INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Going global: Comparing Chinese mobile applications' data and user privacy governance at home and abroad

Lianrui Jia
University of Toronto, Canada, lianrui.jia@gmail.com

Lotus Ruan
Citizen Lab, University of Toronto, Canada, lotusruan@citizenlab.ca

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1502

Abstract: We examine and compare data and privacy governance by four China-based mobile applications and their international versions: Baidu, Toutiao and its international version TopBuzz, Douyin and its international version TikTok, and WeChat. Together, these four applications represent popular Chinese apps branching into diverse overseas markets such as Europe, Brazil, North America, and Southeast Asia. We first present an overview of the ownership, functions, business models and strategies of the reviewed apps. To study the app's interface design, we employ the walkthrough method to examine privacy features during the account registration and deletion stages in app usage. Lastly, we conducted content analysis of the terms of service and privacy policies to establish the app's data collection, storage, transfer, use, and disclosure measures. Our analysis showed variations across apps and within the Chinese and international-facing versions in their data and privacy governance in app design and policies. Baidu has the most unsatisfactory data and privacy protection measures, while ByteDance's TikTok/Douyin and TopBuzz/Toutiao offer more comprehensive user protection from different jurisdictions. Moreover, this paper highlights the role of platform owners (e.g., Google and Apple) in gatekeeping mobile app privacy standards and the role of the state in imposing a data protection framework on overseas versions of China-based mobile apps.

Keywords: Data protection, China, Mobile apps, Globalisation

Article information

Received: 26 Sep 2019 **Reviewed:** 20 Dec 2019 **Published:** 16 Sep 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/going-global-comparing-chinese-mobile-applications-data-and-user-privacy

Citation: Jia, L. & Ruan, L. (2020). Going global: Comparing Chinese mobile applications' data and user privacy governance at home and abroad. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1502

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

In February 2019, the short video sharing and social mobile application TikTok was fined a record-setting penalty (US$ 5.7 million) for violating the Children's Online Privacy Protection Act by the US Federal Trade Commission for failing to obtain parental consent and deliver parental notification. TikTok agreed to pay the fine (Federal Trade Commission, 2019). This settlement implies several significant developments. Owned by the Chinese internet company ByteDance, TikTok is popular worldwide, predominantly among young mobile phone users, while most commercially successful Chinese internet companies are still based in the Chinese market. Such global reach and commercial success makes Chinese mobile applications pertinent sites of private governance on the global scale (see Cartwright, 2020, this issue). China-based mobile applications therefore need to comply with domestic statutory mechanisms as well as privacy protection regimes and standards in the jurisdictions as they expand outward, such as the extraterritorial application of Article 3 of the EU's General Data Protection Regulation (GDPR).

To examine how globalising Chinese mobile apps respond to the varying data and privacy governance standards when operating overseas, we compare the Chinese and overseas version of four sets of China-based mobile applications: (1) Baidu mobile browser - a mobile browser with a built-in search engine owned and developed by Chinese internet company Baidu, (2) Toutiao and TopBuzz - mobile news aggregators developed and owned by ByteDance, (3) Douyin and TikTok - mobile short video-sharing platforms developed and owned by ByteDance, with the former only available in Chinese app stores and the later exclusively in international app stores, and (4) WeChat and Weixin - a social application developed and owned by Chinese internet company Tencent. Together, these four mobile applications represent a global reach of flagship China-based mobile apps and a wide range of functions: search and information, news content, short videos and social. They also represent a mix of more established (Baidu, Tencent) and up-and-coming (ByteDance) Chinese internet companies. Lastly, this sample also demonstrates the varying degree of commercial success as they all offer services globally, with Baidu browser the least commercially successful, and TikTok the most successful.

An earlier study shows that Chinese web services had a bad track record in privacy protection: back in 2006, before China had in place a national regime of online privacy protection, among 82 commercial websites in China, few websites posted a privacy disclosure and an even fewer number of websites followed the four fair information principles of notice, choice, access and security (Kong, 2007). These four principles are to enhance self-regulation of the internet industry by providing consumers notice, control, security measures, and ability to view and contest the accuracy and completeness of data collected about them (Federal Trade Commission, 1998). In 2017, only 69.6 percent of the 500 most popular Chinese websites had disclosed their privacy policies (Feng, 2019). These findings suggest a significant gap between data protection requirements on paper and protection in practice (Feng, 2019). In a recent study, Fu (2019) finds improvement of the poor privacy protection track record of the three biggest internet companies in China (Baidu, Alibaba, and Tencent). Her study shows that BAT's privacy policies are generally compliant with the Chinese personal information protection provisions but lack sufficient considerations to transborder data flows and in the case of change of ownership (such as merger and acquisitions (Fu, 2019). Moreover, the privacy policies of BAT offer more notice than choice—that user either is forced to accept the privacy policy or forego the usage of the web services (Fu, 2019, p. 207). Building on these findings, this paper asks: does the same app differ in data and privacy protection measures between international and Chinese versions? How are

these differences registered in the app's user interface design and privacy policies?

In the following analysis, we first outline the evolving framework of data and privacy protection that governs the design and operation of China-based mobile apps. The next section provides a background overview of key functions, ownership information, business strategies of examined apps. The walkthrough of app user interface design studies how a user experiences privacy and data protection features in various stages of app usage. Last, we present the comparison of privacy policies and terms of service between the two versions of the same China-based apps to identify the differences in data and privacy governance. We find that not only different apps vary in data and privacy protection, the international and Chinese versions of the same app also show discrepancies.

GOVERNANCE '*OF*' GLOBALISING CHINESE APPS

Law and territory has always been at the centre of debates in the regulation and development of the internet (Goldsmith & Wu, 2006; Kalathil & Boas, 2003; Steinberg & Li, 2016). Among others, China has been a strong proponent of internet sovereignty in global debates about internet governance and digital norms. The 2010 white paper titled *The Internet In China* enshrines the concept of internet sovereignty into the governing principles of the Chinese internet. It states: "within Chinese territory the internet is under the jurisdiction of Chinese sovereignty" (State Council Information Office, 2010). The principle of internet sovereignty was later reiterated by the Cyberspace Administration of China (CAC), the top internet-governing body since 2013, to recognise "each government has the right to manage its internet and has jurisdiction over information and communication infrastructure, resources and information and communication activities within their own borders" (CAC, 2016).

