Issues in Information Systems
Volume 24, Issue 2, pp. 304-319, 2023

DOI: https://doi.org/10.48009/2_iis_2023_127

Cultural differences in privacy protection: a case study of DiDi privacy violations

Jing Hua, *Robert Morris University, jxhst641@mail.rmu.edu*
Ping Wang, *Robert Morris University, wangp@rmu.edu*

Abstract

This study explores the cultural factors in privacy protection through a case study of DiDi, a ride-hailing company in China that was investigated for privacy violations. The study analyzes the influence of Confucianism and collectivism on the concept of privacy and practices of privacy protection in China, as well as the role of high-power distance in shaping what is deemed in the public interest. Theoretically, this research proposes a model of cultural differences that underline the privacy concepts and practices in China and the West. This model and the DiDi case study will contribute to understanding and facilitating cross-cultural comparisons of privacy concepts and practices. The significance of this study lies in informing and enlightening privacy researchers and practitioners on privacy policies and strategies in diverse cross-cultural contexts.

Keywords: Cultural factors, data privacy, privacy protection, DiDi, privacy violations

Introduction

In recent years, there has been growing concern over data privacy and protection in China and around the world, as major tech companies have faced increasing regulatory pressure and scrutiny over their handling of user data. In response to these concerns, China introduced the Personal Information Protection Law (PIPL) in November 2021, which imposes strict requirements on data storage localization and other measures aimed at safeguarding user privacy. The PIPL is widely regarded as having even more stringent provisions than the General Data Protection Regulation (GDPR) in Europe.

However, it is crucial to recognize the influence of cultural factors, including philosophy, values, beliefs, and traditions, on privacy concepts, regulations, and practices. The East and West have distinct cultural perspectives that shape their approach to privacy. Understanding these cultural nuances is essential for interpreting and effectively implementing privacy laws and regulations (Gao and O'Sullivan-Gavin, 2015; Da Veiga, 2018; Fung & Etienne, 2021; Li, 2022).

The PIPL only sets out general principles and a framework and does not define some terms such as “grave violation”, annual revenue. There are still uncertainties about how it will be enforced in practice. The value of this study lies in its potential to enhance understanding of PIPL and helping organizations operating in China to mitigate legal risks and reduce associated costs. However, it is important to recognize that the PIPL's current framework may not fully encompass the cultural nuances that shape privacy perceptions and practices in China (Creemers, 2022; Chan & Kwok, 2022; Yanqing, 2022). By delving into the cultural factors underlying the regulations, this research will help to advance in-depth understanding of privacy protection in China and contribute to the development of more culturally sensitive and effective privacy policies and practices.

The goal of this research is to explore the cultural factors that shape privacy protection in China that may differ from those in the West through a case study of the recent penalty imposed on DiDi for violating data protection regulations. By examining this case from a cultural lens approach, this paper will identify the cultural values and traditions behind privacy concepts and practices in China. In general, this study contributes to a deeper understanding of the complexities and of privacy protection in the Chinese context in comparison with privacy concepts and practices in the West, and offers valuable insights for policymakers, businesses, and individuals concerned with data privacy and protection in China.

Literature Review

Comparing Current Regulations on Privacy Protection

The PIPL in China follows the blueprint of the GDPR and has a similar legal framework. They both aim to protect the personal information of individuals and apply to all entities and individuals involved in processing personal information. The two laws impose severe penalties for non-compliance, such as fines of up to RMB 50 million ($7.7 million) or five percent of an entity's annual revenue as well as criminal liability for serious violations of PIPL while the GDPR violators can face fines of up to four percent of their global annual revenue or €20 million, whichever is greater.

Despite the similarities in content, the PIPL has a different focus and priority compared to the GDPR, which represents the essential Western value for individual privacy. The primary focus of PIPL is to safeguard the interests of individuals, society, and national security. Thus, while the GDPR is based on basic human rights, the PIPL aligns closely with national security (Calzada, 2022). It is evident that PIPL will enhance the Chinese government's ability to regulate data and provide a crucial entry point for international multilateral regulations via cross-border data governance (Yanqing, 2022; Calzada, 2022).

Instead of a single comprehensive law to govern the online privacy protection, the US has a few laws to address how to protect consumers' rights. For instance, the Driver's Privacy Protection Act (DPPA) limits the usage of personal information collected by state Departments of Motor Vehicles (DMVs). Under the DPPA, personal information in motor vehicle records can only be disclosed for specific purposes, such as law enforcement activities, litigation, and government agency operations. The Children's Online Privacy Protection Act (COPPA) imposes specific requirements for the collection and use of personal information of children under the age of 13, including in the context of ride-hailing services. Five states have enacted privacy laws that provide additional protection for personal information, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDPA) (National Conference of State Legislatures, 2022). California Consumer Privacy Act (CCPA) is the first comprehensive data privacy protection law which applies to businesses that collect personal information from California residents. Both CCPA and GDPR aim to protect individuals' personal information and give them more control over how their data is collected, processed, and used. However, CCPA stresses more on business practice. For instance, the CCPA allows individuals to opt out of the sale of their personal information.

The ride-hailing industry in China is primarily regulated by the Cybersecurity Law focusing on network security and infrastructure, the Measures for the Administration of Network Booking Taxi Business for taxi business operations, and the PIPL for individual data protection. There are federal laws in the US that address privacy protections for specific industries, such as HIPAA for healthcare industry and GLBA for financial institutions. The US also has several national legal frameworks, including the Cybersecurity Framework by National Institute of Standards and Technology (NIST) addressing security and data breach issues, the Driver's Privacy Protection Act (DPPA) for drivers' privacy protection, and the Children's Online

Privacy Protection Act (COPPA) for children's online privacy protection. Additionally, the Federal Trade Commission Act (FTC Act) addresses consumers' rights and fair business practices.

