Trends and More," Shopify Plus, August 9, 2022, https://www.shopify.com/enterprise/customer-data.

There are two main digital payment systems used by Chinese consumers and tourists that have begun expanding into the global digital payment marketplace in recent years. These are Alipay and WeChat Pay. These two companies provide the top digital payment systems developed and used in the People's Republic of China (PRC)[9].

Due to the popularity and frequent use by Chinese consumers of these platforms, international vendors now want access to these platforms as well to allow Chinese consumers to pay for their products. Beginning in 2010[10], merchants outside of the PRC started to expand their online retail sales through Alipay's Global Merchant Portal[11] and in 2017, Stripe became one of the early US fintech companies to partner with Alipay and WeChat Pay, offering digital merchants the ability to accept digital transactions from Alipay and WeChat Pay[12]. Now the platform is becoming increasingly accessible for international consumers and in 2023 the platform is continuing to see increased growth for international consumers both within and outside of the PRC. In 2018 Alipay launched "Tour Pass", a digital payment tool designed to allow foreign nationals visiting Mainland China without a Chinese bank account or ID to utilize Alipay[13]. At the time of writing, both Alipay and WeChat Pay require Chinese bank accounts for consumers using their services outside of the PRC.

[9] "Infographic: China's Most Popular Digital Payment Services," Statista Daily Data, July 8, 2022, https://www.statista.com/chart/17409/most-popular-digital-payment-services-in-china.
[10] In 2010, American e-commerce platform Vendio was acquired by AliBaba to support a global B2B2C model between the US and China. While Vendio is no longer operational, the partnership has now transformed into a collaboration between AliBaba North America and MoreCommerce.
[11] "Alipay Global Merchant Portal," accessed January 31, 2023, https://global.Alipay.com/platform/ihome.
[12] https://www.reuters.com/article/ctech-us-stripe-partnerships-china-idCAKBN19U10S-OCATC
[13] "Alipay for Foreigners || How to Use Alipay (In and Out of China)," LTL Beijing, February 20, 2022, https://ltl-beijing.com/Alipay-for-foreigners/.

With this growing global use of digital payment systems, and no sign of a return to more analog methods of financing, the legislation of financial institutions must be modernized to meet the concerns of the new digital financial space. Rules for behavior surrounding data privacy have become further fragmented by the increasing complexity of digital and technological services, with different countries, and even the states or provinces within them, having distinct and different regulations and methods for ensuring data privacy. With the growing presence of transnational and foreign digital payment systems, we come to the crux of the issue I seek to address with this paper.

Research Question

Is there existing legal framework within the United States that is violated by the data collection policies of PRC-origin digital payment platforms?

Rather than demonstrating what cases of abuse could already exist, my research assesses whether the existing legal framework to protect personal data under US law is violated by foreign digital payment systems, using systems based in the PRC. Furthermore, irrespective of abiding by US laws, I intend to examine the US legal framework against a select number of these systems to see if the framework requires digital payment systems to act in good faith to protect US consumers using PRC digital payment platforms. I will be using Black's Law Dictionary to define "good faith" as "Sometimes legally binding due diligence around the effort made, information given, or transaction done, honestly, objectively, with no deliberate intent to defraud the other party. Yet, this does not cover a sin of omission, something done or not done in

negligence. Known also as bona fides, implied by law into commercial contracts…"[14]. In this paper, when a company or law is referenced as acting or enforcing good faith, it is implied that the act or enforcement of good faith is in direct relation to data privacy of consumers.

In this project, I define legal framework not just as legislation and regulations, but as the sum of legislative actions, regulatory agencies, legal jurisdiction, and parties with vested interests, including laws and norms, both domestic and international.

If it is the case that the existing legal framework allows companies to act in bad faith to prevent the procurement and possible dissemination of personally identifiable information (PII) in the PRC via transnational data collection by PRC-origin digital payment platforms under the PRC, I shall put forth policy recommendations for the Federal Trade Commission (FTC). These recommendations will emphasize the importance of enforcing digital payment platforms to abide by stronger US consumer privacy protection laws.

Additionally, I will put forth recommendations that US government adopt greater restrictions towards the permissibility of digital payment platforms transferring personally identifiable consumer data outside of US federal jurisdiction. The US Constitution states, under Article III Section 2, that US federal jurisdiction oversees cases between two or more states, cases between the US government and foreign governments, cases of maritime law, and cases involving public officials at the federal level[15]. I recommend that the United States require each digital payment platform allowed to conduct business within the recognized borders of the United States state, in plain terms, any legal obligation or requirement the privately owned

[14] "GOOD FAITH Definition & Meaning - Black's Law Dictionary," The Law Dictionary, October 19, 2012, https://thelawdictionary.org/good-faith/.
[15] "Article III," LII / Legal Information Institute, accessed February 18, 2023, https://www.law.cornell.edu/constitution/articleiii.

enterprise has with a foreign government involving the user data and or consumer database of the enterprise. An example of effective federal legislation can be found in H.R. 3910, also known as the Safeguarding Non-bank Consumer Information Act. Introduced in June 2021, the bill "…directs the Consumer Financial Protection Bureau to establish administrative, technical, and physical safeguard standards applicable to a consumer data aggregator…also gives the bureau enforcement authority regarding violations of this bill…"[16].

Background

The world of data security is a vast, interconnected web of various governments, corporations, and users themselves. The exponential growth of a digital ecosystem has often put innovation before legislation. Although financial data protection, similar to health care data, has historically been one of the better regulated facets of the ecosystem[17], legislation is struggling to keep up with rapid advancements in financial technology, or fintech. According to a 2022 Global Financial Stability Report by the International Monetary Fund, traditional financial intermediaries are quickly needing to cooperate with digital banking systems to maintain their consumer base and remain competitive. These fast digital transitions often come at the expense of thorough regulatory behaviors guiding this shift[18]. This is referred to as the "pacing problem", where technology innovates at a faster pace than government can regulate[19]. And it is a problem

[16] Stephen F. [D-MA-8 Rep. Lynch, "All Info - H.R.3910 - 117th Congress (2021-2022): Safeguarding Non-Bank Consumer Information Act," legislation, June 15, 2021, 2021-06-15, https://doi.org/10/all-info.
[17] "Financial-Data-White-Paper-_-1013_fin.Pdf," accessed February 18, 2023, https://cfsi-innovation-files-2018.s3.amazonaws.com/wp-content/uploads/2020/10/14142025/Financial-Data-White-Paper-_-1013_fin.pdf.
[18] "Fast-Moving FinTech Poses Challenge for Regulators," IMF, April 13, 2022, https://www.imf.org/en/Blogs/Articles/2022/04/13/blog041322-sm2022-gfsr-ch3.
[19] "The Pacing Problem and the Future of Technology Regulation | Mercatus Center," August 8, 2018, https://www.mercatus.org/economic-insights/expert-commentary/pacing-problem-and-future-technology-regulation.

that continues to persist. For example, in 1999, Microsoft was the subject of a landmark antitrust case; today, in 2023, Google is now in the same position[20]. To understand this concept of rapid digitization, it is important to explain the brief history of online data security and technological innovations in fintech. Although there is currently active legislation that works to secure PII in the financial sector, the regulations are insufficient for the growing digital market and rise in e-commerce and digital banking.

The United States

"*A person should not have to have an advanced law degree to avoid being taken advantage of by a multibillion dollar company…*" Parks and Rec

Data security in the US has been primarily based upon policy suggestions and recommendations from corporate entities in fintech. In the US corporate ownership of consumer data is governed by each company through providing their own End User Licensing Agreement (EULA) and Privacy Policy to consumers who choose to use their platforms. Yet even company-specific regulations can be a complicated and shifting ecosystem through mergers and acquisitions (M&A). M&A are defined by Investopedia as "[a] term that describes the consolidation of companies or assets through various types of financial transactions, including mergers, acquisitions…and management acquisitions". In Aynne Kokas's book, *Trafficking Data: China's Quest for Cyber Sovereignty,* Kokas highlights the issue of a lack of an oversight regulatory body for data security policies. She does note that the Council on Foreign Investment in the United States (CFIUS) is the current federal oversight for company acquisitions, but this

[20] Miles Kruppa and Dave Michaels, "Google's Defense in Landmark Antitrust Case Hinges on Lawyers Who Took on Microsoft," WSJ, accessed October 1, 2023, https://www.wsj.com/tech/googles-defense-in-landmark-antitrust-case-hinges-on-lawyers-who-took-on-microsoft-3c1d5059.

body is tasked primarily with investigating "who" is acquiring "what", rather than the state of the company's EULA and Privacy Policy[21].

With innovation rapidly surpassing legislation, the fintech world, for some time, was largely self-governable[22]. Today, with the number of US digital transactions continuing to rise, the urgency to adopt a legal framework for data protection within the US is rising as well.

Although both WeChat Pay and Alipay abroad are methods for Chinese tourists to access foreign merchants, the integration of these payment platforms must be scrutinized. Citcon is a US-based integration service, connecting US merchants and businesses to Chinese consumers through its services via digital payment platforms. Two of these platforms are WeChat Pay and Alipay. Currently, Citcon is still slow in its North American deployment, used almost exclusively in regions and businesses with a large preexisting Chinese tourist community. Due to its limited scope and focus on US merchant to Chinese consumer transactions, Citcon's record will not be used in initial analysis of assessing US legislation of foreign data transfers[23].

State vs Federal Regulations

The United States system of government is distinct, with a framework for developing regulations that is quite different from other nations, including the PRC. In the US, Federal and State legislation are the two primary levels of government that concern themselves with the

[21] Kokas, Aynne. "Trafficking Data." Oxford University PressNew York, September 22, 2022. https://doi.org/10.1093/oso/9780197620502.001.0001.; This gets complicated when some company's have this data because they themselves are the 3rd party referenced in a different company's EULA
[22] "Fast-Moving FinTech Poses Challenge for Regulators."
[23] Tricia Taggart, "CITCON Brings Alipay and WeChat Pay to North America," Citcon, February 22, 2017, https://citcon.com/citcon-brings-alipay-wechat-pay-north-america/.

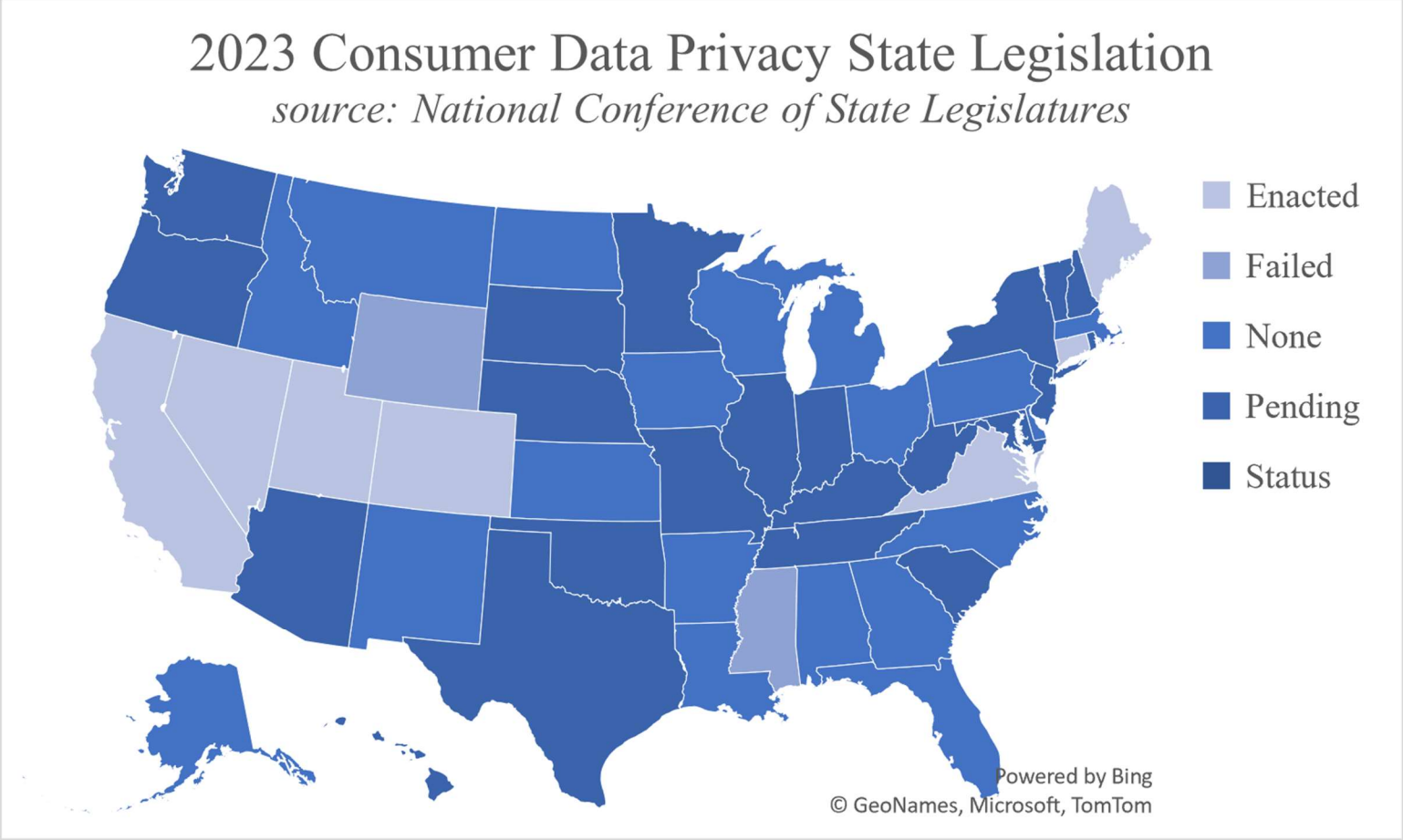
protection of data being circulated in, and exported out of, recognized borders[24]. These borders are specifically internationally recognized as national, geographic borders of sovereign jurisdiction of the US. Through Federal regulation, all US territory is subject to such measures. Through State regulation, only within that state's borders do such measures apply. When it comes to foreign companies seeking to do business in the United States, they are first entering a new national territory, not just each state they choose to operate in.