Under the banner of internet sovereignty, the protection of data and personal information in China takes a state-centric approach, which comes in the form of government regulations and government-led campaigns and initiatives. The appendix outlines key regulations, measures and drafting documents. Without an overarching framework for data protection, China's data protection approach is characterised in a "cumulative effect" (de Hert & Papakonstantinou, 2015), which is composed of multitude of sector-specific legal instruments, promulgated in a piecemeal fashion. While previous privacy and data protection measures are dispersed across various government agencies, laws and regulation, the first national standard for personal data and privacy protection was put forth only in 2013. The promulgation of the *Cybersecurity Law* in 2016 is a major step forward in the nation's privacy and data protection efforts, despite the policy priority of national security over individual protection. Article 37 of the *Cybersecurity Law* stipulates that personal information and important data collected and produced by critical information infrastructure providers during their operations within the territory of the People's Republic of China shall be stored within China. Many foreign companies have complied either as a preemptive goodwill gesture or as a legal requirement in order to access, compete, and thrive in the Chinese market. For example, in 2018, Apple came under criticism for moving the iCloud data generated by users with a mainland Chinese account to data management firm Guizhou-Cloud Big Data - a data storage company of the local government of Guizhou province (BBC, 2016). LinkedIn, Airbnb (Reuters, 2016), and Evernote (Jao, 2018) have stored mainland user data in China, even prior to the promulgation of the *Cybersecurity Law*. The Chinese government asked transnational internet companies to form joint ventures with local companies to operate data storage and cloud computing businesses, such as Microsoft Azure's cooperation with Century Internet and Amazon AWS-Sinnet technology (Liu, 2019).

The Chinese state participates in a wide range of online activities including, among other things, data localisation requirements for domestic and foreign companies (McKune & Ahmed, 2018). The Chinese government attributes data localisation requirements to national security and the protection of personal information on the basis that the transfer of personal and sensitive information overseas may undermine the security of data (Xu, 2015). While others point out the recurring themes of the ideological tradition of technological nationalism and independence as Cyberspace Administration of China's prioritisation of security over personal privacy and business secrets (Liu, 2019). Captured in President Xi's speech "without cybersecurity comes no national security", data and privacy protection is commonly framed under the issue of internet security (Gierow, 2014).

There is a growing demand for the protection of personal information among internet users and a growing number of government policies pertaining to the protection of personal information in China (Wang, 2011). Since 2016, the Chinese government is playing an increasingly active role in enforcing a uniform set of rules and standardising the framework of privacy and data protection. As of July 2019, there are 16 national standards, 10 local standards and 29 industry standards in effect that provide guidelines on personal information protection. However, there is no uniform law or a national authority to coordinate data protection in China. The right to privacy or the protection of personal information (the two are usually interchangeable in the Chinese context) often comes as an auxiliary article along with the protection of other rights. Whereas jurisdictions such as the EU have set up Data Protection Authorities (DPAs) - that are independent public entities that supervise the compliance of data protection regulations, in China the application and supervision of data protection has fallen on private companies and state actors respectively. User complaints against the violation of data protection laws are mostly submitted to, and handled by, private companies themselves rather than an independent agency. This marks the decisive difference underlying China's and the EU's approach to personal data processing: in China, data protection is aimed exclusively at the individual as consumer, versus in the EU, the data protection recipient is regarded as an individual or a data subject and protection of personal data is both a fundamental right and is conducive to the trade of personal data within the Union, as stipulated in Article 1 of the General Data Protection Regulation (de Hert & Papakonstantinou, 2015).

The pre-existing legal modicum and self-regulatory regime of privacy and data protection by Chinese internet platform companies gives rise to rampant poor privacy and data protection practices, even among the country's largest and leading internet platforms. Different Chinese government ministries have also tackled the poor data and privacy regulation of mobile apps and platform in rounds of "campaign style" (□□□□□) regulation—a top down approach often employed by the Chinese government to provide solutions to emerging policy challenges (Xu, Tang, & Guttman, 2019). For instance, Alibaba's payment service Alipay, its credit scoring system Sesame Credit, Baidu, Toutiao, and Tencent have all shown poor track records of data and privacy protection and have come under government scrutiny (Reuters, 2018). Alipay was fined by the People's Bank of China in 2018 for collecting users' financial information outside the scope defined in the Cybersecurity Law (Xinhua, 2018). The Ministry of Industry and Information Technology publicly issued a warning to Baidu and ByteDance's Toutiao for failing to properly notify users about which data it is collecting (Jing, 2018).

As China experienced exponential mobile internet growth, mobile apps stand out as a poignant regulatory target. The Cyber Administration of China put forth the *Administrative Rules on Information Services via Mobile Internet Applications* in 2016 that distinguishes the duties for mobile app stores and mobile apps. Mobile apps, in particular, bear six regulatory

responsibilities: 1) enforce real name registration and verify the identity of users through cell phone number or other personally identifiable information, 2) establish data protection mechanism to obtain consent and disclose the collection and use of data, 3) establish fulsome information gatekeeping mechanisms to warn, limit, suspend accounts that post content that violate laws or regulations, 4) safeguard privacy during app installation processes, 5) protection of intellectual property, 6) obtain and store user logs for sixty days.

As more China-based digital platforms join the ranks of the world's largest companies by measures of user population, market capitalisation and revenues (Jia & Winseck, 2018), various scholarly studies have already started to grapple with the political implications of their expansion. Existing studies call for attention to the distinctions between global and domestic versions of the same Chinese websites and mobile applications in information control and censorship activities and results show Chinese mobile apps and websites are lax and inconsistent at content control when they go global (Ruan, Knockel, Ng, & Crete-Nishihata, 2016; Knockel, Ruan, Crete-Nishihata, & Deibert, 2018; Molloy & Smith, 2018). To ameliorate these dilemmas, some China-based platforms have designed different versions of their products that serve domestic and international users separately. Yet, data and privacy protection of Chinese mobile apps is under-studied, especially as they embark on a global journey. This is ever more pressing an issue as Chinese internet companies that have been successful at growing their international businesses, such as Tencent and ByteDance, simultaneously struggle to provide a seamless experience for international users and complying with data and content regulations at home.

METHODS

We employ a mixed-method approach to investigate how globalising Chinese mobile apps differ in data and privacy governance between Chinese and international versions accessed through Canadian app stores. While Baidu Search, TikTok, WeChat, and Topbuzz do not appear to have region-based features, the actual installation package may or may not differ based on where a user is based and downloads the apps from. First, we conducted an overview of tested mobile apps and functions, looking at issues of ownership, revenue, user population. Each app's function and business model has a direct bearing on the data collection and usage. Secondly, to study how mobile apps structure and shape end users' experience with regards to data and privacy protection, we deployed the walkthrough method (Light, Burgess, & Duguay, 2018). We tested both the Android and iOS version of the same app. In the case of China-based apps (i.e., Douyin & Toutiao), we downloaded the Android version from the corresponding official website of each service and the iOS version from the Chinese regional Apple App Store. For the international-facing apps (i.e., TikTok and TopBuzz), we downloaded their Android versions from the Canadian Google Play Store and the iOS version from the Canadian Apple App Store. Baidu and WeChat do not offer separate versions for international and Chinese users; instead, the distinction is made when users register their account. After we downloaded each app, we systematically stepped through two stages in the usage of the apps: app entry and registration, and discontinuation of use. We conducted the walkthrough on multiple Android and Apple mobile devices in August 2019.