Cultural Differences on Privacy

Previous research has found that individuals' online privacy perceptions and decisions are based on their perceived benefits and costs, which vary depending on their cultural background (Trepte et al., 2017; Da Veiga, 2018), such as cultural norms and practices (Trepte et al,, 2017; Li, 2022), privacy literacy and awareness (Baruh, 2017; Fu, 2019), and unique political systems and moral/privacy discourse (Gao & O'Sullivan-Gavin, 2015; Fung & Etienne, 2021). Consumers' privacy perceptions influence people's privacy concepts and behavior as well. For instance, in China, social norms do not always comply with laws and regulations. According to Trepte et al. (2017), "cultural values and norms are decisive for the way online privacy is perceived and negotiated" (p. 4). With the presence of related privacy laws, different cultures interpret them differently and produce outcome against the regulations. The PIPL takes a particularly strong stance on this issue, classifying information of minors, including images, as sensitive information. Organizations processing this information must obtain explicit consent from the minors or their guardians. In February 2023, a female celebrity in China, Lin, expressed her frustration on the social media platform Weibo after finding her six-year-old daughter's birthday photo had been posted online without her consent. Despite her complaints, the photo remained online, with many social media users questioning her desire to protect her daughter's privacy (NetEase, 2023). This incident highlights the discord between privacy laws and cultural norms in China.

While the PIPL closely mirrors the General Data Protection Regulation (GDPR) in Europe, cultural differences can result in blind spots in the interpretation and application of privacy laws in China. As Creemers (2022) notes, the use of a Western legal framework to understand privacy law in China may not accurately reflect the nuances and complexities of privacy in Chinese society.

Fung and Etienne (2021) conducted a comparative analysis of the approach to AI ethics in China and the EU. The authors argue that although both regions have developed similar ethical frameworks for AI, they differ significantly in their underlying philosophical and cultural values, even though they agree on some basic principles. This implies that the same fundamental principles do not necessarily lead to the same interpretation and implementation, and different regions may address or handle similar issues differently. Confucianism's influence emphasizes social harmony and collective well-being, which contrasts with the western approach that prioritizes individual rights and autonomy. Therefore, the Chinese government has taken the lead in developing and enforcing ethical standards (Fung & Etienne, 2021), including privacy discourse (Ma, 2021), while the EU has relied more on self-regulation by the tech industry (Fung & Etienne, 2021). These philosophical and cultural differences have shaped the unique privacy perception in China, as well as the development and implementation of privacy protection. The Chinese government has initiated privacy violation litigation, with DiDi being one of the first examples.

Du and Wang (2020) investigate the privacy practice in online genetic testing providers. Their conclusions indicate the general status of online privacy protection in China. Firstly, privacy laws do not change organizations' privacy practice much. For instance, only one of 83 online providers added an informed consent form for risk notifications after the law was enacted, and only four companies mentioned related laws. Secondly, the privacy policy serves as a disclaimer. In Du and Wang's study, over half of providers did not provide a privacy policy, and all privacy policies functioned as privacy statements without options for consumers. Thirdly, it was a common practice that data sharing practice was not clearly stated nor were opt-out options provided. For example, even though genetic-related data is sensitive information under the PIPL, 62.7% of providers did not mention their data sharing practice.

Both studies conducted by Fung and Etienne (2021) and Du and Wang (2020) imply that privacy protection in China operates differently from western countries due to its underlying cultural influences, unique history, and political systems, which can be explained by Hofstede's cultural dimensions and the Chinese cultural heritage - Confucianism's pursuit of harmony. Hofstede's six cultural dimensions are among the most popular ways to compare cultural differences. These dimensions can be measured by a cultural index, which includes individualism vs collectivism (IDV), power distance (PDI), uncertainty avoidance (UAI), masculinity vs femininity (MAS), long-term orientation vs short-term orientation (LTO), and indulgence vs restraint (IVR) (Hofstede, 2021). Specifically, cultural index can be used to predict individuals' privacy concerns and behaviors (Li, 2022). Applying Western legal concepts to comprehend Chinese legal developments may result in overlooking important cultural aspects of the Chinese legal system that are crucial for comprehending how law is created, applied, and enforced in China (Creemer, 2022).

Individualism vs Collectivism

According to Hofstede (2011), "Right of privacy," "Speaking one's mind is healthy," "Others classified as individuals," and "Personal opinion expected: one person one vote" (p.11) are associated with cultures that place a strong emphasis on individualism. In such cultures, such as in "developed and western countries" (p.12), the right to privacy is highly valued, individuals are encouraged to express their opinions openly, and each person is seen as a unique and independent entity with their own unique characteristics and abilities. Each individual's opinion is expected to carry equal weight. On the other hand, cultures that place a strong emphasis on collectivism tend to prioritize group membership or community. Individuals are typically classified as either in-group or out-group, and opinions and votes may be predetermined by the group. In such cultures, the interests of the group may take precedence over those of the individual. According to Li (2022), China has a collectivistic culture where people identify themselves as part of a group and prioritize the well-being of the group over their individual interests. Consequently, public interests tend to outweigh the importance of individual privacy in such cultures.