In 2021, Thorin Klosowski, then editor of the New York Time's Wirecutter, a product review blogging component of the newspaper, wrote an article on the state of data privacy in the US. The article takes aim at the disjointed, multitudinous landscape of current federal privacy laws, and notes "…data collected by the vast majority of products people use every day isn't regulated…no federal privacy laws regulating many companies, they're pretty much free to do what they want…" The data economy, the market for the sharing and collection of people's data, is boosted by the lack of data protection laws. There is no incentive for a business profiting from data collection and retention to no longer have this flow of capital without proper legislation. And, as Klosowski goes on to point out, although some states have privacy laws, and others are on their way, individual state legislation will further muddy the waters of privacy compliance and could drive data-mining companies to areas with less-strict legislation. Not to mention that consumers themselves will most likely not want to navigate on a per state basis what rights and privacy protections they may or may not have. "With the wide range of different laws, it is easy to see how people get confused."[25].

[24] In the case above, when referring to borders, this paper differentiates between state borders within a sovereign country that is made up of these individual states, and national borders, wherein any data from within the borders passes over the borders, will now be considered a transnational data transfer.
[25] "The State of Consumer Data Privacy Laws in the US (And Why It Matters) | Wirecutter," accessed September 19, 2023, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

The limited success of state legislation on this issue should still be considered a success. The California Consumer Privacy Act, considered the most comprehensive state legislation in the US, is a testament to the effectiveness of thorough legislation that returns the right of use to the control of the consumer. Colorado, Virginia, and Utah have legislation for data privacy as well; however, each state has areas of focus and different underlying interests that bleed into each individual legislation. Consumers within the United States ought to have a right to privacy throughout the United States. And businesses, too. To further investment in the digital financial landscape within the US, legislation that tasks businesses with consumer protections should be easy-to-follow and require simple compliance. Fifty individual and unique state-level laws cannot do this. One, or at least, fewer than fifty, federal law[s] can achieve this. Protection of a consumer's privacy and their right to control their personal data should not be seen as being at odds with conducting business; rather, it gives the US consumer the conscious choice of participating in the growing digital economy with an understanding of how this landscape is laid out.

State Legislation in the United States



Map of the United States Depicting State Legislation on Data Privacy as of 2023

(credit: Emmeline Nettles)

This map shows the 2023 United States (excluding territories and the District of Columbia) legislation of Consumer Data Privacy at the State level. Three states introduced legislation in 2023 that failed, nineteen have introduced no legislation, seven states have relevant legislation that was previously enacted, and twenty-six states have legislation currently pending.

Row Labels	Count of Law		
Arizona	2	Oklahoma	1
California	2	Oregon	4
Connecticut	4	Rhode Island	2
Hawaii	5	South Carolina	2
Illinois	8	South Dakota	1
Indiana	2	Tennessee	4
Kentucky	1	Texas	2
Maryland	4	Utah	1
Minnesota	7	Vermont	1
Missouri	1	Virginia	2
Nebraska	2	Washington	3
New Hampshire	1	West Virginia	3
New Jersey	14	**Grand Total**	**103**
New York	24		

Table Showing the Number of States with Existing or Pending Legislation as of 2023

(credit: Emmeline Nettles)

This table shows all the states in 2023 that had legislation related to Consumer Data Privacy "Enacted" or "Pending". States with no legislation or failed legislation, as well as territories, were not included in the analysis. For more information, including to view legislation from US territories regarding consumer data privacy, please visit the National Conference of State Legislatures.

In 2023, there were 111 individual or joint resolutions introduced or previously enacted at the state level focused on consumer data privacy. New York alone has been responsible for introducing 24 bills to its state legislature. The legislation around the country ranges from protection of children's online data, biometric and genetic information privacy, and general protections for consumers and their privacy. Four states, California, Colorado, Virginia, and

Utah have passed State Data Privacy Laws, with all but Utah's enacted[26]. With more than 60% of state legislatures currently pushing for some form of consumer data protection, and two states themselves campaigning for protection at the federal level, the United States Congress is in a good spot for starting discussions around what a federal consumer data protection law would look like.

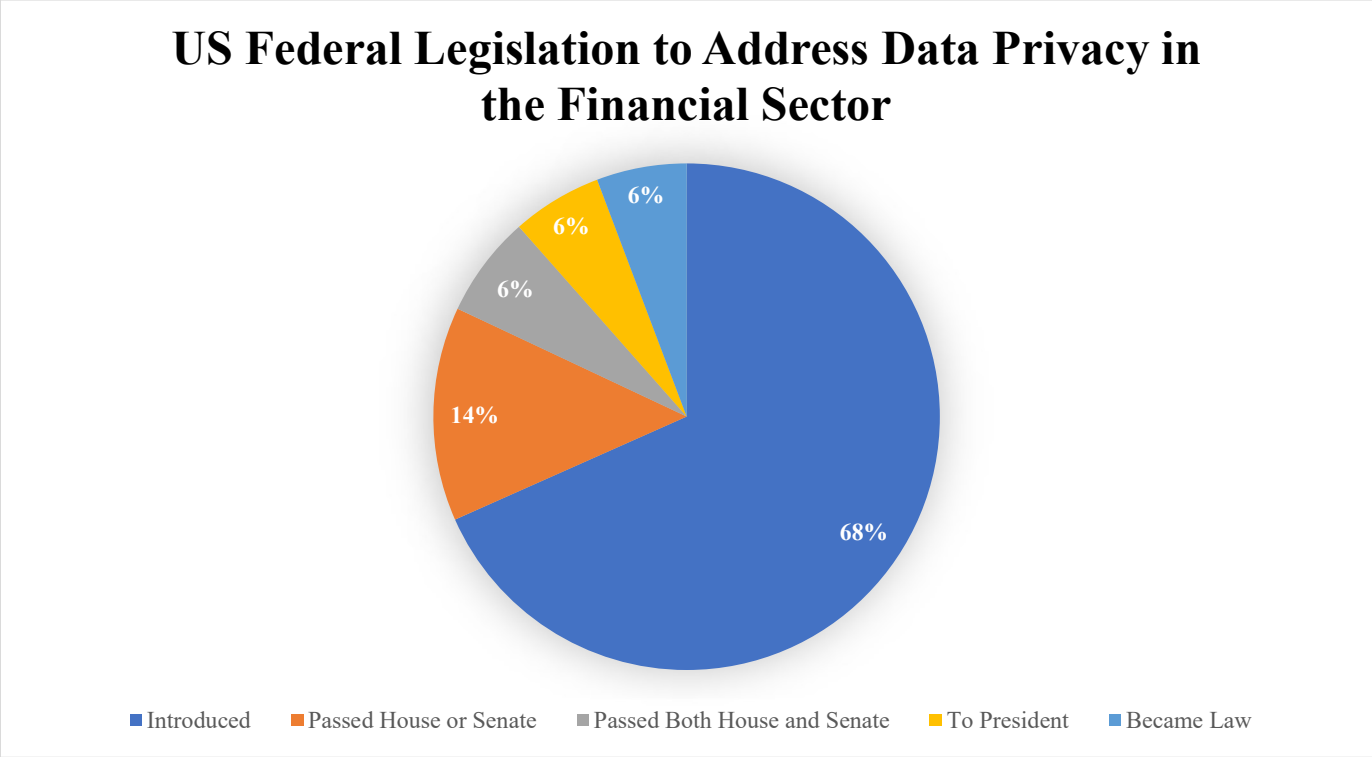
My argument for federal policy around data collection and retention from within the US to outside national borders stems from both the success of state legislation[27] but also concerns around balancing a decentralized internet with decentralized legislation. Although it may seem counterintuitive to have encompassing regulations specific to a whole country when it comes to regulating the Internet, and, at the risk of sounding jingoistic, these 50 states, and territories, make up the United States. Such federal policy around consumer data protection is not concerned with removing or diminishing state-held power; rather it is my hope that these recommendations serve to grant equal rights and protections across all of the US. There is enough overlap with many states with enacted or pending legislation that national-level policy may appear redundant; however, in order to ease the workload of federal compliance, a policy at the federal level will work directly with CFIUS and State Department requirements, rather than being scrutinized at each state-level, and/or tasking states with ensuring compliance with multiple federal directives.

Federal

At the Federal level, the US is severely lacking in regulatory oversight of digital payment systems, and, at the time of this writing, provides very little framework to support users in

[26] Utah's Consumer Privacy Act will be enacted in December 2023
[27] The CCPA being cited in Alipay TC

protecting and securing their own data[28]. What financial oversight currently promulgates throughout the US is focused on traditional financial practices of limiting bank monopolizations and investigating fraudulent practices[29]. The battle to secure finances within the US must include the fight to secure what is fast becoming considered the most valuable resource[30]: user data.



[31]

Pie Chart Describing the Total Federal Legislation on Data Privacy since 1966

(credit: Emmeline Nettles)

[28] "New Treasury Report Shows Fintech Industry Requires Additional Oversight to Close Gaps, Prevent Abuses and Protect Consumers," U.S. Department of the Treasury, January 23, 2023, https://home.treasury.gov/news/press-releases/jy1105.
[29] "Financial-Data-White-Paper-_-1013_fin.Pdf."
[30] *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, 2022, https://www.youtube.com/watch?v=CUYARR7KSgg.
[31] Search: "data privacy" AND "financial"

A quick look at Congressional work towards developing a federal framework around data privacy in the financial sector reveals that of the 190 bills introduced to Congress since 1997, 14% passed one Chamber, 6% passed both the House and the Senate, and only 6% of those introduced were signed into law. In the 26 years of records available, only 16 laws have been signed to address the topic of data privacy. During that same range of time, since 2000 to present, the American Civil Liberties Union has tracked over 50 cases concerning Privacy and Technology processed in US courts, including district courts and the US Supreme Court[32]. While neither broad result indicates the amount of foreign presence overall, I argue that there is now a strong degree of precedence to begin the development of a federal framework that protects the right to privacy and protection of PII both via domestic and transnational exchanges.

Two Acts in particular, the Gramm-Leach-Bliley Act and the Dodd-Frank Act provide protection for personally identifiable information, specifically focusing on protection of financial information. These protections are intended to be achieved through regulation of domestic banking institutions.

Gramm-Leach-Bliley Act

The Financial Services Modernization Act of 1999, known also as the Gramm-Leach-Bliley Act and hereafter in this paper referred to as the acronym GLBA, issued standard rules and regulations to reform and modernize financial services and institutions. Title V of the GLBA, "Privacy", "declares it is the policy of Congress that each financial institution has an

[32] https://wp.api.aclu.org/court-cases?issue=privacy-technology#all_content

affirmative, continuing obligation to respect the privacy and to protect the confidentiality of customer nonpublic personal information."[33].

The Gramm-Leach-Bliley Act (GLBA) is considered to be the current national-level law in the US specific to consumer data privacy. Enacted in 1999, it has not been successfully updated since[34]. The goal of the GLBA is to modernize compliance with consumer privacy rules and more clearly define the roles of regulatory agencies in enforcing this compliance[35]. The Privacy of Consumer Information Rule, hereafter referred to simply as the Privacy Rule, is under the jurisdiction of the Federal Trade Commission (FTC).

The Compliance Guidelines, published and enforced by the FTC, outline which entities are required to comply with the GLBA and what that compliance involves. Alipay and WeChat Pay would be subject to the GLBA, as they fall under the category of a "financial institution" as defined in the Act: "The Privacy Rule applies to businesses that are "significantly engaged" in "financial activities"." Engagement in financial activities is considered by the Guidelines as "significant" when there is a formal arrangement and a high volume of engagement in rendering financial services. Furthermore, commonly used digital payment systems, such as PayPal and Venmo are classified themselves as financial institutions, thus setting a precedent for other

[33] "PLAW-106publ102.Pdf," accessed February 18, 2023, https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf.
[34]An amendment, National Association of Registered Agents and Brokers Reform Act of 2013, failed to be enacted. Randy [R-TX-19 Rep. Neugebauer, "H.R.1155 - 113th Congress (2013-2014): National Association of Registered Agents and Brokers Reform Act of 2013," legislation, September 11, 2013, 2013-03-14, https://www.congress.gov/bill/113th-congress/house-bill/1155.
[35] "Gramm-Leach-Bliley Act," Federal Trade Commission, June 16, 2023, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act. How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act (pdf)

digital payment systems[36]. Thus, the GLBA will be the federal legislation the case studies of Alipay and WeChat Pay will be assessed against.

Under the FTC's purview, the GLBA Privacy Rule protects Nonpublic Personal Information (NPI). The Guidelines consider information that can be obtained from public disclosure, including phone numbers and other personally identifiable information (PII). The GLBA requires financial institutions to provide notice of how NPI is collected, disclosed with affiliates and other third parties, and the security measures taken to protect NPI. A glaring absence in these required privacy notices is storage of NPI by these financial institutions. The whole of the Act, including the Privacy Rule, does not require covered financial institutions to disclose where NPI data is stored, for how long this data is retained, or what justification necessitates the retention. In the absence of regulating data storage disclosure, there are also no requirements regulating where, for how long, and why NPI can be stored. Without requiring these factors of data processing to be regulated, "…companies have the all legal right in the world to do what they're doing and no financial incentive to stop it…"[37]. It is not financially beneficial for companies to protect user data, both NPI and PII alike, beyond what they are legally obligated to do. Therefore, legislation must be updated to meet the privacy issues of an increasingly globalized and digitized financial space.