In addition, we conducted content analysis of the privacy policies and terms of service of each mobile app. These documents demonstrate the governance by mobile apps as well as the governance of mobile apps within certain jurisdictions. They are also key legal documents that set the conditions of user's participation online and lay claim to the institutional power of the

state (Stein, 2013). We examined a total of 15 privacy policies and terms of service in Chinese and English language, retrieved in July 2019. Here are the numbers of documents we examined for each app: Baidu (2), Weixin (2), WeChat (2), TopBuzz (2), TikTok (3), Douyin (2), Toutiao (2). We then conducted content analysis of mobile app privacy policies and terms of service along five dimensions: data collection, usage, disclosure, transfer, and retention. For data collection, we looked for items that detailed the types of information collected, the app's definitions of personally identifiable information, and the possibility to opt out of the data collection process; for data usage, we looked for terms and conditions that delineated third party use; for disclosure, we looked at whether the examined app would notify its users in case of privacy update, merger and acquisitions, and data leakages; for data transfer and retention, we examined whether app specified security measures such as encryption of user data, emergency measures in case of data leaks, terms and conditions of data transfer, as well as the specific location and duration of data retention.

RESEARCH LIMITATIONS

Due to network restrictions, our walkthrough is limited to the Canadian-facing versions of these China-based apps. For each mobile app we studied, its parent company offers only one version of an international-facing app and one version of a China-facing app on the official website. Yet, even though there is only one international-facing app for each of the products we analysed, it remains to be tested whether the app interface, including the app's notification setting differs when downloaded and/or launched in different jurisdictions. Moreover, our research is based on a close reading of the policy documents put together by mobile app companies. It does not indicate whether these companies actually comply with their policy documents in the operation of services, or the pitfalls of notice and consent regime (Martin, 2013). Existing research has already shown that under the Android system, there are many instances of potential inconsistencies between what the app policy states and what the code of the app appears to do (Zimmeck et al., 2016).

OVERVIEW OF APPS

BAIDU SEARCH

Baidu App is the flagship application developed by Baidu, one of China's leading internet and platform companies. The Baidu App provides the search function but also feeds users highly personalised content based on data and metadata generated by users. Often regarded as the Chinese counterpart of Google, Baidu's main business includes online search, online advertising and artificial intelligence. In 2018, the daily active users of Baidu app reached 161 million, a 24% jump from 2017. Although Baidu has embarked on many foreign ventures and expansion projects, according to its annual report, the domestic market still accounts for 98% of Baidu's total revenue for 2016, 2017, and 2018 consecutively. Based on revenue composition, Baidu's business model is online advertising. The major shareholders of Baidu are its CEO Robin Yanhong Li (31.7%) and Baillie Gifford (5.2%), an investment management firm headquartered in Edinburgh, Scotland.

TIKTOK VS DOUYIN, TOPBUZZ VS TOUTIAO

TikTok, Douyin, TopBuzz and Toutiao are among the flagship mobile apps in ByteDance's portfolio. ByteDance represents a new class of up-and-coming Chinese internet companies competing for global market through diversification, merger and acquisitions of foreign apps. ByteDance acquired US video app Flipagram in 2017, France-based News Republic in 2017, and

invested in India-based news aggregator Dailyhunt. TikTok, first created in 2016, was rebranded with ByteDance's US$ 1 billion acquisition of Muscial.ly in 2018. The Chinese version of TikTok, Douyin, was released in 2016 by ByteDance as the leading short-video platform in the country. The Douyin app has several different features that are particular to the Chinese market and regulation. For example, the #PositiveEnergy was integrated into the app as an effort to align with the state's political agenda to promote Chinese patriotism and nationalism (Chen, Kaye, & Zeng, 2020). Douyin also differs from TikTok in the app's terms of service, of which it states that content undermining the regime, overthrowing the socialist system, inciting secessionism, and subverting the unification of the country is forbidden on the platform (Chen, Kaye, & Zeng, 2020; Kaye, Chen, & Zeng, 2020). Such regulation does not exist on TikTok. ByteDance's Chinese news and information app Toutiao was launched in 2012, followed by its English version TopBuzz in 2015, for the international market.

Dubbed as the "world's most valuable startup" (Byford, 2018), ByteDance secured investment from Softbank and Sequoia Capital. ByteDance has made successful forays into North American, European and Southeast Asian markets, reaching 1 billion monthly active users globally in 2019 (Yang, 2019). It is one of the most successful and truly global China-based mobile apps. The company focuses on using artificial intelligence (AI) and machine learning algorithms to source and push content to its users. To accelerate its global reach, ByteDance sources its top-level management from Microsoft and Facebook for AI and global strategy development.

Both apps and their overseas versions have received much legal and regulatory scrutiny. In 2017, Toutiao was accused of spreading pornographic and vulgar information by the Beijing Cyberspace and Informatisation Office. In the 2018 Sword Net Action, China's National Copyright Administration summoned Douyin to better enforce copyright law and put in place a complaint mechanism to report illegal content (Yang, 2018). Reaching millions of youth, TikTok was temporarily banned by Indian court and Indonesia's Ministry of Communication and Information Technology for "degrading culture and encourag[ing] pornography" and for spreading pornography, inappropriate content and blasphemy. TikTok attempted to resolve the ban by building data centres in India while hiring more content moderators (Sharma & Niharika, 2019).

WECHAT/WEIXIN

WeChat or *Weixin* is China's most popular mobile chat app and the fourth largest in the world. It is a paradigmatic example of the infrastructurisation of platforms, where the app bundles and centralises many different functions, such as digital payment, group buying, taxi hailing into one super-app (Plantin & de Seta, 2019). Owned by Tencent, one of China's internet behemoths, WeChat has a user base of 1 billion, though Tencent has not updated the number of its international users since 2015 (Ji, 2015). WeChat's success was built upon Tencent's previous social networking advantages.

Unlike ByteDance which separates its domestic and international users by developing two different versions of its major products (i.e., the internationally-facing TikTok can only be downloaded in international app stores whereas Douyin can only be downloaded in Chinese app stores and Apple's China-region App Store), Tencent differentiates WeChat (international) and Weixin (domestic) users by the phone number a user originally signs up with. In practice, users download the same WeChat/Weixin app from either international or Chinese app stores. The app then decides whether the user is an international or Chinese user during the account registration process. Besides certain functionalities such as Wallet that is exclusive to Chinese users, the overall design of the app and the processes of account registration and deletion are

the same for international and domestic users.