Hofstede's observation aligns with Chinese traditional values, where individuals sacrifice their interests for the collective gain or group well-being, considered a virtue and leadership feature for pursuing overall "harmony" (Gao & O'Sullivan-Gavin, 2015). In China, an individual's rights do not carry the same weight as the group. Li et al. (2017) found that high individualistic countries like the US are generally less likely to accept data collection, regardless of the value exchange offered. In contrast, low individualistic countries like China are more likely to accept data collection in exchange for community welfare and other benefits. The study suggests that high individualistic countries, such as the US, do not place as much importance on the community benefit as a value exchange in comparison to low individualistic countries like China. This phenomenon supports the observation that Chinese laws emphasize general welfare and public interests. People in China generally accept wide surveillance based on their faith and value for greater good.

Power Distance

Hofstede's research identified power distance as one of the cultural dimensions that can explain how people from different cultures may view and respond to power, authority, and hierarchy. According to Hofstede's (2011) cultural dimensions theory, small power distance cultures tend to value equality, fairness, and participation in decision-making, while large power distance cultures tend to accept and expect unequal power distribution and may value obedience and respect for authority figures. Cultures with large power distance cultures believe that power determines what is good or evil, and the legitimacy of power is considered irrelevant. Hierarchies in these cultures are often based on social status or age, where obedience is expected from subordinates, children, or those in lower positions. Disobedience is punished as a warning sign to others for future non-compliance. As a result, collectivistic cultures like China tend to place greater

trust in data collected by governments and large organizations, as opposed to individualistic cultures like the United States (Trepte et al., 2017). This may be attributed to their belief in respecting power and accepting the definition of "good or evil" as defined by authorities.

For an example of high-power index culture, Ma (2021) examines the discourse around privacy in Mandarin Chinese news from 2010 to 2019 and found that the Chinese government had been leading the privacy discourse, with multiple regulations and legislations in progress during the peak of privacy topics in 2018. In a culture of high power-distance index (PDI), individuals generally accept unequal power distribution. They may not have significant power to oppose organizations, which often have collectivist characteristics and tend to determine what is considered good or evil, and what is in the public interest. Furthermore, the collectivistic cultural value of seeking unity and harmony to avoid conflict may contribute to a lack of individual lawsuits against organizations for privacy violations or other grievances. Li (2022) suggests that Power Distance is a more effective factor in predicting and explaining how privacy laws are implemented in China. Despite the fact that the Personal Information Protection Law (PIPL) in China has similar content to the General Data Protection Regulation (GDPR) in the European Union, there are significant differences in the way they are implemented.

Privacy Perception: Human Rights vs Confucianism

Privacy is regarded as a fundamental human right in Western countries. Westin (1967) defines privacy as the ability to control one's information, which is related to free will. It is seen as a property that can cause financial damages. Lyon (2007) defines privacy as "the right to control access to personal information" and views privacy protection as social and legal practices to safeguard individuals' personal information from unauthorized access or use (p. 5). In other words, privacy in the West is considered a fundamental right that allows individuals to protect their autonomy and dignity and define their identity.

In contrast, the concept of privacy in Chinese culture does not have an equivalent word or clear-cut definition. The Chinese term for privacy is "*Yinsi*" (隐私), which translates to hidden secret or shameful secret. It carries a negative connotation and is heavily influenced by Confucianism. Traditional beliefs associated moral people with the absence of "*Yinsi*," suggesting that individual privacy was not highly valued. It was only in the 1990s that individual privacy protection became part of Chinese law, and the discourse on consumer privacy emerged in the 2000s with technological advancements (Gao & O'Sullivan-Gavin, 2015).

Previous research has shown that while consumers in China and Western cultures share similar concerns about privacy in areas such as trading, management, and awareness, there are distinct differences in their perception of privacy regarding trading dimensions and the concept of personal information (Chen & Zhang, 2020). Chinese consumers tend to have more concerns about trading information but may not consider the information collected by organizations as personal compared to Western consumers. This difference can be attributed to cultural and historical influences, where privacy is not actively desired and collective unity and harmony are prioritized (Fung & Etienne, 2021).

The significance of privacy and its perception are also reflected in legislation in China. The Civil Code of China (2020) defines privacy as "the undisturbed private life of a natural person and their private space, private activities, and private information that individuals do not want to be known to others." However, privacy under the Civil Code is explicitly related to the traditional definition of "*Yinsi*," referring to personal secrets that individuals do not reveal to others. The term "*Simi*," translating to "private," encompasses personal secrets. While the Civil Code recognizes the right to withhold disclosure of such information, it implies that personal information is not legally protected until the Personal Information Protection Law

(PIPL) regulates its usage. It should be noted that the PIPL does not solely protect individuals' control or ownership of personal information but rather regulates the circumstances under which personal information is protected by law. This indicates that personal information in China does not receive the same level of legal protection as "*Yinsi*" (privacy) and that the concept of privacy is more narrowly defined within the cultural context, intertwined with notions of "shameful secrets" (Liu et al., 2022).

Differentiating privacy violations from personal information violations, Cheng (2019) explains that activities such as collecting and analyzing Internet users' browsing information for personalized recommendations may raise concerns about personal information consent but may not necessarily infringe upon privacy rights. In contrast, activities like installing surveillance devices infringe upon personal tranquility and privacy rights without necessarily involving personal information. In the United States, these scenarios would generally be considered privacy violations, as personal information and privacy are not distinctly separated. Both personal information and privacy fall under the broader scope of privacy rights. Unauthorized collection and analysis of Internet users' browsing information, as well as unauthorized surveillance can still infringe upon individuals' privacy rights and their right to personal tranquility.

In China, the broader concept of "*Rengequan*" (the right to personality) encompasses "*Yinsi*" (privacy) under the umbrella of personal integrity, privacy, and dignity, which are typically protected within the framework of human rights (Cheng, 2019). However, personal information does not receive the same level of legal protection as "*Yinsi*." Cheng (2019) states that "in terms of personal information, its level of legal protection is weaker than that of privacy [*Yinsi*] rights" (p. 41). The PIPL regulates the usage of personal information but does not govern individuals' freedom of control over privacy, which has a broader scope and is considered both a human right and a property right.