Although this law is sorely in need of being updated for the 21st Century, it has proven its mettle against digital payment systems in the past. In 2018, a case was brought against PayPal,

[36] "PayPal Settles FTC Charges That Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act," Federal Trade Commission, February 27, 2018, https://www.ftc.gov/news-events/news/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information-consumers-about-ability-transfer-funds.
[37] Joe Toscano, "Data Privacy Issues Are The Root Of Our Big Tech Monopoly Dilemma," Forbes, accessed September 9, 2023, https://www.forbes.com/sites/joetoscano1/2021/12/01/data-privacy-issues-are-the-root-of-our-big-tech-monopoly-dilemma/.

including complaints of data privacy in Venmo's handling of financial information. The complaint argued that Venmo misled users about their data privacy when using the payment service. Furthermore, the FTC also claimed that PayPal failed to uphold the Privacy Rule of the Gramm-Leach-Bliley Act[38]. This case is evidence that the federal body of the FTC is able to take on large payment systems already in place in the US. And yet, there is certainly more room for regulation of these digital, financial behemoths beyond the current scope of the Act.

Federal Trade Commission

The Commission, established in 1914, under President Woodrow Wilson, considers its mission is "to protect consumers and promote competition". According to the FTC, their directive under the FTC Act "empowers the agency to investigate and prevent unfair methods of competition, and unfair or deceptive acts or practices affecting commerce…and protecting consumers."[39]

The FTC is considered to be the main federal body responsible for data privacy and should be responsible for implementing any federal legislation that would be enacted for legislation on consumer data. Indeed, of the few laws that exist at the federal level pertaining to data privacy, namely the Gramm-Leach-Bliley Act and the Dodd-Frank Act, the FTC is named as the enforcement body for ensuring compliance with the laws. Although this paper argues that the GLBA is outdated, there has been successful work done by the FTC to enforce data protection as a regulator body onto digital payment systems, such as in the case of Venmo.

[38] "PayPal Settles FTC Charges That Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act."
[39] "What the FTC Does," Federal Trade Commission, September 11, 2018, https://www.ftc.gov/news-events/media-resources/what-ftc-does.

The FTC also is the regulatory agency and coordinating body for the SAFE Web Act, which works to protect consumers from global threats, by partnering with foreign governments and relevant agencies to investigate cases of fraud and other financial protection concerns. Enacted in 2006, the SAFE Web Act has seen amendments since then, most notably to extend investigative abilities into spyware outside of the United States. This law is a further example of the FTC's importance, and more so, their ability, to regulate data protection in a digital, global landscape[40].

Since the FTC is considered the federal leader for data privacy[41], it is important that any recommendations and policy amendments take into account the triumphs and tribulations the FTC has faced in supporting consumer data privacy in the United States.

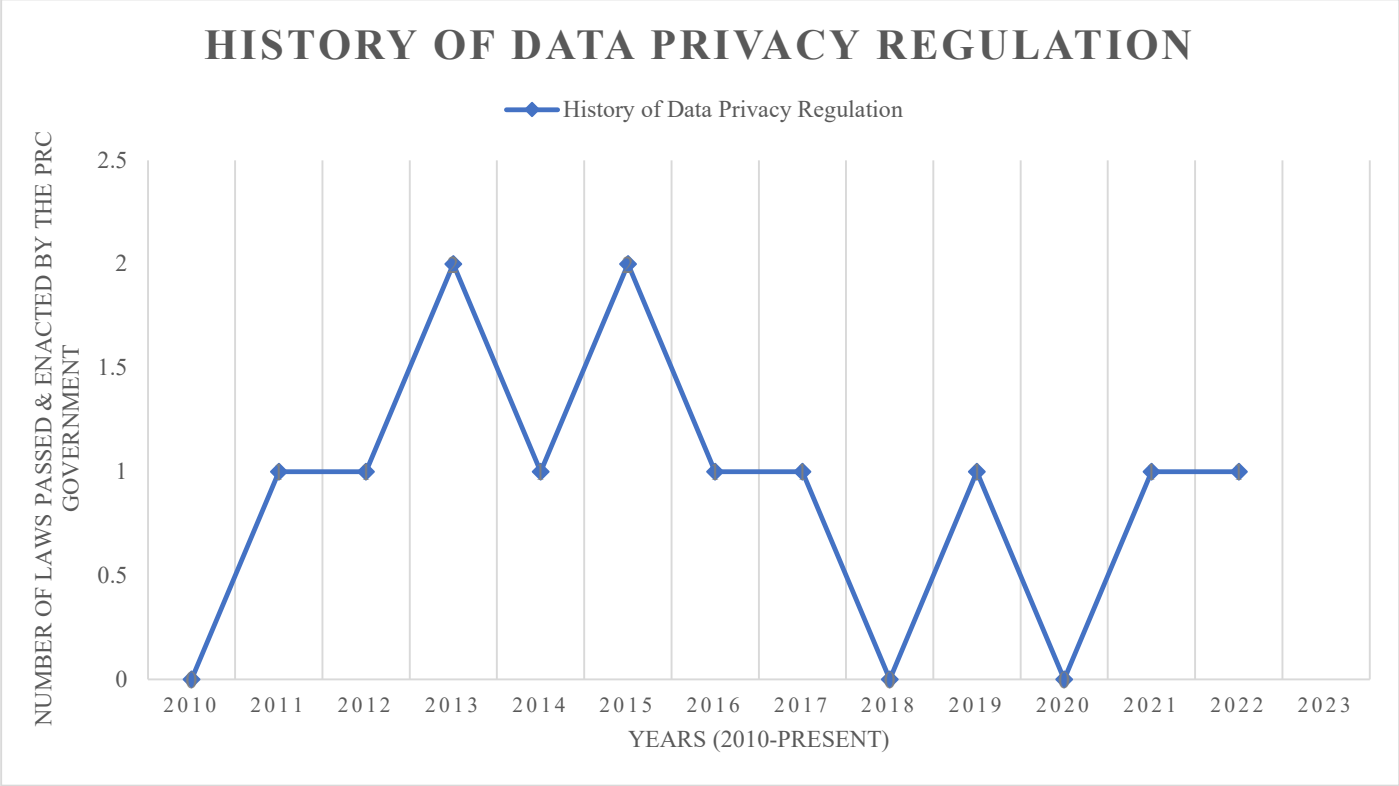
The People's Republic of China

History of Data Collection Norms and Behaviors

Government involvement in managing personally identifying data has a long history in China. Prior to the end of imperial China in 1912, during the Qing dynasty (1644-1912), people in China were recorded via their *dang'an* (档案) or personal records of demographics and activities throughout one's life. Methods of citizen records predate the Qing dynasty system; however, due to each succeeding dynasty often destroying previous records of former dynasties and inventing new methods of data collection, the historical focus will home in on only the Qing

[40] "Letter of the Federal Trade Commission to the U.S. House of Representatives, Subcommittee on Consumer Protection and Commerce, on the U.S. SAFE WEB Act," Federal Trade Commission, October 31, 2019, https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-federal-trade-commission-us-house-representatives-subcommittee-consumer-protection-commerce.
[41] "The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation," Belfer Center for Science and International Affairs, accessed October 4, 2023, https://www.belfercenter.org/publication/role-federal-trade-commission-federal-data-security-and-privacy-legislation.

dynasty's central government (Zhang, 2004). Maoist era China continued to use the dang'an system, as well as introduce the hukou, or household registration system, among other initiatives.



Timeline Chart Depicting Major Data Privacy Regulation since 2010 in the PRC

(credit: Emmeline Nettles; New America's 'Evolution of China's Data Governance Regime')

This timeline, modeled after the Evolution of China's Data Governance Regime by New America, a progressive think tank with a focus in data and cyber, shows the continued investment in data governance by the PRC[42]. This chart is not indicative of the entire data regulation landscape during this period; rather, it focuses on relevant legislation passed by the central government of the PRC that has had or has the potential to have long-reaching impacts,

[42] "The Evolution of China's Data Governance Regime: A Timeline," New America, accessed October 1, 2023, http://newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline/.

across the whole country and extending across its national borders. These laws include the 2017 PRC's Cybersecurity Law, of which data privacy is only part of the focus, to the 2022 Personal Information Privacy Law, the main regulation being the restriction of cross-border data flows out of the country's borders. To match the rapid digitization following its industrialization in the 90s as one of the Asian Tigers, China did not wait to see if companies would self-regulate in a manner acceptable to the ruling party.

The United States and China present opposite ends of the spectrum on best practices for regulating data privacy. On the side of the US, laws from the last century, if not even older, govern companies collecting data through tools that were mere science fiction at the time of enactment, such as Large Language Models and Artificial Intelligence. The laws of China speak to a government with the intense desire to maintain order and control with a high degree of centrality, despite the internet being largely decentralized. In both cases, consumers are on the losing end of the stick. For the US, appreciation and growth of the free market make way for companies to profit from user data, while, in China, the government has the potential to retain personal data. The PRC's retention of PII is not the focus of this paper, though it should be noted that much of today's self-censorship in China originates from the fear of reprisal by the PRC government[43].

Personal Information Protection Law

In 2021, the PRC passed into law the Personal Information Protection Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa* 中华人民共

[43] "China: Freedom on the Net 2022 Country Report," Freedom House, accessed September 29, 2023, https://freedomhouse.org/country/china/freedom-net/2022.

和国个人信息保护法). Known generally as the PIPL, this law offers protection for personally identifiable information of Chinese nationals within the PRC's borders (DigiChina, 2021). Though the PIPL is intended to support personal privacy, the law specifically outlines six broad categories of exceptions where informed consent does not have to be obtained from the persons involved (PIPL, Article 13, 2021). The argument to support these categories is that any unauthorized data collection outside the six specifications would be considered illegal under the PIPL (DigiChina, 2021). Furthermore, the law makes categorical allowance for public health and emergency situations. Article 12 of the PIPL encourages the State to participate in the formation of international norms and rules around data privacy (DigiChina, 2021). Though the PIPL is intended to support personal privacy, the law specifically outlines six general categories of exceptions where informed consent does not have to be obtained from the persons involved (PIPL, Article 13, 2021). The argument to support these categories is that any unauthorized data collection outside the six specifications would be considered illegal under the PIPL (DigiChina, 2021). Furthermore, the law makes categorical allowance for public health and emergency situations.

Based on my analysis I argue that the category of "information disclosed by persons themselves or otherwise already lawfully disclosed…" (DigiChina, 2021) does not denote in what way the persons themselves have disclosed this information. As such, data could be collected by combing through public sites used by Chinese nationals for personally identifiable information with a potential argument from the data collection agency being that the individual publicly disclosed this information themselves.

Rule of Law vs Rule by Law

The notion of Rule of Law versus Rule by Law is a much-discussed concept in studies of the PRC legal system[44]. According to the "Rule of Law" entry in Stanford's Encyclopedia of Philosophy, rule of law is defined as "suppos[ing] to lift law above politics", while rule by law is defined as a "tool of political power"[45]. Rule by law is of the people and by the state, meaning citizens are regulated by state decisions without crossover from either side in the affairs. Rule of law supports democratic representation in governments[46]. The article makes a claim that rule by law is "the state uses law to control its citizens but tries never to allow law to be used to control the state", and references the PRC as a government employing the rule by law methodology[47]. Although the PRC is the oft-cited example, during the era of economic reforms and modernization, then-Premier Zhao Ziyang introduced and supported democratic reforms, seeking to envision the PRC as a "rule of law" nation and state. Though not an unheard-of concept, "rule of law" was not a common practice in any prior iteration of rule in China. During the dynastic ages, the two schools of thought practiced what are known as *lizhi* and *fazhi*. *Lizhi*, practiced by Confucianists, believed that the ruling elite exercised control over doctrine because they were expected to be an ideal example of human behavior. *Fazhi* 法治, coined by Legalist scholars, is the practice of rule by law, intended to maintain societal order and control by the ruling elite.[48]

[44] "Xi Jinping Thought on the Rule of Law," Stiftung Wissenschaft und Politik (SWP), accessed September 19, 2023, https://www.swp-berlin.org/publikation/xi-jinping-thought-on-the-rule-of-law.
[45] Jeremy Waldron, "The Rule of Law," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Summer 2020 (Metaphysics Research Lab, Stanford University, 2020), https://plato.stanford.edu/archives/sum2020/entries/rule-of-law/.
[46] "Rule of Law | Democracy, Human Rights and Governance," U.S. Agency for International Development, September 18, 2023, https://www.usaid.gov/democracy/rule-law.
[47] Waldron, "The Rule of Law."
[48] [Suisheng Zhao.Debating Political Reform in China: Rule of Law vs. Democratization]

To understand norms and rules of behavior, a good first step is assessing the language used to express contentious topics. For example, the promotion and expression of feudalism in the PRC is prohibited. This is inline with the adoption of Marxist ideology during the formation of the Chinese state[49].