APP WALKTHROUGH

We conducted app walkthroughs to examine and compare user experience in data and privacy protection during the app registration and account deletion process. Figure 1 compares the walkthrough results.

ANDROID-IOS DIFFERENCE

Registration processes for Baidu, Douyin, Toutiao and WeChat differ between the Android and iOS versions. The Android and iOS registration processes for TopBuzz and TikTok are similar, therefore they are recorded in one timeline in Figure 1. In general, app registrations on iOS devices comprise of more steps compared to Android, meaning that the apps need to request more function-specific authorisation from users. In the Android versions, access to certain types of data is granted by default when users install and use the app; users need to change authorisations within the app or on the device's privacy settings. For example, TopBuzz and TikTok, both owned by ByteDance, set app push notifications as the default option without prompting for user consent. If users want to change the setting, they need to do so via their device's privacy settings.

"ASK UNTIL CONSENT"

All Chinese versions of apps will prompt a pop-up window displaying a summary of privacy notification, while this is not the case for the Canadian version. However, the pop-up reminder for privacy notification does not give the users a choice to continue usage of the app without ticking "I agree". For example, if you do not agree with the privacy reminder, the app will show the notice again until user consent is obtained to proceed to the next step. This is a reflection of the failure of the notice and choice approach to privacy protection that the users are left without a choice but to accept the terms or relinquish the usage of the app (Martin, 2013). It also mirrors and reaffirms existing study on the lack of choice if users do not agree with a privacy notice. For Douyin, TikTok, Toutiao, TopBuzz, and Baidu, users can still use limited app functions if they do not sign up for an account. However, these apps will still collect information during the use of the apps, such as device information and locational information, as per privacy policies. WeChat and Weixin, on the other hand, mandate the creation of accounts to use app services.

REAL NAME REGISTRATION

For all examined apps, users can choose to register with either cell phone numbers or emails in the international version. However, for all domestic versions, cell phone numbers are mandatory to sign up for services. This is a key difference between the international and domestic versions. The main reason is that Article 24 of China's *Cybersecurity Law* requires internet companies to comply with the real name registration regulation. During account registration, all apps request for access to behavioral data (request for location) and user data (contact). The real name registration process mandated under the Chinese law differs in intent and in practice from those of US-based internet companies and platforms. For example, Facebook, YouTube, now-defunct Google+, Twitter and Snapchat have different policies about whether a user has the option of remaining anonymous, or creating an online persona that masks their identity to the public (DeNardis & Hackl, 2015, p. 764). The decisions made on part of internet companies and digital platforms could jeopardise the online safety and anonymity of minority populations and have potential to stifle freedom of expression. However, in the

Chinese context, the real name registration is overseen and enforced by different levels of government for the purpose of governance and control, following the principle of "real identity on the backend and voluntary compliance on the front end", which means apps, platforms, and websites must collect personally identifying information while it is up to users to decide whether to adopt real name as screen name.

ACCOUNT DELETION

For all apps examined, users need to go through multiple steps to reach the account deletion options: WeChat 5 steps, Douyin 6 steps, TikTok 4 steps, TopBuzz 3 steps. The more steps it takes, the more complicated it is for users to de-register and delete data and metadata generated on the app. All Chinese versions of the tested apps prompt an "account in secure state" notification in the process of account deletion. To have an account in secure state, it means that the account does not have any suspicious changes such as changing password or unlinking the mobile phone within a short period of time before the request, as a security measure. To have an account in a secure state is a prerequisite for account removal. The domestic versions also have screening measures so that only accounts that have a "clean history" can be deleted. A clean history means the account has not been blocked nor engaged in any previous activities that are against laws and regulations. TikTok also offers a 30-day deactivation period option before the account is deleted and TopBuzz requires users to tick "agree" on privacy terms during account deletion. It also offers a re-participation option by soliciting reasons why users delete accounts.

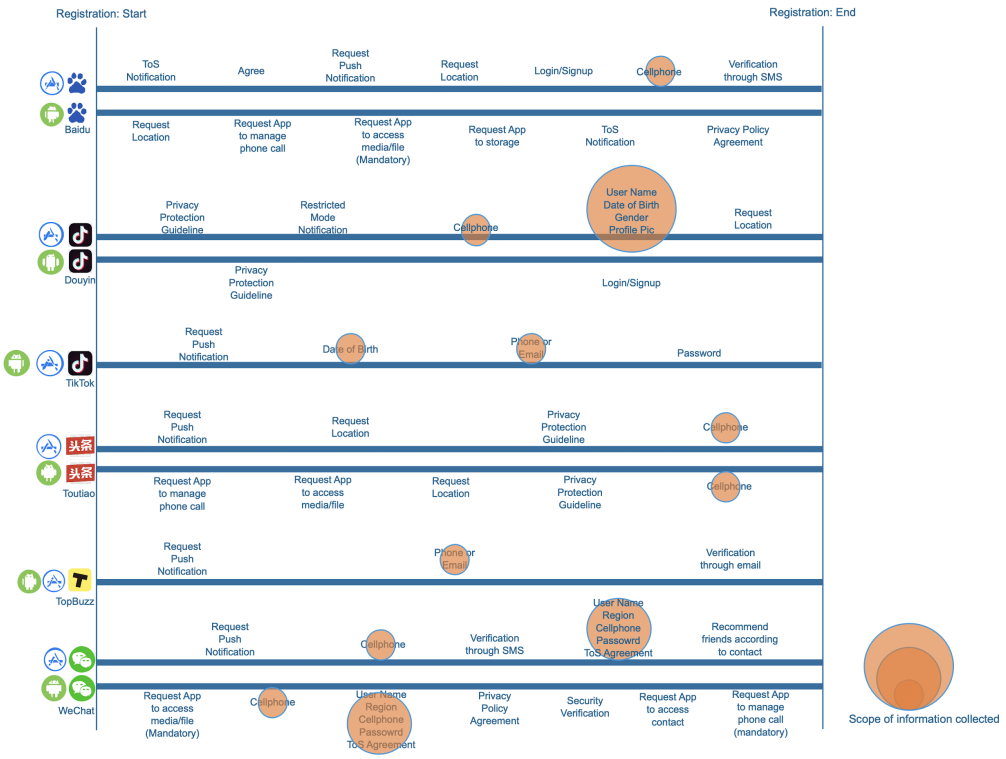

Figure 1: Walkthrough analysis

CONTENT ANALYSIS OF PRIVACY POLICIES AND TERMS OF SERVICE

Table 1: Cross-border regulation

Company	Regions	Privacy policy application scope	Laws and jurisdictions referred	Specific court that legal proceedings must go through
Baidu		Part of larger organization	Relevant Chinese Laws, Regulations	Beijing Haidian District People's court
TopBuzz	EU	Part of larger organization	GDPR and EU	No
	Non-EU	Part of larger organization	US, California Civil Code, Japan, Brazil	Singapore International Arbitration Center
Toutiao		For Toutiao	Relevant Chinese Laws, Regulations	Beijing Haidian District
Douyin		For Douyin	Relevant Chinese Laws, Regulations	Beijing Haidian District People's court
TikTok	US	For TikTok	Yes	Unspecified
	EU	For TikTok	Yes	Unspecified
	Global	For TikTok	No	Unspecified
WeiXin		For Weixin	Relevant Chinese Laws, Regulations	Shenzhen Nanshan People's Court
WeChat	US	For WeChat	No	American Arbitration Association
	EU			The court of the user's place or residence or domicile
	Other			Hong Kong International Arbitration Centre