Privacy in Western cultures encompasses the scope of " *Yinsi* "(Chinese privacy) and personal information, whereas in China, " *Yinsi*" receives higher legal protection, but personal information does not (Cheng, 2019; Creemers, 2022; Wang et al., 2022; Li, 2022; Liu et al., 2022). Cheng (2019) explains that "natural persons do not have an absolute right and right of dominion over personal information but only have interests that are protected by law" (p. 26).

According to Da Veiga (2018), information privacy culture is about addressing the processing of individuals' information, specifically to meet consumers' expectations that their privacy is protected. Consumers have universal concerns about information collection, unauthorized secondary use, and incorrect information (Da Veiga, 2018; Chen & Zhang, 2020). However, there are distinct cultural differences in what is perceived as privacy and how it should be protected. For example, Chinese consumers tend to prioritize data trading and security over concerns about excessive data collection by organizations, likely due to the higher-power distance culture where people respect authorities and accept the determination of "good" by those in power who control discourse (Li et al., 2017; Chen & Zhang, 2020). Furthermore, privacy itself is mixed with traditional notions of "bad reputation" which cannot be eradicated, and the whole meaning and discourse around privacy is led by the government (Ma, 2021). This indicates that individual privacy should make way for collective good in the Chinese cultural context (Bygrave, 2004; Gao & O'Sullivan-Gavin, 2015; Fung & Etienne, 2021; Li, 2022).

In summary, privacy in Chinese culture differs significantly from the human rights concept prevalent in Western societies. The characteristics of privacy protection in China can be attributed to its historical connotations, the influence of Confucianism, collectivistic and high-power distance cultural norms, and legal distinctions between "*Yinsi*" and personal information. While privacy is seen as a fundamental right in the West encompassing both personal information and broader privacy concepts, China's legal framework and cultural perspectives focus more narrowly on "*Yinsi*" and its association with personal

secrets and dignity. These cultural and legal differences contribute to a unique privacy definition and "privacy culture" in China that diverges from Western societies (Fung & Etienne, 2021; Chen & Zhang, 2021).

Proposed Model

Based on the review of existing research literature, this research proposes a model of cultural factors and differences that influence the privacy concepts and practices in China and the West. Table 1 below presents this model of cultural factors and definitions.

Table 1: Cultural Differences between China and the West

Cultural Differences	Privacy Concepts and Practices in China	Privacy Concepts and Practices in the West
Individualism vs. Collectivism	Privacy is often seen as something that can be sacrificed for the greater public good. For example, individuals may accept privacy intrusions by sharing personal information with employers or organizations if it benefits the community or the overall functioning of the group.	Privacy is considered an individual right and valued for personal autonomy. For example, individuals are assumed to have the right to control over personal data and limit its sharing.
Power Distance	High power distance culture influences privacy decisions, with respect for authority. For example, individuals may comply with government surveillance measures for public security and good or evil are determined by authorities.	Less emphasis on power distance in privacy decisions, with more emphasis on personal autonomy. For example, individuals may challenge government surveillance measures based on individual freedom and privacy.
Social Norms	Privacy is often sacrificed for the collective good. *Yinsi* (narrow scope of privacy) is not culturally respected but recently protected by the Civil Code. For example, job postings with requirements to provide specific age and gender are common practice.	Privacy is regarded as a fundamental human right, and individuals in the West highly value and prioritize their personal privacy. They take steps to limit information sharing, even if it could potentially benefit others. For instance, individuals are cautious about sharing personal information online, proactively restrict access to their social media profiles, and utilize privacy settings to control who can view their personal data.

The table above highlights the cultural differences between China and the West in terms of privacy concepts and practices. In China, privacy is viewed differently, and individuals may willingly share personal information for societal benefits. Additionally, the influence of high-power distance culture can lead to compliance with government surveillance measures. In contrast, privacy in the West is seen as an individual right, with individuals having control over their personal data and being more likely to question or challenge government surveillance. Social norms in China regarding privacy are shaped by the concept of *Yinsi*, which is not culturally respected but protected by the Civil Code. In the West, privacy has a broader concept, with individuals prioritizing their own privacy and limiting information sharing, even if it benefits others. These differences reflect varying perspectives on the importance of individual autonomy and collective well-being in relation to privacy.

Privacy protection is influenced by cultural norms and can vary significantly across different cultures. In Western societies, privacy is generally considered an individual right, while in many Eastern societies, it is seen as a collective good (Bygrave, 2004). Da Vegia (2018) argues that privacy culture varies across nations due to different expectations and perceptions of privacy practices. To gain insights into online privacy protection and culture in China, this study proposes a model that examines three key cultural factors in shaping the perception of privacy protection. The model suggests that privacy protection in China is influenced by Confucian and collectivist cultural values, power distance, and collectivist social norms.

Confucian and collectivist culture play a significant role in shaping privacy perceptions in China. It is worth noting that the concept of privacy in Western countries is different from the Chinese perspective as shown in Figure 1. In Western societies, privacy encompasses a broader range of elements, including *Yinsi* (the Chinese privacy), personal information, and more, which are considered as privacy concerns. However, in Chinese culture, certain aspects that fall under the Western notion of privacy may not be categorized or treated as personal or private matters. For instance, it is common practice in China for job postings to include requirements regarding age, gender, physical appearance, and residency. These requirements are considered relevant to the recruitment process and are not necessarily perceived as privacy concerns within the Chinese context. In contrast, such criteria would typically be regarded as privacy-related information in Western societies and may violate laws.