As a disclaimer, this report is presented through an analysis of English documents and translated Mandarin Chinese texts and references. An in-depth explanation of the various translation methods and representation of translated information, along with their merits, are beyond this paper's scope. The translation of 法治 to English is defined as both "rule of law" and "rule by law". Wall Street Journal writer Josh Chin explains why translating 法治 as both forms of rule can and do affect etic analysis of the legal framework within the PRC. "…依法治国, or "ruling the country according to law"…dovetails with the nature of the proposed judicial reforms, which aim to give courts independence from local government but still keep them within…Communist Party control." According to an interview conducted by Chin, "'Using 'rule of law' is profoundly misleading, and I think intentionally misleading,' says John Delury".[50]

Why is the awareness of duplicitous translations necessary in understanding the legal framework of the PRC? Because when approaching legislation of foreign investment, having both an emic and etic perspective is important. Due to the distinction between US and Chinese legal norms and behaviors, the avoidance of commonly understood faux pas cannot be assumed

[49] Reem Nadeem, "Government Policy toward Religion in the People's Republic of China – a Brief History," *Pew Research Center's Religion & Public Life Project* (blog), August 30, 2023, https://www.pewresearch.org/religion/2023/08/30/government-policy-toward-religion-in-the-peoples-republic-of-china-a-brief-history/.

[50] Chin, WSJ, fazhi definition; Another interviewee from this article, David Moser, has an essay citing the difficulties of translation and Chinese language acquisition by native English speakers (https://pinyin.info/readings/texts/moser.html)

or expected; rather, they must be regulated and clearly defined, both in protecting US personal data, and to allow cross-border flows of engagement.

Although this paper primarily concerns itself with a comparative analysis of the US and the PRC, my argument that the US legal framework around data privacy is lacking stems from existing stricter regulations on data privacy within the European Union, or the EU. The General Data Protection Regulation, known also as the GDPR[51], is considered the shining example of legislation protecting individuals' rights and data privacy on the Internet. In the years since its implementation, many services and even states and other countries have gone ahead and updated their data collection policies wholesale, citing the GDPR as tangible inspiration for these new directives and regulations[52]. In the forthcoming section on recommendations for an improved US legal framework, I will highlight the specific regulatory processes and behaviors I believe would be both feasible and effective if implemented at the federal level in the US.

Methodology

For my analysis I looked at the End User Licensing Agreements (EULA) of two Chinese digital payment systems, Alipay[53] and WeChat Pay[54], to assess if their methods of data collection and storage would (and should) be permissible within the United States. EULA are considered legal documents wherein the end-user agrees to certain terms and conditions in order to access the services provided by the company they are entering into an agreement with. The Linux Foundation defines a EULA as a "legal contract between a software developer or vendor and the

[51] For further information and a summary analysis of the document: https://gdpr-info.eu/
[52] https://iapp.org/news/a/three-years-in-gdpr-highlights-privacy-in-global-landscape/
[53] "Alipay Global Merchant Portal."
[54] "WeChat Pay," accessed January 31, 2023, https://pay.weixin.qq.com/index.php/public/wechatpay.

user of the software. It specifies in detail the rights and restrictions that apply to the software"[55]. A common example of an end-user is someone who downloads a mobile application on their cell phone to use for themselves. A college student downloading Venmo to pay their roommate for groceries would be considered an end-user of Venmo.

Alipay and WeChat Pay are two PRC-origin digital payment systems with high volumes of users and a successful adoption of the payment services across consumers, merchants, and more. Although these systems are not implemented at a large, whole-scale model, in the US, these systems are proliferating globally. And because these systems are born out of a nation-state with a distinct, and at times opposing, set of norms and legislative rules for behavior, it is important that consumers and merchants in the US recognize that their assumed protections should not be assumed.

I have also selected these case studies because of the rise in economic globalization. With a safer and better regulated virtual economy, the trend of interconnectedness can continue. I do not seek to encourage isolationism of the US economy, but in order to have an economy that puts the safety of its consumers at the forefront, legislation must precede adoption of technologies supported by the data economy. By examining foreign systems, legislative protections can more completely address the issues of differences in norms and acceptable data collection practices, rather than reacting to privacy concerns on a case-by-case basis.

The concerns of data collection and retention around foreign social media platforms such as Tiktok are not unfounded but are perhaps focusing time and resources on a sector of the digital landscape that is a known source of data harvesting. However, the data of social media

[55] "EULA Definition by The Linux Information Project," accessed October 1, 2023, https://www.linfo.org/eula.html.

accounts are only as useful as the data is valid. Financial data contains vast amounts of genuine, personally identifiable information that is required to conduct business or engage with services as a consumer.

Here, to determine policies on data collection, I provide a brief synopsis of the two systems' End User Licensing Agreements (EULA) in the context of the privacy norms outlined in my Theory & Lit Review section. Specifically, I focus on the sections pertaining to Third-Party involvement and Handling of User Data. Using the Personal Identity Protection Law and the PKU Law Database, I show how the data collection policies of Alipay and WeChat Pay are permissible within the PRC. Next, I assess the systems' data policies under the Gramm-Leach-Bliley Act for data privacy requirements in the financial sector. Finally, I also assess the systems using the California Consumer Privacy Act, which is a more modern data privacy protection that has inspired other states to follow suit. The California Consumer Privacy Act, or CCPA, is considered the strongest data protection law in place in the United States. Its emphasis on reinstating data control into the hands of consumers is central to its laudatory fame, as well as its success in businesses falling in line quite easily with legal compliance[56]. In acknowledging that California has done what few policymakers in the US have succeeded in doing, I still consider a federal legislative approach to be most effective against cross-border data collection. The state of California agrees, with the Attorney General recommending that the FTC adopt a federal policy similar to California's state-level one[57].

[56] "A Federal Privacy Law Could Do Better than California's," Brookings, accessed October 1, 2023, https://www.brookings.edu/articles/a-federal-privacy-law-could-do-better-than-californias/.
[57] "Attorney General Bonta: FTC Should Follow California's Example and Adopt Robust Data Privacy Protections," State of California - Department of Justice - Office of the Attorney General, November 21, 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-ftc-should-follow-california%E2%80%99s-example-and-adopt-robust.

As I analyze both EULAs and Privacy Policies in English, it is important to note the caveat that I analyze the language of a legal document that has been translated. To provide further context in my analyses, I also assessed current documentation on global data securities, as the European and North American legal documentations are written in English[58]. These policies are primarily vendor-facing[59], but I believe that their expectations and data collection across borders is relevant to the concern of transnational data transfers of sensitive user data. Additionally, the documentation for Chinese digital payment systems denotes in all documentation that is also provided in English by the entity responsible that "The Chinese version of this Policy shall prevail if there is any inconsistency between the English version and the Chinese version of this Policy"[60]. Nevertheless, any inconsistencies that arise out of translational differences will only serve to further my case that foreign governments, namely the United States federal government, must require these digital payment system corporations and affiliations to plainly define their collection, handling, storage, and transfer of user data that crosses through their digital payment systems.

Acting in Good Faith Under US Legislative Framework

The importance of assessing these case studies as to whether they are acting in good faith is crucial due to these companies not being modeled on US business practices. If the companies, when conducting or offering their services within the United States, act in bad faith regarding US consumer practices because of a disconnect between what is permissible by law and what is

[58] "US Customer Service Information | Legal | Alipay Docs." Accessed February 14, 2023. https://global.Alipay.com/docs/ac/Platform/grygy5.

[59] "Alipay Global Open Platform Membership Agreement | Legal | Alipay Docs." Accessed February 14, 2023. https://global.Alipay.com/docs/ac/Platform/membership.

[60] "协议内容," accessed March 1, 2023, https://render.Alipay.com/p/yuyan/180020010001196791/preview.html?agreementId=AG00000174.

generally considered to be acting in good faith towards consumers, that may not fall under the legally accepted definition of bad faith, but it can undermine consumer trust and business relationships. As Black's Law Dictionary defines it, bad faith is "The opposite of "good faith," generally implying or involving actual or constructive fraud, or a design to mislead or deceive another, or a neglect or refusal to fulfill some duty or some contractual obligation, not prompted by an honest mistake as to one's rights or duties, but by some interested or sinister motive"[61].

There is much debate around the legal definition of "good" and "bad faith" in that a bad faith actor may be subjectively conducting business; however, the determination of a good or bad faith actor is inherently subjective[62]. For the sake of the paper and the following model for determining the case studies as being likely good or bad faith actors, the Black's Law Dictionary definitions of "good faith" and "bad faith" will be viewed as the lone definitions for each term.

Based on the existing framework provided by the Gramm-Leach-Bliley Act (GLBA) and the California Consumer Privacy Act (CCPA), four factors are chosen to assess the case studies and their associated documents. They are assessed for vagueness, whether or not the data collection and retention policies outlined are clear and easily understood and accessible to an average user of the service. They are also examined for the data policies themselves, where the data collected is being stored as well as how long the data is stored and under what pretense. Lastly, the legal jurisdiction under which each case study operates, as well as through what channels users have

[61] "BAD FAITH Definition & Meaning - Black's Law Dictionary," The Law Dictionary, November 4, 2011, https://thelawdictionary.org/bad-faith/.
[62] "Bad Faith Definition," May 16, 2021, https://web.archive.org/web/20210516212921/http://www.duhaime.org/LegalDictionary/B/BadFaith.aspx.

opportunity for recourse or legal action, are also looked at for determining if the systems would act in good or bad faith towards US consumers.

Should one or both systems be enforced to act in good faith under the GLBA, but not under the CCPA, I will classify one or both systems implementation in the US as "needing strong adherence to any and all State, Local, Territorial and Tribal (SLTT) legislation" and recommend that at both the federal and state level, US legislators must adopt policies that safeguard US citizen data.

Should one or both systems be enforced to act in good faith under both the GLBA and the CCPA, I will classify one or both systems implementation in the US as "consistent with the expectations of US operators of digital payment systems"; however, I recommend that any database centers need by these systems for operation in the US, that the Federal Trade Commission must require these centers remain within the US. This process is known as data localization, and it requires that data collected in a certain region must also be stored there, as opposed to transferring that data to be stored outside of its borders. This is a benefit to both domestic data privacy norms and the domestic economy, as it subjects the stored data to local laws and encourages direct business operations within the location[63].

Should neither system be enforced to act in good faith under either the GLBA or the CCPA, I will recommend that the Federal Trade Commission, in coordination with the US Department of Commerce, to look at the possibility of introducing a Privacy Shield regarding Chinese systems collection of US citizen data. The Privacy Shield would be an adoption of the Data Privacy Framework Agreement that exists between the US and the EU and United Kingdom. As defined

[63] "Data Localization Laws: An Emerging Global Trend," January 6, 2017, https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/.

in its overview, the Data Privacy Framework "…share a commitment to enhancing privacy protection, the rule of law, and a recognition of the importance of transatlantic data flows to our respective citizens, economies, and societies…to foster, promote, and develop international commerce"[64]. This framework allows for individual entities, such as private businesses, to self-certify, meaning they individually commit to upholding the Data Privacy Framework. Rather than reinventing the wheel, this framework could be adapted for foreign businesses providing services in the US.

[64] "I. OVERVIEW," accessed October 7, 2023, https://www.dataprivacyframework.gov/s/article/I-OVERVIEW-dpf?tabset-35584=2.

Good Faith Model	WeChat Pay		Alipay	
Gramm-Leach-Bliley Act				
California Consumer Privacy Act				

Empty Good Faith Model Table Used for Analysis of Case Studies

(credit: Emmeline Nettles)

The above table, referred to as the Good Faith Model throughout the remainder of this paper, is a summation of the assessment that will be used with each document of the two case studies. Analysis of case studies will examine both the legality of the services provided, and if they can operate in accordance with US law, both state and federal. In addition, the Good Faith Model will be used to show that, regardless of legal status of operations, that the case studies may or may not operate in good faith towards US consumers. Upon analysis of case studies of both companies and their associated EULAs, each company will be assessed for its acting in good or bad faith against either US law.

Data Collection and Analysis

To examine data collection practices within transnational digital payment systems and their legal framework for data monetization I employed various methods of qualitative analysis and research on existing scholarship on this subject. These research and data collection methods included expert interviews through my involvement with the Atlantic Council and the State of Colorado, an comprehensive literature review of existing scholarly work on the issue, analysis of

existing legislation and two case Chinese company EULAs and associated agreements and notices as case studies, and a review of US and Chinese legislation since the 1990s.

The comparative aspect of this study was also a key part of my analysis, allowing me to juxtapose the legal frameworks of the US and the PRC with respect to data collection and retention in digital payment systems. This approach highlighted the variations and commonalities in global regulations. I also looked at case studies of real-world instances where data collection and retention were subject to legal scrutiny including the 2018 case of Venmo violating the Gramm-Leach-Bliley Act. These cases provide practical insights into how legal frameworks are applied in practice and their implications for transnational digital payment systems.

To understand the current state of affairs for norms of data privacy in the US and the PRC, I engaged with experts through vigorous discussion and lecture to learn the trends and gaps in legislation going on. Aynne Kokas, author of *Trafficking Data: How China is Winning the Battle for Digital Sovereignty*, addressed the concern that Congress is focusing almost entirely on social media as a threat to data privacy, leaving other areas largely unregulated[65]. Although Kokas regards financial data as more protected than the data collected via agriculture technology, there are still gaps, especially when it comes to an increasingly globalized economy. Additionally, through my work as a consultant with the Atlantic Council's Cyber Statecraft Initiative, where I specialized in foreign cybersecurity concerns, I worked with and learned from many experts, including Kenton Thibaut and Bulelani Jili, both specializing in growing Chinese involvement through the digital and tech space. Winnona DeSombre Bernsen, a cybersecurity specialist working with the Atlantic Council and Harvard's Belfer Center, advised me on scope

[65] Kokas, Aynne, "Trafficking Data: How China Is Winning the Battle for Digital Sovereignty", Wilson Center. 2022.

and possible limitations of my research. Namely, she recommended I limit my case studies to a select number of companies[66], and to focus the concern of data privacy to one sector, in the case of this paper, digital finance. Throughout my time with the State of Colorado's Office of Economic Development and International Trade, I consistently engaged with both state and federal legislation to understand the existing frameworks foreign businesses operate within the boundaries of the US and the state of Colorado.