We retrieved and examined the privacy policies and terms of service of all apps as of July 2019. Baidu only has one set of policies covering both domestic and international users. WeChat/WeiXin, TopBuzz/Toutiao and TikTok/Douyin have designated policies for domestic and international users, respectively. TikTok's privacy policies and terms of service are most regional-specific, with three distinctive documents for US, EU, and global users (excluding US and EU). TopBuzz distinguishes EU and non-EU users with jurisdiction-specific items for users based in the US, Brazil, and Japan in the non-EU users privacy policies. Most policies and terms of service refer to privacy laws of the jurisdictions served, but WeChat and TikTok's global users' privacy policies are vague as they do not explicitly name the laws and regulations but refer to them under "relevant laws and regulations". Compared to the Canadian versions of the same app, Chinese apps provide clearer and more detailed information about the specific court where

disputes are to be solved.

Table 2: Storage and transfer of user data

Company	Regions	Storage of data	Location of storage	Duration of storage	Data transfer
Baidu		Yes	PRC	Unspecified	Unspecified
TopBuzz	EU	Yes Browser behavior data stored for 90 days	third party servers in US & Singapore Amazon Web Services	Varies according to jurisdictions	Yes
	Non-EU	Yes	US and Singapore	Unspecified	Yes
Toutiao		Yes	PRC	Unspecified	No
Douyin		Yes	PRC	Unspecified	Transfer with explicit consent
TikTok	US	Unspecified	Unspecified	Unspecified	Unspecified
	EU	Yes	Unspecified	Unspecified	Yes
	Global	Unspecified	Unspecified	Unspecified	Unspecified
WeiXin		Yes	PRC	Unspecified	Unspecified
WeChat		Yes	Canada, Hong Kong		Unspecified

In terms of data storage, as shown in Table 2, most international versions of examined apps store user data in foreign jurisdictions. For example, WeChat's international-facing privacy policy states that the personal information it collects from users will be transferred to, stored at, or processed in Ontario, Canada and Hong Kong. The company explains explicitly why it chooses the two regions: "Ontario, Canada (which was found to have an adequate level of protection for Personal Information under Commission Decision 2002/2/EC of 20 December 2001); and Hong Kong (we rely on the European Commission's model contracts for the transfer of personal data to third countries (i.e., the standard contractual clauses), pursuant to Decision 2001/497/EC (in the case of transfers to a controller) and Decision 2010/915/EC (in the case of transfers to a processor)." Only Baidu stores user data in mainland China, regardless of the residing jurisdictions of users. However, the latter app's policies do not specify where and for how long the transnational communications between users based in China and users based outside will be stored. Baidu's privacy policies are particularly ambiguous about how long data will be stored. Governed by the GDPR, privacy policies serving EU users are more comprehensive than others in disclosing whether user data will be transferred.

All apps have included mechanisms through which users can communicate their concerns or file complaints about how the company may be retaining, processing, or disclosing their personal information. Almost all apps – with the exception of Baidu – provide an email address and a physical mailing address of where users can initiate communications. TikTok has provided the name of an EU representative in its EU-specific privacy policy, though the contact email provided is the same as the one mentioned in TikTok's other international privacy policies.

Table 3: Privacy disclosure

Company	Regions	Last policy update date	Access to older versions	Notification of update?	Complaint mechanism	Complaint venue
Baidu		No	No	No	Yes	Legal process through local court
TopBuzz	EU	No	Yes	Yes	No privacy officer listed	
	Non-EU	No	No	Yes	Yes	No privacy officer listed
Toutiao		Yes	No	Yes	Yes	No privacy officer listed
Douyin		Yes	No	Yes	Yes	Email and physical mailing address
TikTok	US	Yes	No	Yes	Yes	No privacy officer listed
	EU	Yes	No	Yes	Yes	A EU representative is listed
	Global	Yes	No	Yes	Yes	Email and a mailing address
WeXin		Yes	No	Yes	Yes	Contact email and location of Tencent Legal Department
WeChat		Yes	No	Yes	Yes	Contact email of Data Protection Officer and a physical address

Baidu only mentions that any disputes should be resolved via legal process through local court, which increases the difficulties if users, especially international users, wish to resolve a dispute with the company. WeChat/Weixin is another interesting case: unlike ByteDance which distinguishes its domestic and international users by providing them with two different versions of apps, Tencent's overseas and domestic users use the same app. Users receive different privacy policies and terms of service based on the phone number they signed up with. In addition, the company's privacy policy and terms of service differentiate international users and domestic users not only via their place of residence but also their nationalities. Tencent's terms of service for international WeChat users denote that if the user is "(a) a user of Weixin or WeChat in the People's Republic of China; (b) a citizen of the People's Republic of China using Weixin or WeChat anywhere in the world; or (c) a Chinese-incorporated company using Weixin or WeChat anywhere in the world," he or she is subject to the China-based Weixin terms of service.

However, neither WeChat/Weixin explain how the apps identify someone as a Chinese citizen in these documents. That said, even if Weixin users are residing overseas, they will need to go through the complaint venue outlined in the Chinese privacy policy version rather than taking it to the company's overseas operations.

Our analysis of these apps' data collection practices show some general patterns in both the domestic and international versions. All apps mention the types of information they may collect such as name, date of birth, biometrics, address, contact, location. However, none of the apps, except WeChat for international users offer a clear definition or examples of what counts as personally identifiable information (PII). As for disclosure of PII, all apps state that they will share necessary information with law enforcement agencies and government bodies. TikTok's privacy policy for international users outside the US and EU seems to be the most relaxed when it comes to sharing user information with third parties or company affiliates. All the other apps surveyed state that they will request users' consent before sharing PII with any non-government entities. TikTok's global privacy policy states that it will share user data – without asking for user consent separately — with "any member, subsidiary, parent, or affiliate of our corporate group", "law enforcement agencies, public authorities or other organizations if legally required to do so", as well as with third parties.