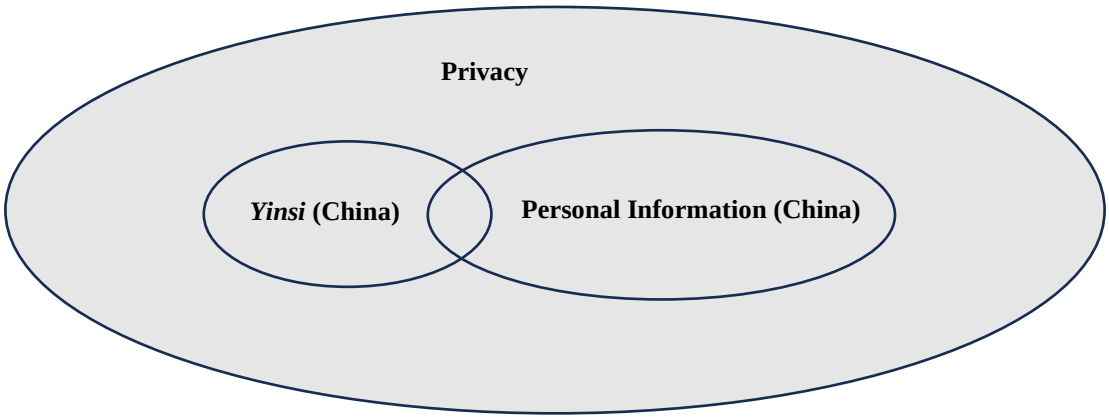

Figure 1: Privacy Scope

Power distance plays a significant role in shaping privacy perceptions in China. The high-power distance culture emphasizes respect for authorities and the acceptance of their decisions as being in the public interest. As a result, what is considered to be done regarding privacy protection is often determined by those who control the discourse and have the power to make decisions.

Collectivist social norms are another key factor of influence on privacy perceptions in Chinese culture. These cultural norms prioritize group harmony and the collective good over individual interests. Therefore, privacy violations involving "outer groups" or entities outside of the collective may be subject to aggressive enforcement.

Overall, this proposed model provides a framework for understanding how cultural factors shape privacy protection in China, highlighting the influence of Confucian and collectivist culture, power distance, and collectivist social norms on the perceived privacy and enforcement of privacy laws.

Methodology: DiDi Case Study

Overview of the DiDi Case

DiDi, a Chinese ride-hailing giant that operates in over 400 cities in China and has expanded globally through investments in Uber and other ride-hailing companies, was listed on the New York Stock Exchange (NYSE) in June 2021 and raised $4.4 billion. However, just two days later, the Cyberspace Administration of China (CAC) announced a cybersecurity review to guard national data security and public interest, prompting DiDi to suspend all new user registrations. DiDi's operations being suspended had a severe impact on the company, causing a loss of revenue of approximately $4.7 billion in the fourth quarter of 2021. This resulted in the company having to cut costs and lay off employees at the beginning of 2022 (Huld, 2022). In December 2021, DiDi announced its delisting from NYSE, and on July 21st, 2022, the CAC announced that DiDi was fined $2.77 billion for illegal collection and use of users' personal data. In addition, the CAC imposed fines of one million Chinese yuan each on DiDi global chairman and chief executive Cheng Wei and President Liu Qing. The penalty also requires DiDi to rectify its data security and privacy protection practices (CAC, 2022).

Violations Cited Per PIPL

According to the Cyberspace Administration of China (CAC) in 2022, DiDi violated the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. The CAC described DiDi's violations as "conclusive evidence, grave circumstances, and despicable character" (Webster, 2022). The violations can be categorized into four categories based on eight items identified by the CAC: excessive data collection, illegal collection of data (without consent or legal basis), illegal processing of data, and other violations such as refusing supervision. Table 2 lists the privacy violations committed by DiDi, including excessive collection of data, illegal collection of data, and illegal processing of data without consent. These violations involved passenger facial recognition information, age group information, occupation information, familial relationship information, home and work addresses, and national identification numbers stored in plain text (Item 3 in Table 2). Additionally, DiDi collected clipboard and application list information, passenger trip intention information, city of residence information, and information on business or travel away from home (Item 2and Item 6 in Table 2), among other things according to CAC.

The CAC announcement indicates that DiDi violated several articles of the Personal Information Protection Law (PIPL). DiDi collected and processed personal information beyond the scope necessary to achieve its business objectives, violating the principles of necessity and minimization, as stated in Article 5 of the PIPL. DiDi's storage of national identification numbers (Item 5 in Table 2) in plain text also violated Article 39 of the PIPL, which requires personal information handlers to adopt technical measures to ensure the security of personal information and prevent unauthorized access, use, disclosure, or destruction of personal information.

DiDi's excessive collection of personal information beyond what is necessary also violated Article 14 of the PIPL, which requires personal information handlers to collect personal information only for legitimate, clear, and specific purposes. Furthermore, DiDi did not clearly notify passengers of the personal information handling purposes, such as users' mobile phone photo albums and device information (Item 1 and Item 8 in Table 2), which violated Article 17 of the PIPL. DiDi also violated Article 19 of the PIPL, which requires personal information handlers to keep user data only for the necessary duration to achieve the purpose of processing.

In conclusion, based on the CAC's review, DiDi's privacy violations violated several articles of the PIPL, including Article 5, Article 14, Article 17, Article 19, and Article 39. Additionally, providing personal information to foreign judicial or law enforcement authorities without approval from competent authorities of China may also be a violation of Article 41 of the PIPL.