Legal Analysis

The study employs a legal analysis approach to dissect the regulatory landscape surrounding data collection within global digital payment networks. This involves examining international agreements, treaties, regulations, and national laws to identify the legal parameters that govern data monetization. The tools and resources used to meet the parameters of reasonable suspicion were a collection of legislative trends, analysis of existing, relevant US and PRC legislation, domestic and foreign EULAs of both Ali Baba and WeChat, and a comprehensive literary analysis of the norms and rules for behavior throughout modern history of the United States, China, and the EU. Dedoose and Obsidian, both digital, user-created databases, were used to highlight ongoing trends throughout the literary and comparative analyses. Using Dedoose, I created tags, called "codes", to mark important content across the documents being analyzed. The tag "Third-Party Regulations" and "Transfer of Data" were the most populated tags, and "Transfer of Data" highlighted the inconsistencies between legislation and service agreements I expected to find.

[66] Having herself conducted research in the area of corporate compliance, she was aware the lift required for even research into one or two companies.

For legislative trends and analysis of existing, relevant legislation within the United States, I combed through the US Congressional Database to understand current policies as well as policymakers' attitudes towards securing financial PII within the US Within the PRC, the RMSV and PIPL were the two national-level ruling documents I analyzed and assessed for understanding rules for behavior regarding PII. Peking University's Law School hosts a database of all recent major legislative documents produced by the PRC government; however, over the Summer of 2023, PKU Law Database became inaccessible for US institutions and their affiliates. At the time of submission, this restriction remained in place. China Law Translate, a database of translated rulings and legislation from the PRC, is hosted by the Yale School of Law, and provides the translations of the RMSV and the PIPL cited in this paper, as well as links to the original text. Journalist Josh Chin has provided expertise on norms and rules for behavior in relation to PII in and outside of the PRC. The English-version sites of Alipay and WeChat Pay have provided translated versions of their EULAs for both merchants and consumers. I also would like to take a moment to acknowledge I-intelligence's workshop on how to conduct open-source intelligence gathering in Mandarin; because of this training, I was able to access further legal documentation not readily available from either company's site[67].

My literary analysis came from thorough and exhaustive review of existing resources and discussions of my topic. Many of the secondary sources collected for this paper focused on either the e-commerce and digital transaction spaces in an increasingly globalized economy or on cultural attitudes in the United States, China, or the EU on data privacy and what companies and their users are each entitled to. This gap between two heavily discussed topics is precisely why

[67] This is again where I would like to highlight that all documents were either first written in English, translated by the author into English, or I myself used Google Translate and/or DeepL for translation into English from the original Mandarin Chinese.

the policy recommendations provided in this paper are an important starting point for legal discussion.

Analysis & Results

My analysis examined multiple documents related to privacy and data protection policies of Alipay and WeChat Pay. As mentioned in the Methodology section, Alipay and WeChat Pay are two PRC-origin digital payment systems with high volumes of users and a successful adoption of the payment services across consumers, merchants, and more. They are also major factors in economic globalization and the adoption of digital payment systems worldwide. With a safer and better regulated virtual economy, the trend of interconnectedness can continue. Legislation must precede adoption of technologies supported by the data economy.

According to Ant Financial's Privacy Policy, the organization responsible for Alipay and its affiliates, "Your information is stored on a data server located in [Mainland] China." Furthermore, the Privacy Policy does not provide information on how to correct, obtain, or request the deletion of one's own personal data, neither voluntarily submitted by the user nor collected via the service or its affiliates. Ant Financial does describe the types of personal data collected and stored in their data servers; however, the company does not provide information on the length of time for data retention of either active, inactive, nor former users of the service(s). This is especially concerning because of Alipay's new service, Tour Pass.

With Tour Pass, any international tourist visiting Mainland China (excluding Hong Kong SAR and Macao SAR)[68], is able to sign up for a short-term prepaid card, hosted on Alipay's

[68] SAR stands for Special Autonomous Region

system and authorized through the Bank of Shanghai[69]. While the card is only available for foreign tourists within the boundaries of Mainland China, the User Agreement does not discuss data retention or disposal of personal data upon termination of the short term card. The agreement does outline the relationship that the Bank of Shanghai and Alipay enter, one aspect of which involves one party or the other automatically updating user data, such as personal data and changes in banking information. This could potentially mean that once a foreign national travels outside of Mainland China, their user data through Tour Pass may continue to be updated and maintained, all while being stored and processed in a data server within Mainland China.

This paper was the result of a comparative analysis between two nations and their norms, as well as rules for behavior, surrounding the acquisition of personally identifiable information (PII), and how this is expressed in two EULAs for WeChat and Alipay. The analysis is further supported by the use for example of two private companies in the e-commerce and digital transaction industry.

Company A, Alipay, a subsidiary of Ant Financial Group, itself a part of the e-commerce giant, Ali Baba, provides an example of an existing foreign fintech entity operating within the jurisdiction of the United States. Alipay's current presence within the US has been as a financial intermediary for B2B and B2C[70]. US merchants, the precedent of Alipay legally operating in the US for small businesses and organizations (SBOs), have existing agreements with Alipay for the protections of merchant IP in digital transactions. These provide a rough template for how PII

[69] "'Tour Pass' Information Technology Service Agreement," accessed September 19, 2023, https://render.alipay.com/p/c/k2ffmmxp.
[70] B2B stands for "business to business" and B2C stands for "business to consumer". Alipay has allowed for businesses in the U.S. to market their goods to businesses and consumers using Alipay/Ali Baba, but not for businesses using these services to market to consumers within the U.S.

can be protected without sacrificing a large part of the global import market into the United States.

Case Study 1: Alipay

Alipay US, Inc. does not currently fall under the provisions of the GLBA because it is a financial institution providing its services to merchants, and merchants do not fall under the definition of a consumer or a customer in the Act.

CS1-1: Alipay Funds Transfer Terms and Conditions

Alipay Funds Transfer Terms and Conditions is a user agreement between Alipay US and the US-based Company, along with the Company's customer[71]. As Alipay US is based in the state of California, the document was originally published in English, and Section 30 of Schedule B[72] upholds the original English version as the governing document. The agreement's Schedule A explicitly states what expectations and rules of responsibility Alipay, the Company, and the Company's customer are each obligated to adhere to. This includes acceptable use of IP, which party is the sole or primary responsible party for various commitments, and the rules governing the acquisition and transfer of data for any or all parties in the agreement. Due to Alipay US operating within the state jurisdiction of California, clause 20.1[73] denotes that all disputes arising from this agreement will be examined under the state of California's laws and regulations. This means that the California Consumer Privacy Act and associated amendments are applicable to

[71] Customer is defined in the TC as "a customer of the Company (which may be an online or offline merchant) that wishes to make cross-border payment transactions or disbursements through the Company and Alipay"

[72] Language: "Your Agreement has been prepared in English. In the event of any inconsistency between the original English version and any translation, the English version shall prevail to the extent of any inconsistency".

[73] 20.1. Except as otherwise required by Applicable Law, your Agreement and the resolution of any Disputes shall be governed by and construed in accordance with the laws of the State of California without regard to its conflict of laws principles.

data collection and retention concerns for parties in an agreement with Alipay US However, this clause, and many others, provide a caveat for "Applicable Law" to take precedence over all terms and conditions within the agreement, including governing legislation outlined in the Terms and Conditions.

The Terms and Conditions defines "Applicable Law" as "*any law, regulation, rule, requirement, judgment, decree, licensing commitment, order or directive, including, without limitation, any global, federal, country, state or local laws, rules and regulations and including those issued by governmental or regulatory authorities having jurisdiction over the relevant Party, that are applicable to a Party or its business or which a Party is otherwise subject to.*" Although Alipay US is a subsidiary of Ant Financial based in the United States, and this paper examines both the Company and its customers as also being in the United States, the agreement specifies that laws arising from the PRC are Applicable Laws. Under Schedule B, section 4, subsection E "Sanctions", funds transfer and any other actions listed within the agreement are prohibited from being conducted with, by, or for those sanctioned under the Ministry of Public Security and the Ministry of Commerce for the PRC, as well as those sanctioned by US authorities. Sanctions prohibit applicable parties, such as those doing business with or out of the United States or China, conducting business with individuals or entities that have been "blacklisted" by the governments of the US and PRC. For example, Alipay US, under US Sanctions, cannot provide its services to individuals or entities within North Korea. Sanctions include the affiliates of those "blacklisted" as well, meaning Alipay US cannot do business with anyone who will, under reasonable suspicion or prior evidence, use Alipay's services for an individual or entity in North Korea.

This agreement, a collection and retention as the responsibility and concern of the Company in the agreement; Alipay itself obtains data of the Company and the Company's customers through the Company. I consider these Terms and Conditions requiring the company and its affiliates to act in good faith for merchant purposes and their financial digital intermediaries. However, the expectation is that users, both individuals and companies, based in the United States, should not be held to the legal compliance expectations of a foreign nation. Going further, not explicitly stated, and again, this Terms and Conditions is not directed towards data collection and retention by Alipay, any data shared with Alipay is unspecified as to where the data is stored, which of Alipay's affiliates may or may not be able to access and hold the data itself, and other unknowns that would be of larger concern for PII and customer data. The concern that arises from this is the lack of clarity or opportunity to seek clarity when it comes to data collected and retained by Alipay. It is also simply not time or cost-effective for each company to negotiate with digital financial intermediaries for clarity and assurance on customer data protection. Therefore, it is necessary to enact legislation that would require any and all digital financial intermediaries to clarify from the start the what, where, why, and length of retention for consumer data, as well as make known what opportunities for recourse consumers have.

The Alipay Funds Transfer Terms and Conditions does appear to legally abide by both the Gramm-Leach-Bliley Act and the California Consumer Protection Act (CCPA), despite not explicitly making reference to either law. It can be inferred that the current structure of the agreement does already adhere to both regulations and the associated requirements since Section 20 of the document states that the laws of the State of California are the ruling laws, except in specified circumstances that are left unspecified in the document. However, if and when Alipay

becomes used directly by consumers, Alipay will need to update the Funds Transfer, specifically when it comes to the data collected for internal purposes and compliance.

Does this agreement show a concerted effort on the part of Alipay? No. Because of the vagueness of data retention, and the fact that data can be retained even after a receiving party terminates their contract for longer than is stipulated by law, this is not in line with the efforts of either the GLBA or CCPA to commit to limiting unnecessary data collection and retention.

CS1-2: Alipay's PayFac Data Handling Notice

Alipay's PayFac Data Handling Notice is a statement of notice for users of Alipay's wallets and digital funding privileges that states what data is collected, how it is used, and with whom, if any party, as well as the rights users have for controlling their own data. The notice denotes that it is similar to CS1-1, with the merchant being the primary responsible party for data collection and retention, and that Alipay's PayFac service is a digital financial intermediary. The list of data collected by Alipay when using the PayFac service is consistent with other financial digital intermediaries, such as verifying and authorizing credit purchases and shipping addresses. Two items that Alipay specifies they collect at the time of using the service are (1) government identification and (2) the user's image, also referred to in the notice as a "selfie"[74]. The notice explains that the data collected by Alipay are for the purposes of fraud prevention and identity verification.

There is an ongoing debate of what visual identifications constitute PII, and furthermore, which of those identifications should be at least protected and at most prohibited from prolonged

[74] Section 1: What Personal Data We Collect About You, identity and verification information for purposes of fraud prevention and identity authentication, such as your age (when purchasing age restricted goods), authorization to use a payment method, government identification numbers, and your image (selfie).

retention. The United States Department of Defense's Privacy, Civil Liberties, and Freedom of Information Directorate considers "Biometric records such as photographic image (especially of face or other distinguishing characteristic) …" as PII, whereas the International Standards Organization outlines specific parameters that would consider a photograph as PII, namely those used in government identification. For identification via photograph or government identification to prevent fraud, collection for verification purposes is not common practice, but it is also not unheard of for fully digitized commerce. To continue to prevent fraud, but also to put the control back into the hands of the consumer, retention of PII must be better defined in terms of where and for how long PII is kept, as well as enfranchise consumers by providing the ability to request the removal of PII, especially visual identification.

In this case of data handling, Alipay is a service provider for digital transactions of payment and goods/services between a customer and merchant. Alipay obtains PII when a customer uses Payfac services via a digital merchant; therefore, the responsibility for PII security falls to the merchant utilizing Payfac services[75]. To provide goods/services more securely to its customers, the merchant agreement with Alipay should restrict the use cases in which Alipay would need to collect and retain PII for rendering Payfac services. Furthermore, Alipay, in agreement with merchants using Payfac services, and as a general show of good faith, should indicate the length and location of collected and retained data obtained from customers using Alipay's associated services.

The document of CS1-2 is in line with both the GLBA and CCPA, because it serves as a source of information about data handling, and it is not an agreement directly between Alipay as

[75] From Section 4: Your Choices and Privacy Rights with Respect to Your Personal Data, The merchant (sic.) (rather than us) decide how and why your personal data is collected, used and shared, and how long it is retained.

a service provider and the consumer. Furthermore, the notice is an example of a good faith act on the part of Alipay, as the notice outlines what information Alipay collects through the merchant a consumer is using. In the case of using Payfac, the duty of responsible data handling falls to the merchant, as any information collected by Alipay was already collected by the merchant.