CONCLUSION

This study shows that not only different Chinese mobile apps vary in data and privacy protection but also the Chinese domestic and international versions of the same app vary in data and privacy protection standards. More globally successful China-based mobile apps have better and more comprehensive data and privacy protection standards. Similar to previous findings (Liu, 2019; Fazhi Wanbao, 2018), our research shows that Baidu, compared to other apps, has the most unsatisfactory data and privacy protection measures. ByteDance's apps: TopBuzz/Toutiao, TikTok/Douyin are more attentive to users from different geographical regions by designating jurisdiction-specific privacy policies and terms of service. In this case, the mobile app's globalisation strategies and aspirations play an important part in the design and governance of mobile app data and privacy protection. ByteDance is the most internationalised company, when compared to Baidu and Tencent. ByteDance's experience of dealing with fines from the United States, Indian and Indonesian law enforcement and regulatory authorities has helped revamp its practices overseas. For instance, TikTok updated its privacy policy after the Federal Trade Commission's fine in February 2019 (Alexander, 2019). Faced with probing from US lawmakers and a ban from US Navy, TikTok released its first Transparency report in December 2019 and the company is set to open a "Transparency Center" in its Los Angeles office in May 2020, where external experts will oversee its operations (Pappas, 2020). For Tencent, with an expanding array of overseas users, the company was also among the first to comply with the GDPR. Tencent updated its privacy policy to meet GDPR's requirement on 29 May 2018 — a day after it came into force.

For China-based internet companies that eye global markets, expanding beyond China means that they must provide a compelling experience for international users and comply with laws and regulations in jurisdictions where they operate. In this regard, nation-states and their designed ecosystem of internet regulations have a powerful impact on how private companies govern their platforms. Our analysis suggests that nation-based regulations on online spaces have at times spilled beyond their territory (e.g., Tecent's WeChat/Wexin's distinguishing domestic and international users based on their nationality). However, the effects of state

regulations on transnational corporations are not monolithic. They vary depending on how integrated a platform is into a certain jurisdiction, where its main user base is, and what its globalisation strategies are. For example, ByteDance's TikTok is more responsive to international criticism and public scrutiny than the other applications in this study potentially because of the app's highly globalised presence and revenue streams.

Secondly, this paper highlights that in addition to app makers, other powerful actors and parties shape the app's data and privacy protection practices. One of the actors is mobile app store owners (e.g., Google Play and Apple App Store). As the walkthrough analysis demonstrates, the app interface design and requests on Apple iOS do a better job at informing and notifying data access for mobile phone users. The Android version of tested apps have set user consent for push notification as default in some cases, therefore it requests individual efforts to navigate and learn how to opt out or withdraw consent. Examined mobile apps operating in the Android system are more lenient in requesting data from users, as compared to iOS. The gatekeeping function of mobile app platforms that host these apps and set the standards for app designers and privacy protection further indicates a more nuanced and layered conceptualisation of corporate power in understanding apps as a situated digital object. This further shows that in a closely interconnected platform ecosystem, some platform companies are more powerful than others with their infrastructural reach in hosting content, providing cloud computing and data services (van Dijck, Nieborg, & Poell, 2019). Even though Tencent, ByteDance and Baidu are powerful digital companies in China, they still rely on Google Play store and Apple's App Store for the domestic and global distribution of their apps, therefore subjecting to the governance of these mobile app stores (see Cartwright, 2020, this issue). Another example is the mini-programmes, which are "sub-applications" hosted on WeChat, where developers and apps are subject to WeChat's privacy policies and developer agreements. This shows that apps are always *situated* in and should be studied together with the complex mobile ecosystem and their regional context (Dieter et al., 2019). Therefore, we should consider the relational and layered interplay between different levels of corporate power in co-shaping the data and privacy practices of mobile apps.

As shown in the analysis, the international-facing version of the same China-based mobile app provides relatively higher levels of data protection to app users in the European Union than its Chinese-facing version. This further highlights the central role of nation states and the importance of jurisdiction in the global expansion of Chinese mobile apps. As non-EU organisations, Chinese app makers are subject to the territorial scope of GDPR (Article 3) when offering services to individuals in the EU. On the other hand, Chinese-facing apps have operationalised Chinese privacy regulations in app design and privacy policies compliant with rules such as real name registration. Through the analysis of terms of service and privacy policies, this paper shows that China-based mobile apps are generally in compliance with laws and data protection frameworks across different jurisdictions. However, there lacks detailed explanations of data retention and storage when users are in transit, for example, when an EU resident travels outside, do they have the same level of privacy protection as residing in the EU? On average, EU users of Chinese mobile apps are afforded greater transparency and control with regards to how data is used, stored and disclosed compared to other jurisdictions for these four particular sets of China-based mobile apps. Under China's privacy regulation regime, which itself is full of contradictions and inconsistencies (Lee, 2018; Feng, 2019), data and privacy protection is weak for domestic Chinese users. Certain features of the app, such as the "security clearance" declaration during account deletion for domestic versions of Chinese mobile apps also shows the prioritisation of national security over the individual right to privacy as key doctrines in China's approach to data and privacy protection under the banner of internet

sovereignty. This, however, is not unique to China as national security and privacy protection is portrayed in many policy debates and policymaking processes as a zero-sum game (Mann, Daly, Wilson, & Suzor, 2018). The latest restrictions imposed by the Trump administration on TikTok and WeChat in the US citing concerns over the apps' data collection and data sharing policies (Yang and Lin, 2020) is just another example of the conundrum China-based apps face in their course of global expansion and global geopolitics centered around mobile and internet technologies. To be sure, data and privacy protection is one of the biggest challenges if China-based apps continue to expand overseas and it is going to incur a steep learning curve and possible reorganisation of a company's operation and governance structure.