Table 2: DiDi Privacy Violations under the PIPL Cited by CAC

Category	Item	Description
Excessive collection of data	2	8.323 billion pieces of user clipboard and application list information
	3	107 million pieces of passenger facial recognition information, 53.5092 million pieces of age group information, 16.3356 pieces of occupation information, 1.3829 million pieces of familial relationship information, and 153 million pieces of home and work address
	4	167 million pieces of precise location information
	5	142,900 pieces of driver personal information and ID
Illegal collection of data	1	11.9639 million pieces of screenshot information and photo albums
	8	inaccurate and unclear explanation of 19 personal information handling purposes
Illegal processing of data without consent	6	53.976 billion pieces of passenger trip intention information, 1.538 billion pieces of city of residence information, and 304 million pieces of information on business or travel away from home
	7	frequently requiring irrelevant "telephone permissions"
Others	"Circumstances grave, and the character despicable"	Poor response to supervising department

In addition, the Cyberspace Administration of China (CAC) cited five reasons for imposing administrative penalties on DiDi in relation to the cybersecurity review. The first reason was DiDi's failure to comply with the supervising department's requirements, which posed serious risks and hidden dangers to national cybersecurity and data security. The other four reasons included privacy violations such as the large-scale collection of personal information, including sensitive data, over a period of seven years, and DiDi's failure to fulfill its cybersecurity and data security protection obligations (Webster, 2022).

Discussion

Cultural Factors in the DiDi Case

Amidst reports and analyses of DiDi's punishment, it is worth noting the emphasis that the CAC placed on DiDi's failure to correct its errors when requested to do so by the authorities. This highlights the significance of high-power distance in Chinese culture, where respect for authority is crucial. Furthermore, the CAC also stressed the severity of the long period of time over which the violations took place and the large volume of information that was handled illegally across several DiDi products. This aligns with the Chinese emphasis on collective good, where actions that harm the community as a whole are heavily punished. It is also interesting to note that none of the violations are related to cross-border data transfer, which is an area of cybersecurity where foreign and multinational companies are more likely to come across than domestic companies, indicating a possible cultural difference. In contrast, the perception of privacy in China may be

different, as evidenced by the fact that DiDi's privacy policy did not change before and after the violations, suggesting a cultural gap in privacy expectations (DiDi, 2021). These cultural factors and their influence on privacy protection practices across cultures will be further as below.

Influence of Collectivism

In terms of the influence of collectivism culture on DiDi's operations, there are three key points to consider in relation to the recent fines imposed on the company. Firstly, the large scale of excessive and potentially illegal data collections are common practices in China due to a lack of strict privacy laws and regulations. Secondly, CAC's explanation during the Q & A session highlights the importance of national security concerns, which is a distinct characteristic of collectivist culture. This is because any risk to the group interests will draw much attention than other circumstances. Thirdly, DiDi has been strategically partnering with local Chinese governments to share its technology and a trove of data, for instance, the “social credit systems” and a “cashless” society (Chan & Kwok, 2022, p. 140), which is considered for the greater good of creating a safe society. When the large scale and seven years privacy violations have been doing good, or "everybody" is doing the same thing - collecting data without consent, then violations become acceptable and not seen as illegal, which is expressed as "情有可原" in Chinese and translates to "understandable," "justifiable," or "excusable."

Furthermore, when comparing privacy violations cases in China to those in the US, there are significant cultural differences between individualistic cultures and collectivistic cultures. There are limited reports or public records about privacy violations even after the PIPL became effective, and there have been no cases reported and initiated by individuals against organizations for privacy violations in China. In contrast, according to Violation Tracker, in 2023, seven out of twelve privacy violation cases were private lawsuits initiated by individuals or organizations (see Table 3). In the US, three out of four lawsuits against Uber for privacy violations were initiated as private lawsuits.

Overall, the influence of collectivism on DiDi's privacy violations and the lack of individual lawsuits on privacy violations in China (LawInfoChina, n.d.) highlights the importance of cultural factors when it comes to privacy issues and legal actions. It is essential to consider cultural differences when discussing privacy policies and to ensure that legal and ethical standards are in place to protect individuals' rights.

Table 3: Privacy Violation Lawsuit in 2023 (Good Jobs First, n.d.)

Company	Primary Offense Type	Initiating Agency
Zywave Inc.	privacy violation	private lawsuit-federal
Life Hope Labs	privacy violation	HHSOCR
GoodRx Holdings Inc.	privacy violation	FTC
Banner Health	privacy violation	HHSOCR
Snap Finance LLC	privacy violation	private lawsuit-federal
DNA Diagnostics Center	privacy violation	MULTI-AG
NFI Industries Inc.	privacy violation	private lawsuit-federal
DirecTV	privacy violation	private lawsuit-federal
Forefront Dermatology SC	privacy violation	private lawsuit-federal
Ambry Genetics	privacy violation	private lawsuit-federal
Aeries Software Inc.	privacy violation	private lawsuit-federal
GoodRx Holdings Inc.	privacy violation	DOJ_CIVIL

Influence of Power-Distance

The timeline of the cybersecurity review of DiDi reflects the strong influence of Chinese traditional culture, which emphasizes higher power distance and obedience from subordinates. This is evident from the sequence of events that occurred. Prior to DiDi's planned listing on the US stock exchange, signals were released to warn DiDi to delay its listing (Wei & Zhai, 2021). Two days after DiDi went public, the Cyberspace Administration of China (CAC) announced the investigation, which led to DiDi's removal from Chinese app stores. Despite government recognitions of DiDi's accomplishments in job creation and partnership with local governments, DiDi received punishment for "maliciously evading supervision." (Webster, 2021). This suggests that the higher power distance in Chinese culture may have influenced the government's decision to punish DiDi for not complying with its regulations, even though DiDi is seen as a successful and well-respected company in China.