CS1-3: Alipay Privacy Policy for Merchants

Alipay US does not currently have a privacy policy specific to individuals and those not-otherwise classified as a "merchant" or digital financial intermediary. This privacy policy is designated for those seeking to sell/provide a good/service in a digital space using Alipay's services.

Section 2 of the Privacy Policy, "How We Obtain Your Personal Information", first describes common, and perhaps more well known, methods of PII collection. These include that the user knowingly and purposefully provides their data for the use of Alipay services, as well as the use of cookies in collecting technical information about the use of services. The concern about Alipay's data collection methods comes from Alipay's acquisition of potential PII through social media[76]. Section 3 of the policy outlines the reasons for data collection and retention, explicitly listing thirteen general reasons. Following this list, the policy provides the additional note that not-otherwise-specified reasons for collection and retention are valid, provided notice is sent to the user. This indicates that the thirteen reasons, one of the reasons being to provide marketing and direct advertising, permit PII collection and authorization potentially unknown to the individual whose PII is collected.

[76] publicly available sources, such as public registers and social media.

This policy provides a mostly thorough understanding of Alipay's data handling practices, albeit with the absence of the impetus of this paper. The policy does not indicate where data, including PII, is retained, although it may be transferred to the EU, Singapore, China, or remain within the US. The policy does state that a legitimate interest for Alipay's collection and retention of data is the interest of Alipay to exist in good conduct outside of its areas of operation, also not readily specified[77]. This means that potential PII could be collected and retained on the basis of Alipay believing the data could be useful in order to be seen in a good light outside of legal requirements.

Section 7, "International Transfers of Your Personal Information", highlights the need for federal and nationwide legislation. Those within the European Union are afforded the right to limit the transfer of their data across national borders under the GDPR (but not anywhere else?). The policy makes allowances for the future of new national legislation, so this privacy policy is capable of being adapted in a more protective measure if federal legislation were to exist[78].

Section 8, "Your Choices and Privacy Rights with Respect to Your Personal Information" under the subsection specific to data rights within the United States, is mostly limited to users learning what data Alipay has about users. There is little option for mandating Alipay delete a user's data, though individuals can request this service.

Section 9 is specific to the California Consumer Privacy Act, again providing evidence that existing state-level privacy acts are effective and ought to be expanded nationwide.

[77] to comply with codes of conduct, codes of practice and similar good conduct principles which do not have the force of law in the countries in which we operate, but are prudent for Alipay Group to apply
[78] Notwithstanding the foregoing, where expressly required by applicable law or regulatory order, we will not transfer personal information outside the country from which it was collected

The Merchant Agreement legally meets the requirements of the GLBA and CCPA, and makes specific remarks towards its compliance with the CCPA in Section 9. However, the agreement highlights the specific areas in which interests that are not in line with consumer data protection are served at the expense of the consumer's autonomy in handling their own data. This lack of information on data storage is not in good faith with the GLBA, but its explanation of data collection, what data is obtained, and how, is acting in good faith with the CCPA.

CS1-4: Alipay General Disclaimer

The General Disclaimer Alipay provides to merchant customers using Alipay services is not of much value to the discussion in this paper. However, it is important to note different US courts are authorized to arbitrate concerns of this disclaimer from the court designated for arbitration of concerns arising from the Funds Transfer Terms and Conditions. The General Disclaimer designates New York[79] as the state whose jurisdiction will be used for legal purposes, while the Funds Transfer Terms and Conditions authorizes California for the same purpose. There is no provided justification for this difference, nor is it apparent that this distinction is necessary, given that Alipay US operates within the state of California. To facilitate continued operations within the US in a more fluid, as well as more-protected, digital financial space, federal policy around the handling of PII by non-banking institutions in the financial space, must be codified to negate state-to-state disputes and gaps arising from more decentralized jurisdiction.

[79] This Disclaimer shall be construed and governed by the laws of New York, without regard to the conflict of law principles thereof.

Case Study 2: WeChat Pay

WeChat Pay is a service provided by the company, Cai Fu Tong, also known as Tenpay. WeChat, or Weixin, is the platform used by Tenpay to host its service. WeChat rose to fame as one of the top social media apps used in the PRC, and its messaging function has become popular worldwide, with many expats, diaspora, and those with friends and colleagues in the PRC using WeChat to stay connected. Unlike Alipay, WeChat Pay does not have a subsidiary dedicated to the United States or other locations outside of the PRC, and, resulting from this, all documents from both Tenpay and WeChat are translations of the original documents written in Mandarin Chinese. All documents for this case study are translations obtained from Tenpay and WeChat; however, both sites explicitly state that in the event of any and all "errors" arising from the user agreements, that the original Mandarin Chinese document will be upheld as the final judgment.

Tenpay's purpose is as a non-banking digital financial service. In the scope of WeChat Pay, Tenpay works to connect users with a bank in order to connect digital transactions. Through WeChat Pay, Tenpay also provides users with the ability to send each other funds, similar to how Venmo and Paypal operate. While not the focus of this paper, it is important to note that in recent years, Tenpay has been formally chastised and fined at least three times by the Chinese government's State Administration for Foreign Exchange (SAFE) for not properly abiding by forex rules and regulations. A future consideration for research is the security and application of forex rules in the digital space, as well as preventing currency exchange handlers from treating consumers unfairly and profiting from market manipulation.

To understand the rules and regulations around WeChat Pay, it is important to provide a high-level overview of the service, including its connection to the social media service of

WeChat. This case study will remain focused on WeChat Pay as a platform providing digital payment services, but understanding that WeChat has additional services that result in overarching data collection potentially unrelated to the financial services it provides.

First, WeChat Pay is inaccessible to those who do not have a social media account with WeChat. Tenpay uses the existing functions within WeChat to support funds transfer between individuals, as well as use the verification processes already required for use of the messaging services. WeChat Pay is also limited, for consumers, where WeChat Pay can set up and authorize a bank account. This ability is limited to Chinese banking institutions. There are numerous WeChat Pay service providers for merchants seeking to gain business from Chinese consumers, but this is not the focus of the paper.

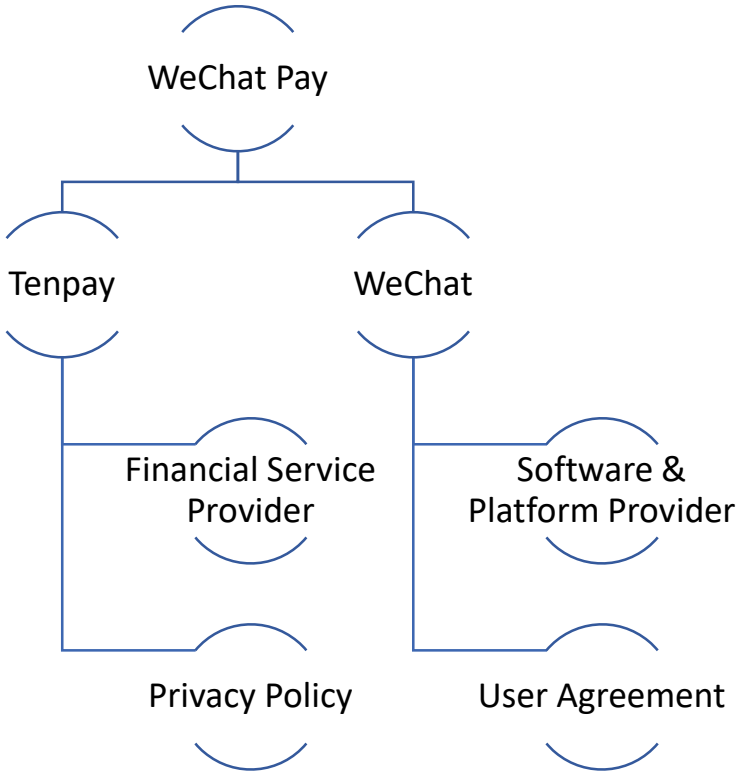


Diagram Depicting the Ownership and Control of WeChat Pay

(credit: Emmeline Nettles)

Second, WeChat Pay is considerably less expansive than all the applications Ant Financial provides; however, Alipay and WeChat Pay both focus on digital transactions, both business to consumer, also known as B2C, and C2C, consumer to consumer[80]. WeChat Pay, as mentioned previously, is similar to Venmo, a common digital payment transfer service used in the US. WeChat Pay has, at its core, two services: Balance Payment and Quick Payment. Balance Payment is defined in the WeChat Pay User Service Agreement as paying via the payment account a user has via WeChat Pay. Quick Payment is more familiar to the US audience, as it operates synonymously with Venmo. In Quick Payment, the user can conduct digital transactions by linking their bank account to WeChat Pay. Similar to Venmo, if the balance in the WeChat Pay account, including the Balance Payment, contains insufficient funds, the user can obtain sufficient funds through Quick Payment, including authorizing the WeChat Pay service to automatically "top up" insufficient funds from an authorized bank account automatically. Finally, while not an independent service from Balance and Quick Payments, WeChat Pay conducts foreign currency transactions on behalf of the user when conducting international business.

WeChat Pay is a complimentary case study to Alipay. Whereas Alipay has existed in the US e-commerce space since the late 2000s, albeit as primarily a merchant service, WeChat Pay has not existed in the US market before, although WeChat itself has become an infamous topic in recent congressional and judicial discussions. WeChat has often been lumped in in discussions of

[80] Alipay also provides B2B services, but as the focus of this paper is consumer data privacy, this difference is not relevant.

data collection of users in the social media space as being an unlawful foreign influence, but it has not been highlighted as a service to consider in the growing digital transaction space. Alipay has precedence in operating within the United States but has largely been considered a non-issue. WeChat has precedence in legislation against its services, but its financial service has received little attention to date.

CS2-1: WeChat Payment System User Service Agreement

Our first document for analysis under Case Study 2 is the WeChat Payment System User Service Agreement. Despite the agreement being hosted on WeChat's website, the agreement itself is a user agreement with Tenpay, the service provider of the digital payment system. Following documents in this case study will focus directly on WeChat's role itself in WeChat Pay.

The agreement with Tenpay is largely unremarkable, if not difficult to read at times due to the translation. The agreement states what services are provided by Tenpay, defines the operations of Balance and Quick Payments. The agreement even defines what Tenpay considers to be sensitive user data[81], and advises steps for remediation should the user's data become compromised.

Section 4, Use of Service, informs the user that use of WeChat Pay authorizes Tenpay to open a bank account on behalf of the user for transactions conducted through Tenpay. The associated bank is user-chosen but restricted to banks available for Tenpay to conduct its services. The agreement does not define its services as restricted to the PRC, but later sections define China, specifically Guangdong, as the base of operations for WeChat Pay. Further,

[81] Financial information such as bank accounts, passwords, PII such as biometrics and geographic data

banking institutions are limited to Chinese banks, although, like Alipay, foreign tourists to China are gaining the ability to utilize digital payment systems during their stay in the PRC. Section 4 also states what constitutes misuse of WeChat Pay services. 4.14 defines one misuse of service: "Oppose the basic principles set in the Constitution, endanger national security, leak state secrets, subvert state power, or undermine national unity". Undermining national unity is a concern addressed in many policies and regulations originating from the PRC, and it is an action that is not well-defined, often purposefully left unclear in order to adapt to fears of disunion and political unrest.

Section 6, Observation of Local Laws, advises users against "being involved in political and public events for using the Service". It goes on to state that such involvement is grounds for possible suspension or termination of the user's WeChat Pay account. The translation here is unclear as to what constitutes involvement resulting from using WeChat Pay services. Section 6 resembles Section 4 of the agreement in not using the services for degradation of state power; however, what constitutes misuse of the service for political subversion is not readily defined in the agreement. This is a concern, as, owing to the nation and state in this agreement being the PRC, Sections 4 and 6 could very likely result in discrimination of users based on political party or agenda, which is a protected class in the United States.

Section 12, Application of Law, and Dispute Resolution, places this agreement under the governance of Nanshan District, Shenzhen, Guangdong Province in the PRC. All arbitration will be held in Nanshan District and this agreement will follow laws with respect to Nanshan legislation. This section does make acknowledgement of conflicting laws, such as when WeChat Pay is used outside of Nanshan, or outside of China. This user agreement provides an addendum specific to the use of WeChat Pay services within the European Union.

When assessing the user service agreement, WeChat Pay's End-User License Agreement (EULA), it is not difficult to determine if the agreement would pass the Good Faith Model, as the agreement is not even inline with the GLBA and CCPA. The legal basis for CS2-1 is rooted in, and regulated by the PRC court of law. Some of the restrictions of using the service, such as religious discrimination and societal discourse, are anathema to core tenets of American norms of behavior and the constitution itself, let alone the GLBA and CCPA.

CS2-2: Weixin Privacy Policy and Software License Agreement

Section 6, Protection of User's Personal Information, provides users of Weixin services with an understanding of the data being collected, how the data is used, what abilities users have for changing, removing, or otherwise opting out of certain Weixin services. This section also sets forth limitations on what data may be shared with third parties. Regarding WeChat Pay, it is an opt-in application within Weixin services. Users must authorize base functions of the WeChat application to access any opt-in services.

Section 7, Main Rights and Obligations, maintains that Weixin is permitted to retain user data after a user deletes or otherwise terminates their WeChat account for the maximum length of time permitted for data retention. The agreement gives Weixin the authority to determine length of time for retention of user data without specification for limitations on the company even after a user no longer uses the services provided, such as WeChat Pay. Furthermore, Weixin is not obligated to return user data to the user themselves. Except as required by law, there should not be this indefinite period of retention once a user ceases accessing a service or otherwise terminates their relationship with the payment system. A user must accept the terms of agreement for using a service in order to use that service. Following this logic, once a user terminates their relationship with the service, that agreement ought to itself be terminated.