REFERENCES

Alexander, J. (2019, February 27). TikTok will pay $5.7 million over alleged children's privacy law violations. *The Verge*. https://www.theverge.com/2019/2/27/18243312/tiktok-ftc-fine-musically-children-coppa-age-gate

Balebako, R., Marsh, A., Lin, J., Hong, J., & Cranor, L. F. (2014, February 23). *The Privacy and Security Behaviors of Smartphone App Developers*. Network and Distributed System Security Symposium. https://doi.org/10.14722/usec.2014.23006

BBC News. (2016, July 18). Apple iCloud: State Firm Hosts User Data in China. *BBC News*. https://www.bbc.com/news/technology-44870508

Byford, S. (2018, November 30). How China's Bytedance Became the World's Most Valuable Startup. *The Verge*. https://www.theverge.com/2018/11/30/18107732/bytedance-valuation-tiktok-china-startup

C.A.C. (2016, December 27). Guojia Wangluo Anquan Zhanlue. *Xinhuanet*. http://www.xinhuanet.com/politics/2016-12/27/c_1120196479.htm

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Chen, J. Y., & Qiu, J. L. (2019). Digital Utility: Datafication, Regulation, Labor, and Didi's Platformization of Urban Transport in China. *Chinese Journal of Communication*, *12*(3), 274–289. https://doi.org/10.1080/17544750.2019.1614964

Chen, X., Kaye, D. B., & Zeng, J. (2020). #PositiveEnergy Douyin: Constructing 'Playful Patriotism' in a Chinese Short-Video Application. *Chinese Journal of Communication*. https://doi.org/10.1080/17544750.2020.1761848

de Hert, P., & Papakonstantinou, V. (2015). *The Data Protection Regime in China*. [Report]. European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf

Deibert, R., & Pauly, L. (2017). Cyber Westphalia and Beyond: Extraterritoriality and Mutual Entanglement in Cyberspace. *Paper Prepared for the Annual Meeting of the International Studies Association*.

DeNardis, L., & Hackl, A. M. (2015). Internet Governance by Social Media Platforms. *Telecommunications Policy*, *39*(9), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., Vlist, F., & Weltevrede, E. (2019). Multi-Situated App Studies: Methods and Propositions. *Social Media + Society*, 1–15.

Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing Platform Power. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1414

Federal Trade Commission. (1998). *Privacy Online: A Report to Congress* [Report]. Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

Federal Trade Commission. (2013). *Mobile Privacy Disclosures: Building Trust Through Transparency* [Staff Report]. Federal Trade Commission. https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission

Federal Trade Commission. (2019, February 27). *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* [Press release]. Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc

Feng, Y. (2019). The Future of China's Personal Data Protection Law: Challenges and Prospects. *Asia Pacific Law Review*, *27*(1), 62–82. https://doi.org/10.1080/10192557.2019.1646015

Fernback, J., & Papacharissi, Z. (2007). Online Privacy as Legal Safeguard: The Relations Among Consumer, Online Portal and Privacy Policy. *New Media & Society*, *9*(5), 715–734. https://doi.org/10.1177/1461444807080336

Flew, T., Martin, F., & Suzor, N. (2019). Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance. *Journal of Digital Media & Policy*, *10*(1), 33–50. https://doi.org/10.1386/jdmp.10.1.33_1

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

Fuchs, C. (2012). The Political Economy of Privacy on Facebook. *Television & New Media*, *13*(2), 139–159. https://doi.org/10.1177/1527476411415699

Gierow, H. J. (2014). *Cyber Security in China: New Political Leadership Focuses on Boosting National Security* (Report No. 20; China Monitor). merics. https://merics.org/en/report/cyber-security-china-new-political-leadership-focuses-boosting-national-security

Gillespie, T. (2018a). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. Yale University Press.

Gillespie, T. (2018b). Regulation Of and By Platforms. In J. Burgess, A. Marwick, & T. Poell (Ed s.), *The SAGE Handbook of Social Media* (pp. 254–278). SAGE Publications. https://doi.org/10.4135/9781473984066.n15

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of Borderless World*. Oxford University Press.

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Greene, D., & Shilton, K. (2018). Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development. *New Media & Society*, *20*(4), 1640–1657. https://doi.org/10.1177/1461444817702397

Jao, N. (2018, February 8). Evernote Announces Plans to Migrate All Data in China to Tencent Cloud. *Technode*. https://technode.com/2018/02/08/evernote-will-migrate-data-china-

tencent-cloud/

Jia, L., & Winseck, D. (2018). The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization. *International Communication Gazette*, *80*(1), 30–59. https://doi.org/10.1177/1748048517742783

Kalathil, S., & Boas, T. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment for International Peace.

Kaye, B. V., Chen, X., & Zeng, J. (2020). The Co-evolution of Two Chinese Mobile Short Video Apps: Parallel Platformization of Douyin and TikTok. *Mobile Media & Communication*. https://doi.org/10.1177/2050157920952120

Knockel, J., Ruan, L., Crete-Nishihata, M., & Deibert, R. (2018). *(Can't) Picture This: An Analysis of Image Filtering on WeChat Moments* [Report]. Citizen Lab. https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-filtering-on-wechat-moments/

Kong, L. (2007). Online Privacy in China: A Survey on Information Practices of Chinese Websites. *Chinese Journal of International Law*, *6*(1), 157–183. https://doi.org/10.1093/chinesejil/jml061

Lee, J.-A. (2018). Hacking into China's Cybersecurity Law. *Wake Forest Law Review*, *53*, 57–104. http://wakeforestlawreview.com/wp-content/uploads/2019/01/w05_Lee-crop.pdf

Light, B., Burgess, J., & Duguay, S. (2018). The Walkthrough Method: An Approach to the Study of Apps. *New Media & Society*, *20*(3), 881–900. https://doi.org/10.1177/1461444816675438

Liu, J. (2019). China's Data Localization. *Chinese Journal of Communication*, *13*(1). https://doi.org/10.1080/17544750.2019.1649289

Logan, S. (2015). *The Geopolitics of Tech: Baidu's Vietnam*. Internet Policy Observatory. http://globalnetpolicy.org/research/the-geopolitics-of-tech-baidus-vietnam/

Logan, S., Molloy, B., & Smith, G. (2018). *Chinese Tech Abroad: Baidu in Thailand* [Report]. Internet Policy Observatory. http://globalnetpolicy.org/research/chinese-tech-abroad-baidu-in-thailand/

Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia. *International Communication Gazette*, *80*(4), 369–384. https://doi.org/10.1177/1748048518757141

Martin, K. (2013). Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online. *First Monday*, *18*(12). https://doi.org/10.5210/fm.v18i12.4838

McKune, S., & Ahmed, S. (2018). The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda. *International Journal of Communication*, *12*, 3835–3855. https://ijoc.org/index.php/ijoc/article/view/8540

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Pappas, V. (2020, March 11). *TikTok to Launch Transparency Center for Moderation and Data Practices* [Press release]. TikTok. https://newsroom.tiktok.com/en-us/tiktok-to-launch-transparency-center-for-moderation-and-data-practices

Plantin, J.-C., Lagoze, C., Edwards, P., & Sandvig, C. (2016). Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Plantin, J.-C., & Seta, G. (2019). WeChat as Infrastructure: The Techno-nationalist Shaping of Chinese Digital Platforms. *Chinese Journal of Communication*, *12*(3). https://doi.org/10.1080/17544750.2019.1572633

Reuters. (2016, November 1). Airbnb Tells China Users Personal Data to be Stored Locally. *Reuters*. https://www.reuters.com/article/us-airbnb-china/airbnb-tells-china-users-personal-data-to-be-stored-locally-idUSKBN12W3V6