It is worth noting that the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law were not in effect in 2015 when DiDi first violated related laws. The Cybersecurity Law was enacted in 2017, the Data Security Law in 2021, and the Personal Information Protection Law in 2020. However, there were other laws and regulations related to data security and privacy that were in effect in China in 2015, including the General Principles of the Civil Law, the Law on Protection of Consumer Rights and Interests, and the Regulation on Protection of Personal Information of Telecommunications and Internet Users. However, the CAC still fined DiDi under the three new laws without providing detailed explanations.

In contrast, a data breach resulting in the theft of 48.5 million pieces of personal information occurred in 2022 from Shanghai police systems due to system vulnerabilities (Baptista, 2022). However, there have been no further reports about the investigation, nor have there been reports challenging the excessive data collections from the government. This implies that the acceptance of data collection for public good and the government's power decide what should be protected and in what ways.

Confucian and Collective Culture Norm

DiDi's privacy policy was updated on July 8, 2021, a few days after the CAC announced its cybersecurity investigation (DiDi Global, 2021). The current policy supported the CAC's accusations, such as excessive precise location collection and illegal and excessive information collection, including sensitive information. From the policy content, it appears that DiDi has not corrected its operations to comply with the laws. However, no privacy-related reports or complaints against its continuous violations have been found. This may imply that the excessive data collection, including sensitive information, could be justified as being for safety reasons or evidence for consumer service disputes. Chinese consumers may not view this information collection as a violation of privacy due to Confucian and collective cultural norms or limited privacy perception in a narrow context (Gao & O'Sullivan-Gavin, 2015, p. 236). The conclusion that "Chinese Internet users' awareness of their right to privacy is weak" (Fu et al., 2019) could be explained by different perceptions on privacy between Eastern and Western cultures.

DiDi's Privacy Practice: Personal Information Protection and Privacy Policy

DiDi's privacy policy is 19,655 words, 31 pages, which requires 39-65 minutes to read (based on the average reading rate of 300-500 Chinese characters per minute). Although DiDi mentions third parties and their privacy policies in the document, no links are provided to access them. The link provided to associated companies that DiDi shared data with is plain text with company names only, with no further link to control

data sharing. The only option users have is to turn off personalized service (advertisements), which is hidden in the plain text. Consumers need to read the whole policy to find it.

Overall, DiDi has not changed its privacy practices based on its updated privacy policy. No reports were found to indicate that DiDi's continuous violations have been reported, which may suggest that DiDi's excessive data collection is now under the umbrella of public safety and customer service, and that the CAC may have achieved its goal of punishing disobedience and warning privacy violations.

In the DiDi case, several cultural and societal factors may be influencing privacy perceptions and regulations in China. These include the emphasis on collectivism, which prioritizes group harmony and unity over individual rights and privacy. Additionally, China has a high-power distance, which means that individuals may be less likely to question or challenge authority figures, including the government's regulations on data privacy. Confucian and Collective Culture Norms also play a role in shaping privacy perceptions in China, as individuals may be more willing to share personal information with large organizations and trust that it will be used in their best interest.

Conclusion

Case studies are useful in providing in-depth analysis of a particular phenomenon, entity, or situation. The DiDi case study offers a valuable insight into China's unique privacy culture, which is influenced by Confucianism, particularly collectivism, high power distance, and a narrow perception of privacy. Despite legal changes, social norms and technological advancements do not always align with these changes.

This study proposes a model of cultural factors and cross-cultural differences, emphasizing as Confucian and collectivist culture's influence on privacy protection in Chinese culture. It also highlights the role of high-power distance in determining what is considered in the public interest or collective good. Moreover, the model suggests the possibility of strict enforcement of privacy violations involving "outer groups" due to collectivist cultural norms in China.

Limitations of this study include its narrow focus on the case of DiDi and possible limited access to relevant data. Future studies could expand the analysis to other companies and industries in China to better understand how cultural factors impact privacy protection in different contexts. Further research could also explore other cultural factors beyond Confucianism that may influence privacy perception and protection in China.

Qualitative research, such as interviews or focus groups with Chinese citizens and privacy experts, could provide a deeper understanding of their perspectives on privacy and cultural influences. Such knowledge could help organizations comply with the PIPL more efficiently by knowing what and why actions need to be taken and meeting users' expectations.

In addition, future research should address dynamics in cultural factors on privacy concepts and practices, which may be changing with increasing globalization and cross-cultural communication. Cranor and Habib (2022) present specific metrics for usable privacy policy/consent interfaces that are generally desirable in the western cultures to address user needs and options in privacy protection. Consumers in China have expressed greater concerns about data leaks and trading (Chan & Zhang, 2020). It would be valuable to research into cross-cultural influence and acceptance of privacy protection practices.

References

Baptista, E. (2022, August 12). Hacker offers to sell data of 48.5 million users of Shanghai's COVID app. Reuters. https://www.reuters.com/world/china/hacker-offers-sell-data-485-mln-users-shanghais-covid-app-2022-08-12/.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A Meta-Analytical review. Journal of Communication, 67(1), 26-53. https://doi.org/10.1111/jcom.12276

Bygrave, L. A. (2004). Privacy protection in a global context–a comparative overview. Scandinavian Studies in Law, 47(2004), 319-348.

Cheng, X. (2019). 民法典编纂视野下的个人信息保护 [Personal information protection from the perspective of Civil Code compilation]. China Legal Science, 2019(4), 71–73. https://doi.org/10.14111/j.cnki.zgfx.2019.04.002

Cranor, L. F., & Habib, H. (2023). Metrics for success: Why and how to evaluate privacy choice usability. Communications of the ACM, 66(3), 35-37.