Therefore, the service provider should no longer have the privilege of holding onto data of former users as it pleases.

Section 8, User's Code of Conduct, prohibits use of Weixin for degrading national unity with respect to the PRC, akin to the WeChat Pay User Agreement. As before, this is not an uncommon tenet for services with social components in the PRC, especially ones that have group organization abilities. The restriction or termination of services based on what is a protected class in the US would be key facets in policy around foreign digital payment systems. This license agreement as well as the user agreement in CS2-1 are specific to consumers or individuals using WeChat Pay and Weixin services.

The Weixin Privacy Policy Guidelines focused primarily on the security of user data with respect to the use of the social media and messaging services provided by Weixin. The Guidelines explicitly state that the Tenpay Privacy Policy will be followed when using WeChat Pay. The final document for analysis in the WeChat Pay Case Study covers the Tenpay Privacy Policy.

WeChat as a social media application, which is the main application discussed in the software agreement, is already used in the US, though it is being increasingly restricted, particularly the use of the service by government affiliates. The opportunities to opt-out of certain information gathering, except of course where necessary to enable functionality of WeChat services, is in line with the CCPA, and its promise to secure its users' data properly shows its compliance with the GLBA. But, as has become increasingly apparent in recent years, the data privacy policy of WeChat as it pertains to the US, is not in good faith with US consumers. WeChat's ability to retain data as it sees fit, and to blacklist users who may be considered to be undermining "national unity" or otherwise politically engaged in ways the CCP

disagrees with, can have their data retained or otherwise handled. Self-censorship is beyond the scope of this paper, yet it bears mentioning that the fear of reprisal from such data collected from social media services and functionalities is a real fear in China, and beyond, as expats and the diaspora feel its effects.

CS2-3: Tenpay Privacy Policy

Like with CS2-1 and CS2-2, the Tenpay Privacy Policy was analyzed as a translated document and is subject to discernment via the original Mandarin Chinese.

Section 1, Your Rights, informs users of what data will be collected from them upon using associated Tenpay services, how to view and modify what user data Tenpay has collected, delete user data within associated applications, and how to cancel an account with Tenpay or opt-out of specific services. The data that can be deleted by users is restricted only to transaction history within WeChat Pay, and deletion of the history does not negate previous transactions, nor any data transfers conducted at the time of payment or services rendered. Cancellation of a user account will cause Tenpay to cease processing new user data, but previous user data will be retained for legal compliance purposes.

Section 4, How We Store and Protect Your Personal Information, specifies the rights but also obligations Tenpay has with respect to user data collected within the PRC, or Mainland China as the agreement also terms it. This specific base of data is retained within the PRC and is subject to both the Personal Information Protection Law as well as the Implementation Measures of the People's Bank of China for Protecting Financial Consumer's Rights and Interests. These measures taken to secure domestic data and strive to store user data domestically are an excellent example of why the US should follow suit. Not only does this prevent misuse or mishandling of data once it is transferred across national borders, the rules and regulations for appropriate

handling of data, not to mention appropriate use of services by a user will be standardized within the region.

Section 7, Circumstances Where Personal Information Could Be Processed Without Your Consent, states when and how user data may be collected outside of the user explicitly providing the data to Tenpay. Namely, two methods of non-explicit collection are "supervision by public opinions for the public interest and other activities" and "any personal information that you disclose or that has been lawfully disclosed". The latter method, of personal or lawful disclosure, does not explicitly state what these methods are constrained to, which, if taking into account that Tenpay provides its services through a social media application, could be through messaging services or otherwise unspecified data a user provides without being conscious of its use or potential misuse regarding financial security and activities.

The Cross-Border Payment Information section names the domestic bank involved in cross-border payments as the China CITIC Bank Corporation. All user data involved in cross-border payments coming from within the PRC are protected by the Personal Information Protection Law, requiring Tenpay and its affiliates, including overseas partners and merchants, to maintain the security of PII involved in cross-border payments. This section also notes that users conducting payments within the PRC via an international credit card will have the Personal Information Protection Law and associated regulations apply to their transactions too. The data handling policies surrounding cross-border transactions via Tenpay are presently constrained to Chinese users undertaking transactions involving cross-border payments. There is currently no policy in place for foreign users undertaking similar transactions.

This last case study does not raise any immediate red flags with either the GLBA or CCPA, though the Federal Trade Commission (FTC) would likely still examine these Cross-

Border Payments, as would the Council on International Foreign Investment in the United States (CFIUS). The agreement and understanding of what services Tenpay can provide in cross-border investment actually seem to be in good faith, too. Tenpay promises to users of the investment service to protect their personal information, and uphold the standards of Chinese data protection laws even once the information is transferred outside of PRC borders.

Results of the Good Faith Model

Good Faith Model	Alipay (CS1)				WeChat Pay (CS2)		
	CS1-1	CS1-2	CS1-3	CS1-4	CS2-1	CS2-2	CS2-3
Gramm-Leach-Bliley Act	Bad Faith	Good Faith	Bad Faith	Bad Faith	Bad Faith	Developing Faith	Good Faith
California Consumer Privacy Act	Bad Faith	Good Faith	Good Faith	Bad Faith	Bad Faith	Developing Faith	Good Faith

Table Showing the Results of the Good Faith Model Assessment

(credit: Emmeline Nettles)

My summary of the Good Faith Model Assessment, indicated above, shows that a majority of the EULAs and associate documents analyzed in the case studies indicate the potential of these companies acting in bad faith towards US consumers. And even the documents currently in-line with good faith actions under the GLBA and the CCPA may prove to act in bad faith, such as the software licensing agreement of WeChat (Weixin), hence CS2-2's status of "Developing Faith".

In closing my analysis, I reexamine the parameters the Good Faith Model is structured on. If it is the case that there is an insufficient legal framework to prevent the procurement and possible dissemination of personally identifiable information (PII) in the PRC via transnational

data collection by PRC-origin digital payment platforms under the PRC, I shall put forth policy recommendations for the Federal Trade Commission (FTC). These recommendations will emphasize the importance of enforcing extrinsic digital payment platforms to abide by US consumer privacy protection laws. Additionally, I will put forth recommendations that the US government adopt greater restrictions towards the permissibility of digital payment platforms transferring personally identifiable consumer data outside of US federal jurisdiction. Following the assessment using the Good Faith Model, only one document for Alipay and one for WeChat Pay appeared to act in good faith under both the GLBA and the CCPA.

Conclusion

Following my qualitative research, analysis of US legal framework and the rules of behavior for Alipay and WeChat Pay, I return to the question posed at the beginning of this paper:

> *Research Question: Is there existing legal framework within the United States that is violated by the data collection policies of PRC-origin digital payment platforms?*

My research found that there are no present violations of US legislation by either company's data collection and retention practices. These companies are not the big, bad, evil corporation. Alipay and WeChat Pay both have strong legal teams that ensure compliance with the laws pertaining to the region they operate in. This paper does not seek to issue a civil suit

against either company, because there are no existing laws within the United States that either company violate. And therein lies the issue. Legality does not beget morality, or in the case of data privacy, autonomy of individuals.

The United States, with the case of social media and other digital services and products in that realm, cry out via court cases and congressional hearings that user data should be a protected resource. And it should be, but that outcry should not end with social media, and, frankly, is only one piece of the puzzle for PII protection, but that debate is not part of this paper[82]. What is part of this paper is how little concern there is for regulating the digital financial space. The mid-to-late 20th century saw an exchange of cash and check for credit and debit cards, and the 21st century is seeing a transition from these to digital payment systems[83]. And why would people not want to do this exchange? Easily accessible on one's phone, along with all the other services being hosted on one's mobile device, digital payment systems are simply easier, for both consumer and merchant.

There is no turning the tide when it comes to the adoption of digital payment systems, both US-based and foreign companies. And there does not need to be a turn. The tide is visible, and so there is time to construct and install strong levees of data protection. In the following section, I will put forth recommendations for the development of a federal framework to introduce stronger, more effective legislation and compliance requirements that return control of data to those whose data is being collected.

[82] "Why a Ban on TikTok Won't Solve All Data Privacy Concerns," PBS NewsHour, March 30, 2023, https://www.pbs.org/newshour/nation/why-a-ban-on-tiktok-wont-solve-all-data-privacy-concerns.
[83] Rampton, "The Evolution of the Mobile Payment."

In my thesis I examined the current state of the legislative framework in the United States to assess the laws dedicated to protecting consumer privacy. Given that federal consumer privacy laws have not been updated since the turn of the century, I utilized two case studies of foreign payment systems that have been created since after these laws were last amended to determine if these laws should be updated to address the current needs and concerns of consumer data privacy.

For context, when the Gramm-Leach-Bliley Act was enacted, and also the last time the law was altered, there were no digital payment systems that existed independent of banking institutions. Today, these systems are fast replacing other forms of payment. And this rapid shift in financing does not come without issues. Venmo, Alipay and more have all had cases brought against them regarding consumer data privacy.

How do you judge cases for which there has been no legal precedent and there are no existing laws that specifically address the concerns of virtual data collection and retention? This is why I have argued that the US laws and federal legislative framework, specifically the Gramm-Leach-Bliley Act, be amended and its policies be brought into the modern era. It is a common joke that policy moves slowly, which is why it is so necessary that this issue of consumer data privacy be addressed before the collection and retention of US consumer data by foreign entities, namely digital payment systems, morphs into an unmanageable issue.

Policy Recommendations

[1] Create a working group comprised of federal and state agencies, as well as private sector individuals, both merchants and consumers, to research the most effective method to streamline adoption practices of a federal data privacy framework for businesses.

A multilateral, inclusive working group will ensure that US norms and behaviors are more clearly defined in the creation of a federal framework. Similarly, including merchants and consumers, the primary players in this discussion, will foster a dialogue between the two parties and, hopefully, find some common ground wherein user data is, rightfully, revested into consumer hands, but that merchants are given the opportunity to adjust to shifts within the data economy.

The issue of data privacy is multifaceted, and each player in the game is looking through a different lens. However, I will refer back to the role of the FTC, and why it was created in the first place. "…to protect consumers". This modus operandi must remain integral to the formation and updating of American legislative policies, and will require fighting against the business trend of collecting as much data as possible, rather than "only necessary" information.

[2] Amend the Gramm-Leach-Bliley Act by expanding the consumer data covered to be PII rather than only NPI. The amended Act should also require financial institutions to provide information on data storage, namely, where the data is stored, the reason for storage, the length of time the data is stored, and what methods of opt-out, or opt-in, consumers have access to.

To more securely provide goods/services to its consumers, the merchant agreement with Alipay should restrict the use cases in which Alipay would need to collect and retain PII for rendering Payfac services. Furthermore, Alipay, in agreement with merchants using Payfac services, and as a general show of good faith, should indicate the length and location of collected and retained data obtained from consumers using Alipay's associated services. Updating the GLBA would support this shift, if Alipay wants to continue operating as a service provider to merchants in the US, as well as potentially expand into providing direct-to-consumer services.

To continue to prevent fraud, but also to put the control back into the hands of the consumer, retention of PII must be better defined in terms of where and for how long PII is kept, as well as enfranchise consumers by providing the ability to request the removal of PII, especially visual identification. Furthermore, the Act should update what collected consumer data is considered protected. Rather than restrict protected information to only the information collected in financial exchanges, the Act should adopt the protection of PII as it pertains to the consumer, rather than NPI, or nonpublic personal information. Any data that can form an intimate understanding of a consumer should be protected, and it should be up to the consumer to choose what information a financial institution should be able to store as it relates to their relationship with the institution.

[3] Task the Council on Foreign Investment in the US and the Federal Trade Commission (CFIUS) with scrutinizing transnational service providers via the parameters of data security and protection norms and practices that exist under a specialized version of the Privacy Shield. Namely, CFIUS should work with foreign entities to ensure that, when conducting business and/or providing services within the US, that no foreign regulations nor foreign business practices shall supersede US legal code. CFIUS should collaborate with the FTC in order to enforce compliance with updated legislation, namely, an amended GLBA.

This modified Privacy Shield would be distinct from the current Data Framework Agreements with the EU and the United Kingdom; instead, under the advice of the Department of Commerce, who works with the present version of the Privacy Shield, CFIUS and FTC should jointly collaborate to allow foreign companies to self-certify under a consumer privacy protection agreement. In keeping with the intentions of the existing Privacy Shield, that protection of private individuals' information can be protected while strengthening economic

exchange, the agreement should reward companies that undertake becoming responsible data handlers in the US.

Future Considerations

Currently, all digital payment systems operating within the US are in compliance with state and federal legislation. But that does not mean that the systems are acting in good faith towards US-based consumers. And due to the difference in norms and rules for behavior, foreign companies might not be aware of what is considered bad faith against consumer data privacy. It is the responsibility of policymakers to strengthen the federal legal framework, and ensure that foreign companies can operate within the US to strengthen our digital economy, while at the same time returning the power of information autonomy to consumers.

Even more so than initiating federal debate of norms and responsibilities, I hope this paper's evidence of reasonable suspicion initiates scholarly and journalistic endeavors towards both widening and deepening the field of digital user rights. The debate of a centralized vs decentralized internet is not discussed in this paper; however, the use of political and sovereign borders in a "borderless" internet is necessary in discussion to promote not just norms of behavior, but actual law and order directives. It is the hope that other nations will follow the example of the EU and, as this paper intends, the United States, too. By having guidelines in place, the globalized economy that has grown exponentially from digitization of the financial sector, companies can continue to innovate and expand their reach, while consumers continue to be protected in a landscape where their data is a hot commodity.