Reuters. (2018, January 12). China Chides Tech Firms Over Privacy Safeguards. *Reuters*. https://www.reuters.com/article/us-china-data-privacy/china-chides-tech-firms-over-privacy-safeguards-idUSKBN1F10F6

Ruan, L., Knockel, J., Ng, J., & Crete-Nishihata, M. (2016). *One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally* (Research Report No. 84). Citizen Lab. https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

Sharma, I., & Niharika, S. (2019, July 22). It Took a Ban and a Government Notice for ByteDance to Wake Up in India. *Quartz India*. https://qz.com/india/1671207/bytedance-to-soon-store-data-of-indian-tiktok-helo-users-locally/

State Council Information Office. (2010). *The Internet in China*. Information Office of the State Council of the People's Republic of China. http://www.china.org.cn/government/whitepaper/node_7093508.htm

Stein, L. (2013). Policy and Participation on Social Media: The Cases of YouTube, Facebook and Wikipedia. *Communication, Culture & Critique*, *6*(3), 353–371. https://doi.org/10.1111/cccr.12026

Steinberg, M., & Li, J. (2016). Introduction: Regional Platforms. *Asiascape: Digital Asia*, *4*(3), 173–183. https://doi.org/10.1163/22142312-12340076

Wanbao, F. (2018, January 6). Shouji Baidu App Qinfanle Women de Naxie Yinsi. *163*. http://news.163.com/18/0106/17/D7G2O0T200018AOP.html

Wang, H. (2011). *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*. Springer Science & Business Media. https://doi.org/10.1007/978-3-642-21750-0

Wang, W. Y., & Lobato, R. (2019). Chinese Video Streaming Services in the Context of Global Platform Studies. *Chinese Journal of Communication*, *12*(3), 356–371. https://doi.org/10.1080/17544750.2019.1584119

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Xu, D., Tang, S., & Guttman, D. (2019). China's Campaign-style Internet Finance Governance: Causes, Effects, and Lessons Learned for New Information-based Approaches to Governance. *Computer Law & Security Review*, *35*, 3–14. https://doi.org/10.1016/j.clsr.2018.11.002

Xu, J. (2015). Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China. In J. Lindsay, T. M. Cheung, & D. Reveron (Eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*(pp. 242–259). Oxford Scholarship Online. https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

Yang, J., & Lin, L. (2020). WeChat and Trump's Executive Order: Questions and Answers. *The Wall Street Journal*. https://www.wsj.com/articles/wechat-and-trumps-executive-order-questions-and-answers-11596810744.

Yang, W. (2018, September 15). Online Streaming Platforms Urged to Follow Copyright Law. *ChinaDaily*. http://usa.chinadaily.com.cn/a/201809/15/WS5b9c7e90a31033b4f4656392.html

Yang, Y. (2019, June 21). TikTok Owner ByteDance Gathers 1 Billion Monthly Active Users Across its Apps. *South China Morning Post*. https://www.scmp.com/tech/start-ups/article/3015478/tiktok-owner-bytedance-gathers-one-billion-monthly-active-users

Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Liu, B., Schaub, F., & Reidenberg, J. (2016, September 28). Automated Analysis of Privacy Requirements for Mobile Apps. *2016 AAAI Fall Symposium Series*. http://pages.cpsc.ucalgary.ca/~joel.reardon/mobile/privacy.pdf

APPENDIX

Current laws, regulations and drafting measures for data and privacy protection in China

Year	Title	Government ministries	Legal effect	Main takeaway
2009	General Principles of The Civil Law	National People's Congress	Civil law	Lays the foundation for the protection of personal rights including personal information, but privacy protection comes as an auxiliary article
2010	Tort Liabilities Law	Standing Committee of the National People's Congress	Civil law	
2012	Decision on Strengthening Online Personal Data Protection	Standing Committee of the National People's Congress	General framework	Specifies the protection of personal electronic information or online personal information for the first time
2013	Regulation on Credit Reporting Industry	State Council	Regulation	Draws a boundary of what kinds of personal information can and cannot be collected by credit reporting business
2013	Telecommunication and Internet User Personal Data Protection Regulations	Ministry of Industry and Information Technology	Department regulation	Provides industry-specific regulations on personal information protection duties

Year	Title	Government ministries	Legal effect	Main takeaway
2013	Information Security Technology Guidelines for Personal Information Protection with Public and Commercial Services Information Systems	National Information Security Standardization Technical Committee; China Software Testing Center	Voluntary national standard	Specifies what "personal general information" □□□□□□ and what " personal sensitive information" □□□□□□ entail respectively; Defines the concepts of "tacit consent" □□□□ and "expressed consent" □□□□ for the first time
2014	Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks	Supreme People's Court	General framework	Defines what is included in the protection of "personal information", with a specific focus on regulating online search of personal information and online trolls
2015	Criminal Law (9th Amendment)	Standing Committee of the National People's Congress	Criminal law	Criminalises the sale of any citizen's personal information in violation of relevant provisions. Criminalises network service providers' failure to fulfil network security management duties.
2016	Administrative Rules on Information Services via Mobile Internet Applications	Cyberspace Administration China	Administrative rules	Reiterates app stores and internet app providers' responsibilities to comply with real-name verification system and content regulations regarding national security and public order; Mentions data collection principles (i.e., legal, justifiable, necessary, expressed consent)
2017	Cybersecurity Law	Standing Committee of the National People's Congress	Law	Requires data localisation; Provides definitions of ""personal information"" Defines data collection principles; Currently the most authoritative law protecting personal information

Year	Title	Government ministries	Legal effect	Main takeaway
2017	Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information	Supreme People's Court	General framework	Defines "citizen personal information", what activities equate to "providing citizen personal information", and what are the legal consequences of illegally providing personal information
2017	Information security technology Guide for De-Identifying Personal Information	Standardization Administration of China	Drafting	Provides a guideline on de-identification of personal information
2018	Information security technology Personal information security specification	Standardization Administration of China	Voluntary national standard / Currently under revision	Lays out granular guidelines for consent and how personal data should be collected, used, and shared.
2018	E-Commerce Law	Standing Committee of the National People's Congress	Law	Provides generally-worded personal information protection rules for e-commerce vendors and platforms
2019	Measures for Data Security Management	Cyberspace Administration China	Drafting	Proposes new requirements with a focus on the protection of "important data", which is defined as "data that, if leaked, may directly affect China's national security, economic security, social stability, or public health and security"
2019	Information security technology Basic specification for collecting personal information in mobile internet applications	Standardization Administration of China	Drafting	Provides guidelines on minimal information for an extensive list of applications ranging from navigation services to input software
2019	Measures for Determining Illegal Information Collection by Apps	Drafting stage		