Cyberspace Administration of China (CAC). (2022, July 21). 国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定 [Decision on the administrative penalty for DiDi Global Inc. in accordance with the cybersecurity review]. http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3), 1129-1150. https://doi.org/10.3390/smartcities5030057

Chan, N. K., & Kwok, C. (2021). The politics of platform power in surveillance capitalism: A comparative case study of ride-hailing platforms in China and the United States. Global Media and China, 7(2), 131–150. https://doi.org/10.1177/20594364211046769

Chen, X., & Zhang, Y. (2020). The construct of information privacy concerns in the Chinese cultural setting. Nankai Business Review International, 12(1), 42–55. https://doi.org/10.1108/nbri-12-2019-0071

Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1). https://doi.org/10.1093/cybsec/tyac011

Da Veiga, A. (2018). An information privacy culture instrument to measure consumer privacy expectations and confidence. Information & Computer Security, 26(3), 338–364. https://doi.org/10.1108/ics-03-2018-0036

DiDi Global. (2021, July 8). Personal information protection and privacy policy. https://www.DiDiglobal.com/read?file=//img-ys011.DiDistatic.com/static/DiDiglobal/do1_jBkIDkuslnB87lR6Pea9&nam

Du, L., & Wang, M. (2020). Genetic privacy and data protection: A review of Chinese direct-to-consumer genetic test services. Frontiers in Genetics, 11. https://doi.org/10.3389/fgene.2020.00416

Fung, P., & Etienne, H. (2021). Confucius, cyberpunk and Mr. Science: Comparing AI ethics between China and the EU. arXiv preprint arXiv:2111.07555.

Fu, T. (2019). China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent. Global Media and Communication, 15(2), 195-213. https://doi.org/10.1177/1742766519846644

Gao, Z., & O'Sullivan-Gavin, S. (2015). The development of consumer privacy protection policy in China: a historical review. Journal of Historical Research in Marketing, 7(2), 232-255.

Good Jobs First. (n.d.). Violation Tracker [Data file]. https://violationtracker.goodjobsfirst.org/

Huld, A. (2022, September 19). DiDi cybersecurity review - Which laws did DiDi break? China Briefing News. Retrieved May 23, 2023 from https://www.china-briefing.com/news/DiDi-cyber-security-review-which-laws-did-DiDi-break/

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. Online Readings in Psychology and Culture, 2(1). https://doi.org/10.9707/2307-0919.1014

LawInfoChina. (n.d.). LawInfoChina database. https://www.lawinfochina.com/search/SearchCase.aspx

Li, Y. (2022). Cross-Cultural Privacy Differences. In (pp. 267-292). Springer International Publishing. https://doi.org/10.1007/978-3-030-82786-1_12

Li, Y., Kobsa, A., Knijnenburg, B. P., & Carolyn Nguyen, M.-H. (2017). Cross-Cultural Privacy Prediction. Proceedings on Privacy Enhancing Technologies, 2017(2), 113–132. https://doi.org/10.1515/popets-2017-0019

Liu, Y., Huang, L., Yan, W., Wang, X., & Zhang, R. (2022). Privacy in AI and the IOT: The Privacy Concerns of smart speaker users and the Personal Information Protection Law in China. Telecommunications Policy, 46(7), 102334. https://doi.org/10.1016/j.telpol.2022.102334

Lyon, D. (2007). Surveillance studies: An overview. Cambridge, UK; Malden, MA: Polity.

Ma, Y. (2021). A structural topic model analysis of privacy in Mandarin Chinese News: 2010–2019. Proceedings of the Association for Information Science and Technology, 58(1), 792–794. https://doi.org/10.1002/pra2.564

National People's Congress of the People's Republic of China. (2020). Civil Code of the People's Republic of China (English Version). http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf

NetEase. (2023, February 5). Lin Xinyu protects daughter for 6 years, only to be betrayed by a friend and angrily scolds media for exposing daughter's frontal photos [Weibo post]. NetEase. https://www.163.com/dy/article/HSQF4BU10517BIU3.html

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. Social Media + Society,3(1), 205630511668803. https://doi.org/10.1177/2056305116688035

Wang, C., Zhang, J., Lassi, N., & Zhang, X. (2022). Privacy protection in using artificial intelligence for healthcare: Chinese regulation in comparative perspective. Healthcare, 10(10), 1878. https://doi.org/10.3390/healthcare10101878

Webster, G. (2022, July 22). Translation: Chinese authorities announce $1.2B fine in DiDi case, describe "despicable" data abuses. DigiChina. https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-DiDi-case-describe-despicable-data-abuses/

Wei, L., & Zhai, K. (2021, July 6). Chinese regulators suggested DiDi delay its U.S. IPO. The Wall Street Journal. https://www.wsj.com/articles/chinese-regulators-suggested-DiDi-delay-its-u-s-ipo-11625510600

Westin, A. (1967). Privacy and freedom New York: Atheneum, 1967. Privacy and Personnel Records, The Civil Liberties Review (Jan./Feb.,1976) S, 28-34.

Yanqing, H. "Game of Laws": Cross-Border Data Access for Law Enforcement Purposes: Models in the United States, Europe, and China; Beijing Institute of Technology School of Law: Yale, MI, USA, 2022; pp. 1–16.

Zhong, R. (2021, April 10). China fines Alibaba $2.8 billion in landmark antitrust case. The New York Times. https://www.nytimes.com/2021/04/09/technology/china-alibaba-monopoly-fine.html