A future research question to be examined from the findings of this paper is what the feasibility of requiring data collected to be stored locally would be, and what economic effects

such a requirement would have. If this was an easy transition, companies would have already made these shifts, and the US government would have been a strong supporter, owing to its purported boost to the domestic economy. Clearly there are other factors, possibly linked to difficulties stemming from globalization at play.

It is never too early to improve laws to protect consumers in an economy that continues to innovate and accelerate. But there will be a point where it can be too late for preventative measures, and, instead the US government will need to employ damage control from hard-learned lessons. While these digital payment systems remain largely unregulated in their data collection, and moreso, their retention, the concern of misuse or malicious use of this data is not a matter of "if" harm will result, but "when". The internet may appear borderless, but the individuals using it still exist under a legal system, whether it be rule of law or rule by law. This means that these peoples' data and personally identifiable information need to be protected under these same laws, even when that information is collected across digital systems.

Bibliography

"'Tour Pass' Information Technology Service Agreement." Accessed February 27, 2023. https://render.Alipay.com/p/c/k2ffmmxp.

"Alipay Fund Transfer Terms and Conditions | Legal | Alipay Docs." Accessed September 7, 2023. https://global.alipay.com/docs/ac/Platform/4lnjflvu.

"Alipay Global Merchant Portal." Accessed January 31, 2023. https://global.Alipay.com/platform/ihome.

"Alipay Global Open Platform Membership Agreement | Legal | Alipay Docs." Accessed February 14, 2023. https://global.Alipay.com/docs/ac/Platform/membership.

"Alipay Privacy Policy for Merchant Services | Legal | Alipay Docs." Accessed September 7, 2023. https://global.alipay.com/docs/ac/Platform/privacy.

"Alipay's PayFac Data Handling Notice | Legal | Alipay Docs." Accessed September 7, 2023. https://global.alipay.com/docs/ac/Platform/bahzqeb-.

"Bad Faith Definition," May 16, 2021. https://web.archive.org/web/20210516212921/http://www.duhaime.org/LegalDictionary/B/BadFaith.aspx.

"Data Localization Laws: An Emerging Global Trend," January 6, 2017. https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/.

"EULA Definition by The Linux Information Project." Accessed October 1, 2023. https://www.linfo.org/eula.html.

"Federal Courts & the Public | United States Courts." Accessed February 18, 2023. https://www.uscourts.gov/about-federal-courts/federal-courts-public.

"General Disclaimer Alipay US, INC. | Legal | Alipay Docs." Accessed September 7, 2023. https://global.alipay.com/docs/ac/Platform/qhns4axo.

"I. OVERVIEW." Accessed October 7, 2023. https://www.dataprivacyframework.gov/s/article/I-OVERVIEW-dpf?tabset-35584=2.

"Privacy Shield | Privacy Shield." Accessed January 31, 2023. https://www.privacyshield.gov/welcome.

"Safeguarding Non-Bank Consumer Information Act." Accessed September 19, 2023. https://www.govinfo.gov/bulkdata/BILLSUM/117/hr/BILLSUM-117hr3910.xml.

"Service Agreement." Accessed September 7, 2023. https://weixin.qq.com/cgi-bin/readtemplate?lang=en_US&t=weixin_agreement&s=default&cc=CN.

"Tenpay Privacy Policy." Accessed September 7, 2023. https://posts.tenpay.com/posts/62fd7a3664e33216012f2c433495df43.html.

"The Pacing Problem and the Future of Technology Regulation | Mercatus Center," August 8, 2018. https://www.mercatus.org/economic-insights/expert-commentary/pacing-problem-and-future-technology-regulation.

"The State of Consumer Data Privacy Laws in the US (And Why It Matters) | Wirecutter." Accessed September 19, 2023. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

"UCITA." Accessed October 1, 2023. https://cs.stanford.edu/people/eroberts/cs201/projects/2000-01/ucita/index.html.

"US Customer Service Information | Legal | Alipay Docs." Accessed February 14, 2023. https://global.Alipay.com/docs/ac/Platform/grygy5.

"WeChat Pay." Accessed January 31, 2023. https://pay.weixin.qq.com/index.php/public/wechatpay.

"WeChat Payment Agreement." Accessed September 7, 2023. https://weixin.qq.com/cgi-bin/readtemplate?lang=en_US&check=false&t=weixin_agreement&s=pay.

"法律法规_北大法宝法律数据库_司法案例全文_法律法规检索平台-北大法宝 V6 官网."

Accessed January 31, 2023. https://www.pkulaw.com/.

Belfer Center for Science and International Affairs. "The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation." Accessed September 29, 2023. https://www.belfercenter.org/publication/role-federal-trade-commission-federal-data-security-and-privacy-legislation.

Bellamy, Fredric D., and Fredric D. Bellamy. "US Data Privacy Laws to Enter New Era in 2023."

Reuters, January 12, 2023, sec. Legal Industry. https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/.

Brookings. "A Federal Privacy Law Could Do Better than California's." Accessed October 1, 2023. https://www.brookings.edu/articles/a-federal-privacy-law-could-do-better-than-californias/.

Chua, Edelyn. "Mobile Payment in China: Step-by-Step Guide to Using Alipay and WeChat Pay

without a Chinese Bank Account." *The Travel Intern* (blog), March 11, 2020.

https://thetravelintern.com/china-mobile-payment-guide-Alipay-wechat-pay/.

cyber/data/privacy insights. "Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA," April 11, 2022. https://cdp.cooley.com/cross-border-data-transfers-pipl-vs-gdpr-vs-ccpa/.

Daily Life with Alipay, 2016. https://www.youtube.com/watch?v=QlW60frlH6w.

DigiChina. "Behind the Facade of China's Cyber Super-Regulator." Accessed October 1, 2023. https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/.

DigiChina. "Translation: Personal Information Protection Law of the People's Republic of China -

Effective Nov. 1, 2021." Accessed January 31, 2023.

https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

Federal Trade Commission. "Gramm-Leach-Bliley Act," June 16, 2023.

https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

Federal Trade Commission. "Letter of the Federal Trade Commission to the U.S. House of Representatives, Subcommittee on Consumer Protection and Commerce, on the U.S. SAFE WEB Act," October 31, 2019. https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-federal-trade-commission-us-house-representatives-subcommittee-consumer-protection-commerce.

Federal Trade Commission. "PayPal Settles FTC Charges That Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act," February 27, 2018. https://www.ftc.gov/news-events/news/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information-consumers-about-ability-transfer-funds.

Federal Trade Commission. "What the FTC Does," September 11, 2018. https://www.ftc.gov/news-events/media-resources/what-ftc-does.

Freedom House. "China: Freedom on the Net 2022 Country Report." Accessed September 29, 2023. https://freedomhouse.org/country/china/freedom-net/2022.

Herman, Sean. "Council Post: Should Tech Companies Be Paying Us For Our Data?" Forbes. Accessed January 22, 2023. https://www.forbes.com/sites/forbestechcouncil/2020/10/30/should-tech-companies-be-paying-us-for-our-data/.

IMF. "Fast-Moving FinTech Poses Challenge for Regulators," April 13, 2022. https://www.imf.org/en/Blogs/Articles/2022/04/13/blog041322-sm2022-gfsr-ch3.

Jansen, Monika. "VIII. Privacy —GLBA," 2021.

Krygier, Martin. Review of *Review of On the Rule of Law. History, Politics, Theory*, by Brian Z. Tamanaha. *Journal of Law and Society* 32, no. 4 (2005): 657–66.

LII / Legal Information Institute. "16 CFR Part 313 - PART 313—PRIVACY OF CONSUMER FINANCIAL INFORMATION." Accessed September 9, 2023. https://www.law.cornell.edu/cfr/text/16/part-313.

LII / Legal Information Institute. "Article III." Accessed February 18, 2023. https://www.law.cornell.edu/constitution/articleiii.

LTL Beijing. "Alipay for Foreigners || How to Use Alipay (In and Out of China)," February 20, 2022. https://ltl-beijing.com/Alipay-for-foreigners/.

Ma, Yihan. "Topic: E-Commerce in China." Statista, November 17, 2022. https://www.statista.com/topics/1007/e-commerce-in-china/.

Michaels, Miles Kruppa and Dave. "Google's Defense in Landmark Antitrust Case Hinges on Lawyers Who Took on Microsoft." WSJ. Accessed October 1, 2023. https://www.wsj.com/tech/googles-defense-in-landmark-antitrust-case-hinges-on-lawyers-who-took-on-microsoft-3c1d5059.

Nadeem, Reem. "Government Policy toward Religion in the People's Republic of China – a Brief History." *Pew Research Center's Religion & Public Life Project* (blog), August 30, 2023. https://www.pewresearch.org/religion/2023/08/30/government-policy-toward-religion-in-the-peoples-republic-of-china-a-brief-history/.

New America. "The Evolution of China's Data Governance Regime: A Timeline." Accessed October 1, 2023. http://newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline/.

Pasquali, Marina. "Topic: E-Commerce Worldwide." Statista, November 28, 2022. https://www.statista.com/topics/871/online-shopping/.

PBS NewsHour. "Why a Ban on TikTok Won't Solve All Data Privacy Concerns," March 30, 2023. https://www.pbs.org/newshour/nation/why-a-ban-on-tiktok-wont-solve-all-data-privacy-concerns.

Rampton, John. "The Evolution of the Mobile Payment." *TechCrunch* (blog), June 17, 2016. https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment/.

Rep. Lynch, Stephen F. [D-MA-8. "H.R.3910 - 117th Congress (2021-2022): Safeguarding Non-Bank Consumer Information Act." Legislation, June 15, 2021. 06/15/2021. http://www.congress.gov/.

Rep. Neugebauer, Randy [R-TX-19. "H.R.1155 - 113th Congress (2013-2014): National Association of Registered Agents and Brokers Reform Act of 2013." Legislation, September 11, 2013. 2013-03-14. https://www.congress.gov/bill/113th-congress/house-bill/1155.

Rep. Pfluger, August [R-TX-11. "H.R.7302 - 117th Congress (2021-2022): Cyber Deterrence and Response Act of 2022." Legislation, November 1, 2022. 11/01/2022. http://www.congress.gov/.

Reuters. "China Bans 'Feudal' Names for Health Foods." July 13, 2007, sec. World News. https://www.reuters.com/article/idINIndia-30320720070615.

sscott. "Silicon Valley's Role in Foreign Policy and What Others Can Learn from It, Part I." *Atlantic Council* (blog), November 2, 2020. https://www.atlanticcouncil.org/blogs/geotech-cues/silicon-valleys-role-in-foreign-policy-and-what-others-can-learn-from-it/.

Stanley, Holly. "What Is Customer Data? Definition, Collection Methods, Trends and More." Shopify Plus, August 9, 2022. https://www.shopify.com/enterprise/customer-data.

State of California - Department of Justice - Office of the Attorney General. "California Consumer Privacy Act (CCPA)," October 15, 2018. https://oag.ca.gov/privacy/ccpa.

State of California - Department of Justice - Office of the Attorney General. "Attorney General Bonta: FTC Should Follow California's Example and Adopt Robust Data Privacy Protections," November 21, 2022. https://oag.ca.gov/news/press-releases/attorney-general-bonta-ftc-should-follow-california%E2%80%99s-example-and-adopt-robust.

Statista Daily Data. "Infographic: China's Most Popular Digital Payment Services," July 8, 2022. https://www.statista.com/chart/17409/most-popular-digital-payment-services-in-china.

Stiftung Wissenschaft und Politik (SWP). "Xi Jinping Thought on the Rule of Law." Accessed September 19, 2023. https://www.swp-berlin.org/publikation/xi-jinping-thought-on-the-rule-of-law.

Taft, Jessie G. "The Promise and Pitfalls of the California Consumer Privacy Act." dli-cornell-tech, April 11, 2020. https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act.

Taggart, Tricia. "CITCON Brings Alipay and WeChat Pay to North America." Citcon, February 22, 2017. https://citcon.com/citcon-brings-alipay-wechat-pay-north-america/.

The Law Dictionary. "BAD FAITH Definition & Meaning - Black's Law Dictionary," November 4, 2011. https://thelawdictionary.org/bad-faith/.

The Law Dictionary. "GOOD FAITH Definition & Meaning - Black's Law Dictionary," October 19, 2012. https://thelawdictionary.org/good-faith/.

Toscano, Joe. "Data Privacy Issues Are The Root Of Our Big Tech Monopoly Dilemma." Forbes. Accessed September 9, 2023. https://www.forbes.com/sites/joetoscano1/2021/12/01/data-privacy-issues-are-the-root-of-our-big-tech-monopoly-dilemma/.

Trafficking Data: How China Is Winning the Battle for Digital Sovereignty, 2022. https://www.youtube.com/watch?v=CUYARR7KSgg.

U.S. Agency for International Development. "Rule of Law | Democracy, Human Rights and Governance," September 18, 2023. https://www.usaid.gov/democracy/rule-law.

US Department of the Treasury. "New Treasury Report Shows Fintech Industry Requires Additional Oversight to Close Gaps, Prevent Abuses and Protect Consumers," January 23, 2023. https://home.treasury.gov/news/press-releases/jy1105.

Waldron, Jeremy. "The Rule of Law." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Summer 2020. Metaphysics Research Lab, Stanford University, 2020. https://plato.stanford.edu/archives/sum2020/entries/rule-of-law/.

William & Mary Law School. "Democracy and the Rule of Law." Accessed February 21, 2023. https://law.wm.edu/academics/intellectuallife/researchcenters/postconflictjustice/internships/internship-blogs/2021/claire-gardner/democracy-and-the-rule-of-law.php.

World Bank, “COVID 19 Drives Global Surge in use of Digital Payments”, June 22, 2022., https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments