Journal of Private International Law, 2019
Vol. 15, No. 1, 186–209, https://doi.org/10.1080/17441048.2019.1599771

Chinese private international law and online data protection

Jeanne Huang*

This paper explores how Chinese private international law responds to online data protection from two aspects: jurisdiction and applicable law. Compared with foreign laws, Chinese private international law related to online data protection has two distinct features. Chinese law for personal jurisdiction is still highly territorial-based. The "target" factor and the interactive level of a website have no play in Chinese jurisprudence. Regarding applicable law, Chinese legislators focus more on the domestic compliance with data regulations rather than their extra-territorial application. Moreover, like foreign countries, China also resorts to Internet intermediaries to enhance enforcement of domestic law. These features should be understood in the Chinese contexts of high-level data localization and Internet censorship.

Keywords: personal jurisdiction; China; applicable law; private international law; data protection; online

How would online[1] data technology challenge the development of private international law? Recent years have witnessed growing literature on the nature of data and its implications on private international law.[2] The typical example is

*Jie (Jeanne) Huang, Associate Professor University of Sydney Law School. Thanks to anonymous reviewers and attendees at the XXth International Academy of Comparative Law Congress and the UNSW Private International Law and Intellectual Property Workshop for helpful comments on a draft. All errors remain to be my own. Email: Jeanne.huang@sydney.edu.au.

[1]For the purpose of this paper, "online", "Internet" and "information networks" are exchangeable and include the Internet, radio and television broadcasting networks, fixed communication networks and mobile communication networks, with computers, TV sets, fixed telephones, mobile phones and other electronic devices as receiving terminals, as well as local area networks open to the public.

[2]E.g, Dan Jerker B. Svantesson, "Jurisdictional issues and the internet – a brief overview 2.0", (2018) 34 *Computer Law and Security Review* 715, 715–722. T Lutzi, "Internet Cases in EU Private International Law—Developing a Coherent Approach", (2017) 66 *ICLQ* 687, 687–721; A Rahman, "Personal Jurisdiction on the Internet: A Global Perspective", (2015) 14 *Journal of Internet Commerce* 114, 114–21. R Matulionyte, "Calling for Party Autonomy in Intellectual Property Infringement Cases", (2013) 9 *Journal of Private International Law* 77, 77–97. B Ubertazzi, "Intellectual Property Rights and Exclusive (Subject Matter) Jurisdiction: Between Private and Public International Law", (2011) 15 *MARQUETTE IP LAW REV.* 357, 357–448; C O'Reilly, "Finding Jurisdiction to Regulate

the debate between exceptionalism and unexceptionalism.[3] In 2018, the Clarifying Lawful Overseas Use of Data Act (hereinafter "CLOUD Act")[4] was enacted in the U.S. and the General Data Protection Regulation (hereinafter "GDPR")[5] became effective in the EU. Both have pushed this debate to a new apex.[6] This Paper adds to this debate from a new aspect: it exams how Chinese private international law has responded to online data protection from two aspects: jurisdiction and applicable law. It argues that the development of private international law should not simply depend on what data technologically or even legally is. We need to consider the overall data policy and the tradition of private international law in a country. This Paper finds that neither exceptionalism nor unexceptionalism can fully explain the current development of Chinese private international law. The law develops by interacting with China's overall data protection policy and the tradition of private international law in China.

Google and the Internet", (2011) 2 *European Journal of Law and Technology* 1, 1–2, 8; XQ Feng and QJ Liu, "Legal Problems of Internet Domain Name in China", (2008) 3 *International Journal of Private Law* 382, 382–98; JM Jensen, "Personal Jurisdiction in Federal Courts over International E-Commerce Cases", (2006) 40 *Loyola of Los Angeles Law Review* 1507, 1511–41. N Bettelheim, "Personal Jurisdiction and The Internet: Cyber Differences Shed New Light on Existing Conflicts", (2006) *Journal of Internet Law* 22, 24; Z Tang, "Exclusive Choice of Forum Clauses and Consumer Contracts in E-Commerce", (2005) 1 *Journal of Private International Law* 237, 237–68; O Bigos, "Jurisdiction Over Cross-Border Wrongs on The Internet", (2005) 54 *ICLQ* 585, 591–92; PS Berman, "Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era", (2005) 153 *University of Pennsylvania Law Review* 1819, 1819–1882.

[3]Data unexceptionalism argues that data is not significantly different from traditional subjects, so the jurisdictional challenges presented by data are not conceptually as novel as they seem. E.g. AK Wood, "Against Data Exceptionalism", (2016) 68 *Stan. L. Rev.* 729, 789. Data exceptionalism argues that data is fundamentally different from traditional subjects, so the traditional conflict of laws for jurisdiction should be reformed. E.g. J Daskal, "The Un-Territoriality of Data", (2015) 125 *Yale Law Journal* 326, 326–399; J L Goldsmith, "Against Cyberanarchy", (1998) 65 *The University of Chicago Law Review* 1199, 1199–1250; DR Johnson and D Post, "Law and Borders: The Rise of Law in Cyberspace", (1996) 48 *Stanford Law Review* 1367, 1367–1402. Scholars consider the dichotomy between exceptionalism and unexceptionalism visions was a false one, e.g. PS Berman, "Legal Jurisdiction and the Deterritorialization of Data", (2018) 71 *Vanderbilt Law Review* 11, 15.

[4]Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R.4943) is a U.S. law enacted on 24 March 2018.

[5]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

[6]E.g. ZD Clopton, "Territoriality, Technology, and National Security", (2016) 83 *The University of Chicago Law Review* 45, 51–54; and J Daskal, "Borders and Bits", (2018) 71 *Vanderbilt Law Review* 179, 218.

This Paper has three Sections. The A Section focuses on personal jurisdiction. It argues that Chinese law for personal jurisdiction related to online data protection has two distinct features. First, Chinese law is still highly territorial-based by allowing courts to exercise jurisdiction on a non-resident defendant solely based on the location of a server. Second, when exercising jurisdiction, Chinese courts do not consider the "target" factor and the interactive level of a defendant's website. The B Section discusses the applicable law to online data protection. Similar to its territorial-oriented personal jurisdiction rule, Chinese applicable law for online data protection uses the geographic location of data activities in China as a connecting factor. Moreover, like foreign countries, China also resorts to Internet intermediaries to enhance enforcement of domestic law. The development of both jurisdiction and applicable law fits into the Chinese contexts of high-level data localization and Internet censorship. They are also consistent with the Chinese tradition of private international law. The C Section concludes the Paper and draws two broad international implications from China's example.

A. Personal jurisdiction

Chinese law for personal jurisdiction related to online data protection has two distinct features. First, Chinese law is still highly territorial-based. For example, it allows courts to exercise jurisdiction on a non-resident defendant solely based on the location of a server.[7] In contrast, private international law in many foreign countries have moved away from the territorially-based jurisdiction rule.[8] Second, when exercising jurisdiction, courts in many foreign countries would consider whether a non-resident defendant's website has target the forum or how interactive the defendant's website is.[9] However, the "target" factor and the interactive level have no play in Chinese jurisprudence.[10]

1. *Personal jurisdiction based on the location of a server*

Personal jurisdiction based on the location of a server is a territorially-based jurisdiction rule and is "developed in an era when physical geography was more consequential than it is today".[11] It has been rejected by many foreign courts but widely accepted in China.

[7]See *infra* Section 1.1.2.
[8]DC Andrews and JM Newman, "Personal Jurisdiction and Choice of Law in the Cloud", (2013) 73 *Maryland Law Review* 313, 388.
[9]PL Bellia, "Chasing Bits across Borders Frontiers of Jurisdiction", (2001) *University of Chicago Legal Forum* 35, 73.
[10]See *infra* Section 1.1.2.
[11]G I Zekos, "Cyber versus Conventional Personal Jurisdiction", (2015) *Journal of Internet Law* 3, 5.

(a) *Foreign jurisprudence explicitly rejects personal jurisdiction solely based on the location of a server*

U.S. courts recognize two broad categories of personal jurisdiction on a non-resident defendant, namely, specific and general jurisdiction.[12] The traditional test establishing specific personal jurisdiction on a non-resident defendant has three prongs.[13] First, the defendant must come within the terms of the applicable state long-arm statute.[14] Second, the defendant must have minimal contacts with the forum state such that the assertion of jurisdiction would not violate the due process clause.[15] This requires the defendant to have purposely availed itself of the privilege of conducting activities in the forum state, and the lawsuit arises out of or is related to the defendant's purposeful contacts with the forum or the defendant's forum contacts is so extensive that no such relationship is necessary.[16] And third, the exercise of jurisdiction must be fair and reasonable.[17] In the Internet era, U.S. courts cannot exercise personal jurisdiction on a non-resident defendant solely based on the location of a server without satisfying the three-prong test. For example, in *Penguin Group (USA) Inc. v. American Buddha*,[18] American Buddha was accused of copyright infringement by Penguin Group (USA) Inc. American Buddha argued that the situs of injury is where copying and uploading of the books took place, i.e. where its servers were located in either Oregon or Arizona. The Southern District of New York agreed. This decision was reversed by the appellate court, which held that in the context of the Internet, it was "illogical" to equate the situs of a plaintiff's injury with the place where the content was uploaded, namely where the server is located.[19] Therefore, New York courts could exercise personal jurisdiction on American Buddha.

Likewise, under Australia law, the location of an infringer's servers and other computing equipment also appears to be irrelevant to personal jurisdiction. In *Dow*

[12]If a defendant is engaged in "continuous and systematic" activity in the forum state, U.S. courts can exercise general jurisdiction regardless of the cause of action. *Helicopteros Nacionales de Colom., S.A. v. Hall*, 466 U.S. 408, 414 (1984). This paper will focus on specific jurisdiction because it is more frequently used in cases involving non-resident defendants.

[13]*International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945), *World-Wide Volkswagen Corp v. Woodson*, 444 U.S. 286, 291–92 (1980), *Asahi Metal Industry Co. v. Superior Court*, 480 U.S. 102, 108–09 (1987).

[14]BT Ward, "Where in the World Is Internet Jurisdiction: A US Perspective", (2010) 4 *International Journal of Value Chain Management* 5, 7–9.

[15]RL Garnett, "Trademarks and the Internet: Resolution of International IP Disputes by Unilateral Application of U.S. Laws", (2004) 30 *Brook. J. Int'l L*. 925, 930.

[16]*Ibid.*

[17]S Burshtein, "Jurisdiction in Internet Trade-Mark and Domain Name Disputes", (2006) 20 *Intellectual Property Journal* 1, 7–9.

[18]P*enguin Group (USA) Inc. v. American Buddha*, 16 N.Y.3d 295 (N. Y. 2011).

[19]*Ibid,* at 305. P*enguin Group (USA) Inc. v. American Buddha*, 640 F. 3d 497.

Jones & Company Inc. v. Gutnick,[20] the High Court of Australia rejected Dow Jones's argument that only the U.S. court can exercise jurisdiction because its servers are located there. The Court held that material published online was available in comprehensible form only when downloaded on to the computer of a person who has used a web browser to pull the material from the server, and where that person downloaded the material is the place from which the harmful conduct was committed.[21]

In the EU, personal jurisdiction related to tort, delict or quasi-delict is regulated by Article 7(2) of Brussels I Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Recast).[22] It provides that the domestic courts where the harmful event occurred or may occur have jurisdiction.[23] The place where the harmful event occurred or may occur includes where the damage occurred and the place of the event giving rise to it.[24] The European Court of Justice ("ECJ") in *Football Dataco Ltd v. Sportradar GmbH* explicitly forbids courts to exercise personal jurisdiction based upon the geographic location of servers and the infringer's computing equipment.[25]

(b) *Chinese territorialism*

However, in recent years China has strengthened rather than weakened the territorially-based jurisdiction rule. A typical example is that Chinese law permits Chinese courts to exercise jurisdiction over a non-resident defendant if the server used for committing the alleged tort is situated in the forum. According to a Chinese law promulgated in 2000, the Intermediate People's Courts located in the place of infringement or the place of the defendant's domicile have jurisdiction over online copyright infringement cases.[26] The place of infringement

[20] *Dow Jones & Company Inc. v. Gutnick*, [2002] HCA 56.
[21] *Ibid,* at para 44.
[22] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012.
[23] For detailed analysis of Article 7(2) of Brussels I Regulation, see S Neumann, "Intellectual Property Rights Infringements in European Private International Law: Meeting the Requirements of Territoriality and Private International Law", (2011) 7 *Journal of Private International Law* 583, 591–95.
[24] Case 21/76 *Bier v Mines de Potasse d'Alsace* [1976] ECR 1735. James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, Oxford University Press 2011), 153–75.
[25] *Football Dataco Ltd v. Sportradar GmbH* (Case C-173/11, 2012).
[26] Art 2 of Supreme People's Court Judicial Interpretation on Several Issues concerning the Application of Law in the Trial of Cases Involving Copyright Disputes on Computer Networks (hereinafter "SPC on Copyright Disputes on Computer Networks"), adopted on 22 November 2000 and amended on 20 November 2006. Art 15 of the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information

includes where the network server, computer terminal or any other equipment used for committing the alleged infringement is located.[27] Chinese Civil Procedure Law newly amended in 2017 (hereinafter "CPL")[28] and Supreme People's Court Judicial Interpretation Regarding Chinese Civil Procedure Law issued in 2015 (hereinafter "2015 Judicial Interpretation of CPL")[29] apply this jurisdiction ground to all internet tort cases. According to Article 28 of Chinese CPL, the Intermediate People's Courts located at the place where the tort occurs or at the place of the defendant's domicile have jurisdiction over an action instituted for the tort. Articles 25 of the 2015 Judicial Interpretation of CPL further provides that in cases where the tort occurs over the Internet, the place where a tort activity is committed includes the place where the computers and other information equipment used to commit the alleged tort are located.

A case in point is *Sunny Co. v. Taobao Co*. Sunny brought an online trademark infringement action against Taobao in Sunny's domicile at the Gulou District, Nanjing City, Jiangsu Province.[30] Taobao was domiciled in Hangzhou City, Zhejiang Province. Taobao argued that the case should be tried in Hangzhou rather than in Nanjing. The Intermediate People's Court in Nanjing held that the Nanjing Railway People's Court could hear this case because Taobao's server was located in that court's jurisdiction. Therefore, unlike *Penguin Group, Dow Jones,* and *Football Dataco* that abandon the geographic location of the defendant's server as a jurisdictional ground, *Sunny Co.* adopts a sheer territorial approach.

Internet transaction has become much more complicated when various third-party service providers are involved. These third parties include telecommunication network providers, access providers supplying services for storage and transmission, e-commerce platform providers, content service providers, etc. For example, many e-commerce traders operate their websites on a platform provided by a third-party server owner, rather than having their own server. Traders on the largest Chinese C-to-C and B-to-C platform, www.taobao.com, rent part of the service of Taobao's server. These traders operate their websites but are not

Networks (hereinafter "SPC Provisions on Infringement of the Right of Dissemination"), adopted on 17 December 2012 and effective on 1 January 2013. Art 2 of Provisions of 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, issued on 21 August 2014 and effective on 10 October 2014.

[27] *Ibid.*

[28] China Civil Procedure Law, recently amended for the third time as adopted at the 28th Session of the Standing Committee of the Twelfth National People's Congress on 27 June 2017 and effective on 1 July 2017.

[29] Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law, adopted on 18 December 2014 and effective on 4 February 2015.

[30] *Sunny Co. v. Taobao Co*., Civil Decision rendered by the Intermediate People's Court in Nanjing Jiangsu Province, (2014) Ning Zi Min Xia Zhong Zi No. 7.

responsible for the operation of the server. Suppose a plaintiff alleges that an e-commerce trader promotes counterfeited products on the Taobao platform by illegally using its trademark, could this plaintiff bring a case against the trader in the place where the Taobao's server is located? E-commerce traders also need network service providers, such as China Mobile, to provide connection, transmission, information storage space, or other network services. Suppose a plaintiff alleges that an e-commerce trader uses China Mobile's server to send out commercial spams, could this plaintiff litigate the case against the trader in the place where the China Mobile's server is located?

A relevant case is *Rockwool International A/S v. Dalian Rockwool Co Ltd*.[31] Rockwool International A/S is a Danish company (hereinafter "Danish Rockwool"). Since 1937, it had been a leading producer of insulation, fireproofing and other products made with stone wool in the world. Although Danish Rockwool entered Chinese market in 1995, it registered the ROCKWOOL trademark in 2013. Dalian Rockwool Co. Ltd (hereinafter "Chinese Rockwool") was a Chinese companyin Dalian City in Liaoning Province. Since 1987, it had used *Rockwool* in its name, its website (www.chinarockwool.com) and its headquarter and factory signage. Danish Rockwool viewed these uses as unauthorised infringement of its trademark. Danish Rockwool did not want to sue Chinese Rockwool in the latter's domicile in fear of local protectionism. It discovered that Chinese Rockwool contracted with a third party server provider to operate its website and the server was located in Jiangmen City, Guangdong Province. It brought a trademark infringement case against Chinese Rockwool in the Intermediate People's Court in Jiangmen City . The Jiangmen court accepted the case based upon the location of the server.

Another example is *Tencent v Qihoo 360 Technology Co. Ltd and Qizhi Software Co. Ltd.*[32] In this case, both defendants resided in Beijing. The defendants argued that the court in Guangdong Province has no jurisdiction because their servers that stored the disputed software was located in Beijing. The Supreme People's Court rejected this argument. It found that Qihoo entrusted a third-party company to provide the web page acceleration service via a transmit server. When users downloaded Qihoo software from its official website www.360.cn, the downloading actually conducted from the transmit server provided by the third party. The third-party server did not revise the contents of the Qihoo website. It only copied and stored the website and improved the downloading speed. The Supreme People's Court held that this transmit server helped to disseminate the disputed software, so the place where it was located should be the

[31] *Rockwool International A/S v. Danian Rockwool Co Ltd.,* judgment issued by the Intermediate People's Court of Jiangmeng City Guangdong Province, (2014) Jiang Zhong Fa Zhi Min Chu Zi No. 95.

[32] *Tencent v Qihoo 360 Technology Co. Ltd and Qizhi Software Co. Ltd,* decided by the Supreme People's Court (2012) Min San Zhong Zi No. 3.

place where the tort occurred. When Qihoo uploaded software to its own server but allowed the users to download it via a third-party transmit server, it should expect that the court located in the place where the transmit server is located can hear disputes related to the software. A transmit server was located in Guangdong Province. Therefore, the court in Guangdong Province has jurisdiction on this case.

Rockwool and *Tencent* look apparently similar with a recent Australian case *Australian Competition and Consumer Commission v Valve Corporation (No 3)*[33], because in all three cases the third-party servers are located in the forum. Valve is a U.S. company and has no domicile in Australia. Australia Federal Court exercised jurisdiction on it partly because (1) Valve relied on third-party content delivery providers in Australia to provide proxy caching for Valve in Australia, and (2) Valve contracted with third-party service providers to provide content online in Australia and other places in the world, and Valve knew that the providers had servers in Australia.[34] However, *Valve* should be distinguished from *Rockwool* and *Tencent,* because Valve had approximately 2.2 million Australian accounts and earned significant revenue from Australia. These factors are more important for the Australian court to determine jurisdiction than the location of the server. Unlike *Valve*, the geographic location of the server is the sole factor for courts to exercise jurisdiction in *Rockwool* and *Tencent*.

(c) *Why does Chinese private international law allow courts to exercise personal jurisdiction solely based on the location of a server?*

The judgment of *Sunny Co* explains why personal jurisdiction can be based on the location of a non-resident defendant's server.[35] The infringer connects his or her computer or other terminals with a server to upload, download and disseminate information.[36] The terminal is essential because the infringer sends his or her "infringement order" from there.[37] However, online infringement does not occur until the order reaches the Internet server,.[38] Therefore, the location of the terminal or the server is where the online tort is committed.[39] Moreover, the court at the place where the server is located has proximity to collect evidence

[33] *Australian Competition and Consumer Commission v Valve Corporation (No 3),* [2016] FCA 196. This decision was upheld by the Full Court of the Federal Court of Australia, [2017] FCAFC 224, 351 ALR 584.
[34] *Valve Corporation (No 3),* [2016] FCA 196, paras 198–205. [2017] FCAFC 224, para 153.
[35] *Sunny Co. v. Taobao Co*., Civil Decision rendered by the Intermediate People's Court in Nanjing Jiangsu Province, (2014) Ning Zi Min Xia Zhong Zi No. 7.
[36] *Ibid.*
[37] *Ibid.*
[38] *Ibid.*
[39] *Ibid.*

and enforce judgments by deleting infringing contents from the server.[40] However, the location of the infringer's computer or other terminals may be fortuitous. Outsourcing the Internet service to a third-party is likely to make the location of the server unpredictable and unknown to the infringees. In Internet tort cases, collecting evidence is more than investigating the server and enforcing judgments often involves monetary compensation having no connection with the server either.

Therefore, this territorial-based jurisdiction rule should be construed from other aspects: it should be interpreted in the nationwide data localisation policy in China. Chinese law requires data localisation in fields of financial information,[41] population health information,[42] online publication,[43] online lending,[44] online taxi reservation,[45] online map service,[46] etc. The 2017 China Cybersecurity Law further provides that personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of China shall be stored within China.[47] In three aspects, this is a comprehensive data localisation requirement. First, "critical information infrastructure" has been defined broadly including but not limited to (1) infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs, and (2) other infrastructure, in case of damage, lost functions or data leakage, will result in serious damage to state security, the national economy, people's livelihood and public interest.[48] This definition is very comprehensive because energy, transport,

[40]This is significant to achieve global removal, block or delisting of the infringing contents from the Internet, see DJB Svantesson, "Jurisdiction in 3D- 'Scope of (Remedial) Jurisdiction' as a Third Dimension of Jurisdiction", (2016) 12 *Journal of Private International Law* 60, 63.

[41]Art. 6 of the Notice to Urge Banking Financial Institutions to Protect Personal Information, issued by the People's Bank of China on 21 January 2011 and effective on 1 May 2011.

[42]Art. 10 of the Measures for Administration of Population Health information, issued by National Health and Family Planning Commission and effective on 5 May 2014.

[43]Art. 8 of the Provisions on the Administration of Online Publishing Services, issued by Ministry of Industry & Information Technology and effective on March 10, 2016.

[44]Art. 27 of the Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions, issued by China Banking Regulatory Commission, Ministry of Industry & Information Technology, and Ministry of Public Security on 17 August 2016 and effective on the same date.

[45]Art. 27 of Interim Administrative Measures for the Business of Online Taxi Booking Services, issued jointly by the Ministry of Transport and other six state departments on 27 July 2016 and effective on 1 November 2016.

[46]Art. 34 of Regulations on Map Administration, issued by State Council on 26 November 2015 and effective on 1 January 2016.

[47]Art 37 of the China Cybersecurity Law, issued by the Standing Committee of the National People's Congress on 11 July 2016 and effective on 6 January 2017.

[48]*Ibid.*, art 31.

water conservancy, finance, public services represent very large industries. The Cybersecurity Law defines "network data" as all kinds of electronic data collected, stored, transmitted, processed and generated through the network.[49] However, no criteria are provided for "important data", which leaves potential for a broad definition. Personal information, whether important or not, collected and produced by critical information infrastructure operators shall be stored within China.[50] Second, this Article sets a default rule for data localisation and only in exceptional scenarios can critical information infrastructure operators provide such information and data to overseas parties or store it overseas. Critical information infrastructure operators shall conduct a security assessment according to the measures issued by the national cyberspace administration in conjunction with relevant departments of the State Council.[51] Two months before the China Cybersecurity Law came into effect, in April 2017, China's State Internet Information Office published draft Measures to Assess Whether Personal information and Important Data Can be Moved out of China for public opinions.[52] This draft extended the security assessment requirement from critical information infrastructure operators to all network operators. It provided that in any of the following circumstances, any network operators must report to industry or government supervisory authorities and the latter shall arrange a security assessment: (1) the data includes more than 500,000 entries of personal information, (2) the data is more than 1,000 GB, (3) the data includes information about a nuclear facility, the chemistry, biology, national defence and military industries, population and public health, large engineering projects, maritime environment as well as sensitive geographic information etc., (4) the data is about network security information of critical infrastructure and (5) other data that may impact upon national security and social public interests and industry or a government supervisory authority considers an assessment necessary.[53] In the following circumstances, data shall not be moved outside of China: (1) personal information without the person's permission or which may harm their interests, (2) when data may create risks to national politics, economy, science, defense and other security issues and may negatively impact on national security and harm social and public interests, (3) other circumstances determined by the national network and telecommunication department, police

[49] *Ibid.*, art 76.
[50] "Personal information" means all kinds of information recorded in an electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person's name, date of birth, personal identity card number, biology-identified personal information, address and telephone number. *Ibid*.
[51] *Ibid.*
[52] Measures to Assess Whether Personal information and Important Data Can be Moved outside of China (draft), published for public opinions by State Internet Information Office on 11 April 2017.
[53] *Ibid*, art 9.

department or security department.[54] If this draft becomes law, the government will have more control on data transmission and storage of all network operators in China. The third reason that the Cybersecurity Law imposes a comprehensive data localisation requirement is that the result of violating the data localisation requirement is severe. The competent government department can order the critical information infrastructure operator to take corrective action, confiscate its illegal income, impose a fine and may order it to suspend relevant business operations, cease operation for rectification, or close down the website and even revoke its business license.[55]

In this context, it is unsurprising that Chinese private international law allows courts to exercise personal jurisdiction solely based on the location of a server. Private international law becomes a tool to facilitate the public policy goal of cybersecurity.[56]

2. *The "target" factor and the interactive level of a defendant's website*

(a) *The "target" factor*

Private international law in foreign countries generally provide that a court can exercise personal jurisdiction when a non-resident defendant's activity "target" the forum (hereinafter "the 'target' factor"). For example, in the U.S., the seminal defamation case *Calder v. Jones* holds that a forum has personal jurisdiction over a non-resident defendant who committed an intentional act, expressly targets at the forum state, knowing that harm is likely to be suffered in the forum state. [57] In the Australian context, the leading case for the "target" factor is *Ward Group Pty Ltd v Brodie & Stone Plc.*[58] In this case, an Australian plaintiff claimed declarations and injunctions for trade mark infringement and passing off against the UK defendants. The Federal Court of Australia dismissed the suit because the advertising on the UK defendants' global websites targeted potential purchasers anywhere in the world at large, rather than specially targeted customers

[54]Art. 11 of Measures to Assess Whether Personal information and Important Data Can be Moved outside of China (draft).
[55]*Ibid*, art 66.
[56]This is not a unique case for China. The EU GDPR and the US Cloud Act also use private international law to achieve their public policy goals (privacy and personal information protection 1for the EU and combating serious crime for the US). For more detailed discussion, see infra Section 2.1.
[57]*Calder v. Jones*, 467 U.S. 783 (1984). In this case, Jones resided in California and her television career was centered there; the allegedly libelous article was written and edited by an editor and a writer residing in Florida with few contacts with California; the article was drawn from California sources and the magazine had its largest circulation in California. The U.S. Supreme Court held that "California is the focal point both of the story and of the harm suffered", so based on the "effects" of the defendants' Florida conduct in California, California could exercise personal jurisdiction over them. *Ibid*, at 788–789.
[58]*Ward Group Pty Ltd v Brodie & Stone Plc,* (2005) 143 FCR 479.

in Australia.[59] The "target" factor also appears in the EU jurisprudence. *Football Dataco Ltd* holds that the infringing act took place at least in the Member State where the person who requested and then received the data was located, provided that there was evidence that the person sending the data intended to target members of the public in that Member State.[60]

However, contrasted with foreign jurisprudence, Chinese courts does not consider the "target" factor when exercising personal jurisdiction on non-resident defendants. For example, in *Yahoo Inc. v Wang Lu,* Yahoo Inc. argued that it was registered in the U.S. and its servers that stored the disputed copyright infringement material was located in California, so the No. 1 Intermediate People's Court in Beijing had no jurisdiction.[61] The court rejected this argument and held that Beijing was the place where the tort occurred. This is because Wang used a computer in a notary office located in the forum to access Yahoo website and discovered Wang's works were illegally published online. This decision was affirmed by the Beijing High People's Court. Likewise, based on a trap purchase conducted by the attorney and a notary public hired by the plaintiffs, Apple Inc., a California company, was hailed into Beijing courts in several online copyright infringement cases, such as *Mr Mai Jia v. Apple Inc. and iTunes S. a. r. l.*[62]

[59] *Ibid*, the court reached this conclusion not only because the UK defendants subjectively did not target the Australian market, but also objectively, no evidence showed that the defendants had ever sold any products infringing the plaintiff's trademark in Australia, and the case was solely based on a trap purchase conducted by the plaintiff's solicitor. This means the UK defendants did not use this trademark in Australia except in the trap purchase. The court held that the trap purchase demonstrated that the plaintiff consented to that particular sale in Australia.

[60] *Football Dataco Ltd v. Sportradar GmbH* (Case C-173/11, 2012), paras 38–42. The ECJ hold that the UK court has jurisdiction for three reasons. Firstly, the subject matter of the data could have been of particular interest to members of the public in the UK because data on Sportradar's server related to English and Scottish football league matches and this shows Sportradar's intention to attract members of the public in the UK. Secondly, it was known by Sportradar's website operator that its data is likely to be accessed by members of the public in the UK. Sportradar's customers included a UK-based betting agency, which shows Sportradar's awareness that end-users accessing its data could be from the UK. Third, although Sportradar is a German company, it provides access to its football data in English. This also suggests Sportradar's intention to target a particular member state.

[61] *Yahoo! v Wang Lu,* (2006) Gao Min Zhong Zi No. 1365.

[62] Eg., *Mr. Mai Jia v. Apple Inc. and iTunes S. a. r. l.*, Civil Judgment issued by the Beijing No. 2 Intermediate People's Court, (2012) Er Zhong Min Chu Zi No. 5279, affirmed by the Beijing High People's Court, retried and affirmed by the Supreme People's Court in 2015, (2015) Min Shen Zi No. 1298. In this case, the plaintiff does not reside in Beijing. The court neither discussed whether the Apple app targets the Beijing/Chinese market nor what volume of sales actually made in Beijing/China. According to the Supreme People's Court Provisions on Infringement of the Right of Dissemination, the court exercised jurisdiction based on a trap purchase conducted by Mai's attorney in Beijing. Other similar cases include Han Ai Lian v. Apple Inc, (2012) Er Zhong Min Chu Zi No. 1560, Hao Qun v Apple

In these cases, plaintiffs were all Chinese novelists and did not reside in Beijing. Cases are concerned with apps that are uploaded to the iTunes store by third parties and contain copyright infringement materials.

Also involved a trap purchase, *Shanghai Shanda Group v. Apple Inc, C1wan Game (Beijing) Co., Ltd, and Beijing Zuoyi Xunchang Science Co., Ltd* is an unfair competition case.[63] Apple Inc. argued that the Beijing Haidian District Court had no jurisdiction because no prima facie evidence showing that it jointly committed the unfair competition against Shanda with the other two defendants who sold apps on AppStore. The court rejected this argument. Because the notary public hired by Shanda used an iPadmini to download an app from AppStore and this app allegedly conducted the unfair competition with the Shanda's online game. iPhone and iPad are developed, manufactured and sold by Apple Inc. These are the prima facie evidence showing that Apple Inc. is related to the alleged joint tort. The third defendant is registered in the Haidian District where the court is located. According to Article 21 of the CPL, the Haidian District People's Court have jurisdiction on Apple Inc. because it had jurisdiction on the third defendant.[64]

Ward Group, Yahoo, Mai Jia and *Shanghai Shanda Group* all involve trap purchases. However, different from *Ward Group* where the Australian court refrained from exercising jurisdiction, Chinese courts exercised jurisdiction based on trap purchases without considering whether the defendants targeted the forum and what the sales volume the defendants made there. In *Mai Jia,* Apple Inc. argued that the court awarded damages without considering the sales volume in the forum.[65] The plaintiff requested the compensation of CNY 30,423 as the cost of the trap purchase and CNY 1,290,000 as loss of profits. The court considered the originality of the plaintiff's works, their market value, the infringing activities conducted by the defendants and their negligence, and awarded CNY 200,000 as loss of profits and CNY 5,000 as reasonable litigation costs. The court did not indicate that CNY 200,000 was limited to the damages that the plaintiff suffered in the forum. The Supreme People's Court rejected Apple's argument and affirmed the number of damages.

Inc, (2012) Er Zhong Min Chu Zi No. 1557; Li Cheng Peng v Apple Inc, (2012) Er Zhong Min Chu Zi No. 2236; Kong Xian Zhao v Apple Inc, (2012) Er Zhong Min Chu Zi No. 1600.

[63] *Shanghai Shanda Group v. Apple Inc, C1wan Game (Beijing) Co., Ltd, and Beijing Zuoyi Xunchang Science Co., Ltd,* issued by the Beijing Haidian District Court, (2016) Jing 73 Min Xia Zhong No. 401.

[64] Article 21 of the CPL provides that, when a case involves multiple defendants, where the places of domicile or places of habitual residence of several defendants in the same action are located within the jurisdiction of two or more people's courts, both or all of such people's courts shall have jurisdiction over all defendants.

[65] *Mr Mai Jia v. Apple Inc. and iTunes S. a. r. l.*, Civil Judgment issued by the No. 2 Intermediate People's Court, (2012) Er Zhong Min Chu Zi No. 5279.

Moreover, both *Rockwool* and *Mai Jia* involve a network service provider. In *Mai Jia*, Apple Inc. is the network service provider that provides an online platform (i.e. iTunes store) to sell the disputed apps. In its judgment, the Supreme People's Court highlighted Apple's negligence in running this platform which jointly contributed to the alleged copyright infringement. In *Rockwool,* the Dalian Rockwool did not own and run www.chinarockwool.com; it rented the service from a third-party network service provider and built the website on the third-party server. Different from *Mai Jia,* the network service provider is not a party to the litigation in *Rockwool* and the judgment does not discuss whether the network service provider jointly conducted online trademark infringement with Dalian Rockwool. But the court exercised jurisdiction based on the geographic location of the network service provider's server. *Rockwool* reveals an ironic situation where a court can exercise jurisdiction on a non-resident defendant on a network service provider's server who is not a party to the action.

(b) *The interactive level of a defendant's website*

The leading case to consider the interactive level of a non-resident defendant's website is *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[66] This U.S. case establishes a sliding scale test for courts to determine personal jurisdiction. At one end of the sliding scale are active websites where a non-resident defendant clearly conducts business over the Internet, such as contracting with residents and repeatedly transmitting computer files over the nternet. The forum can exercise personal jurisdiction over the defendant. Passive websites are at the other end of the scale, where a non-resident defendant simply posts information online which is viewable for residents in the forum jurisdiction. The forum cannot exercise personal jurisdiction in the case of a passive website. In the middle of the scale are interactive websites where a user can exchange information with the host computer. Whether the court can exercise jurisdiction on an interactive website is based on the level of interactivity and commercial nature of the exchange of information.

Chinese courts explicitly rejected the sliding scale test in *Zhangjiakou Great Wall Brewery (Group) Limited Co v. COFCO Corporation.*[67] In this case, COFCO alleged that its registered trademark "Great wall brewery" is illegally used on the website of Zhangjiakou Great Wall Brewery. The Court in Beijing where the COFCO is domiciled exercised jurisdiction. Zhangjiakou Great Wall Brewery argued that the court had no jurisdiction because the websites should be divided into two types. One is active websites and the other passive websites.

[66] *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).
[67] *Zhangjiakou Great Wall Brewery (Group) Limited Co v. COFCO Corporation,* decided by the Beijing IP Court, Civil Division, (2016) Jing 73 Min Xia Zhong No. 68. COFCO's full name is China National Cereals, Oils and Foodstuffs Corporation.

The former can send out information to actively solicit customers, but the latter only posts information on its website and does not interact with customers. Zhangjiakou Great Wall Brewery argues that its website is a passive one, so the place where the customer is domiciled, namely the court in Beijing, has no jurisdiction. However, the Beijing IP court rejected this argument. The court held that Article 25 of the 2015 Judicial Interpretation of the CPL does not divide websites into active websites and passive websites. The Zhangjiakou Great Wall Brewery's argument would improperly limit the scope of application of the 2015 Judicial Interpretation. Moreover, Article 10.1(12) of the Chinese Copyright Law defines the right to disseminate information on the Internet as the right to provide works to the public in a wired or wireless manner so that the public can obtain the works at the time and place of their choice. In most cases of infringing other's right to disseminate information online, the defendant uploads other's works online and disseminate to the public. If the Zhangjiakou Great Wall Brewery's argument is correct, Article 25 of the Judicial Interpretation of the CPL cannot apply to all these cases, which obviously contradicts with the legislator's intention.

(c) *Why do the "target" factor and the interactive level of a defendant's website have no play in Chinese private international law?*

Both the "target" factor and the interactive level of a website help to justify when a forum should exercise personal jurisdiction on a non-resident defendant and when the forum should refrain from doing that. And the forum is often the plaintiff's domicile. Chinese law is pro-Chinese plaintiff by neither containing the "target" factor nor considering the interactive level of a defendant's website.

According to Chinese CPL, when an action is instituted against a defendant who has no domicile in China for a tort dispute, the court in the place where the tort occurs may have jurisdiction over the action.[68] The place where the tort occurs includes the place where the harm of a tort occurs, which further includes the plaintiff's domicile.[69] For online intellectual property (hereinafter "IP") infringement, allowing a plaintiff (i.e. the victim of the infringement) to bring a case in his or her domicile against an infringer can help deter infringement. This helps to enhance IP rights protection in China.[70]

Moreover, in circumstances prescribed by law, a court in the place where the computer or other equipment that an infringee discovers the infringing contents can also exercise personal jurisdiction over a non-resident defendant. This place is unnecessarily the plaintiff's domicile. For example, article 2 of the Supreme

[68]Art. 265 of the CPL.
[69]Art. 28 of the CPL and arts 24–25 of the 2015 Judicial Interpretation of the CPL.
[70]ZS Tang, YP Xiao and ZG Huo, *Conflict of Laws in the People's Republic of China* (Elgar Asian Commercial Law and Practice 2016), 82–84.

People's Court Judicial Interpretation Regarding Copyright Disputes on Computer Networks provides that if the place where the infringement occurs and the defendant's domicile *are difficult to identify*, the place where the computer or other equipment that the infringee discovers the infringement can be considered as the place where the infringement occurs.[71] This Judicial Interpretation was replaced by the Supreme People's Court Provisions on Infringement of the Right of Dissemination in 2012.[72] . The latter stipulates that where both the place of infringement and the defendant's domicile *are either difficult to identify or located outside of China*, the place where "the computer terminal or other equipment where the infringee discovers the infringing contents" is located may also be considered as the place where the infringement occurs.[73] When the law moves from "*difficult to identify*" to "*either difficult to identify or located outside of China"*, the legislator aims to largely facilitate Chinese plaintiffs to bring actions against foreign defendants. Compared with foreign laws, Chinese law is significantly more pro-plaintiff without requiring the "target" factor and proving the interactive level of the website.

Given that most of the online contents are created and controlled by U.S. internet companies, such as Google, Yahoo!, and Microsoft, even some non-U.S. western scholars argue that over relying on the connecting factors that focus on the defendant's place of acting, or the place of uploading, would lead to the improper import of American ideology.[74] This has special significance for China, because its politics, culture, standards, and values are distinct from those of the U.S. Therefore, Chinese courts feel the need to provide a forum for Chinese plaintiffs to protect their right of dissemination. In contrast, the "target" factor and the interactive level of a website may chill a court from exercising jurisdiction, which does not fully fit into the Chinese context.

Nevertheless, China's practice may not be consistent with the United Nation Convention on the Use of Electronic Communications in International Contracts, where China is a party. Article 10(3) of the Convention provides that "an electronic communication is received at the place where the addressee has its place of business".[75] Article 6(4)(a) also provides that "a location is not a place of business merely because that is where equipment and technology supporting an information system used by a party in connection with the performance of a

[71]Art 2 of the SPC on Copyright Disputes on Computer Networks.
[72]Art 15 of SPC Provisions on Infringement of the Right of Dissemination. Its Article 3 provides that infringement of the right of dissemination refers to the cases where a network user or network service provider provides, on an information network, any work, performance, or audio or video recording which a right holder enjoys the right to disseminate on information networks without the permission of the copyright holder.
[73]*Ibid*, art. 15.
[74]R Mortensen, R Garnett and M Keyes, *Private International Law in Australia* (3rd edn, LexisNexis Butterworths 2015), 60.
[75]China signed the Convention in 2006 but has not ratified it yet.

contract are located." Although the Convention regulates contracts, it shares common implications with tort, that is if "the computer terminal and other equipment" is owned by the plaintiff, they should not be in a fortuitous location. Therefore, Chinese courts may need to be more cautious when exercising personal jurisdiction over non-resident defendants based on the location of the infringee's server when it is located outside of his or her domicile or the place of business.

B. Applicable law

The international trend of applicable law to online data protection mainly has two features. First is that courts tend to extra-territorially apply domestic laws to foreign Internet companies who have no physical presence in the fora.[76] Second, the enforcement of domestic law often relies on global Internet intermediaries, such as Google, Yahoo, and Skype.[77] In contrast, because of the high-level data localization and Internet censorship, Chinese legislators focus more on domestic compliance with data regulations rather than their extra-territorial application. However, like foreign countries, China also resorts to Internet intermediaries to enhance enforcement of domestic law.

1. *Connecting factors*

The *United States v. Microsoft* and the CLOUD Act in the U.S., and the GDPR in the EU vividly demonstrate the trend of extra-territorial application of domestic data regulations.

United States v. Microsoft Corp. is concerned with whether the U.S. Stored Communications Act can be applied extraterritorially to Microsoft's server in Ireland.[78] Before the Supreme Court of the U.S. renders a decision, the U.S. Congress passed the CLOUD Act. The Act explicitly provides that a provider of electronic communication service or remote computing service shall disclose to the U.S. government the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, "regardless of whether such communication, record, or other information is located within or outside of the U.S."[79] The Act defines "a customer or subscriber" as a U.S. person and reside in the U.S. "U.S. person" means a citizen or national of the U.S., an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the U.S. or aliens lawfully admitted

[76] See *infra* Section 2.1.
[77] See *infra* Section 2.2.
[78] *United States v Microsoft Corp.*, No. 17-2, 584 U.S. __(2018).
[79] Sec. 3 of the CLOUD Act. The Act allows the U.S. government to conclude executive agreements with foreign governments to for the mutual data disclosure purpose.

for permanent residence, or a corporation that is incorporated in the U.S.[80] The Act is clearly featured with the extra-territorial application.

In the EU, GDPR has replaced the Data Protection Directive 95/46/EC and aims to protect all EU citizens from privacy and data breaches.[81] It will cover the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.[82] It will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities are related to: offering goods or services, irrespective of whether payment is required, to EU citizens; or the monitoring of their behaviours that takes place within the EU.[83] Non-EU business processing the data of EU citizens will also have to appoint a representative in the EU. Therefore, by its expanded territorial reach, the GDPR may create an international EU data protection regime.

Therefore, both the Cloud Act and GDPR use the citizenship or habitual residence of the data subjects as a connecting factor for the application of relevant data protection laws. The geographic location where a server is situated or where data is processed is irrelevant. Unlike the U.S. and the EU, Chinese data protection law uses different connecting factors. Like its territorial-oriented personal jurisdiction rule, Chinese applicable law for online data protection uses the geographic location of data activities in China as a connecting factor.

If a data activity takes place in China, China will apply its data protection law to this activity. The activities may include data collecting, owning, processing, controlling, using, etc. For example, Article 10 of Provisions on the Administration of Internet Information Search Services requires that an Internet information search service provider shall provide objective, impartial and authoritative search result, which shall comply with the socialist values.[84] This is confirmed by the Cybersecurity Law.[85] The application of Chinese law helps reinforce Chinese values[86] and ultimately serves political stability.

A typical example is the broadcasting of Eurovision Song Contest in China. The online streaming technology makes broadcasting a TV program filmed

[80]Sec. 5 of the CLOUD Act.
[81]GDPR was adopted on 8 April 2016 and took effect on 25 May 2018.
[82]Art. 3.1 of the GDPR.
[83]*Ibid*, art. 3.2.
[84]Provisions on the Administration of Internet Information Search Services, issued by the State Internet Information Office on 25 June 2016 and effective on 1 August 2016. Similar laws include article 3 of Provisions of the Administration of Internet Live-Streaming Services, issued by the State Internet Information Office on Nov 4, 2016 and effective on Dec 1, 2016; article 3 of Measures for the Administration of Cyber Performance Business Operations, issued by the Ministry of Culture on Feb 12, 2016 and effective on Jan 1, 2017.
[85]Art. 50 of the Cybersecurity Law.
[86]See Opinions to Promote the Healthy and Orderly development of Mobile Internet (n83), para 20.

abroad much easier in China. Chinese online broadcaster Mango TV has partnered with the European Broadcasting Union (hereinafter "EBU") to broadcast the Eurovision Song Contest in China for a few years. In May 2018, the EBU decided to terminate this year's partnership with Mango TV. It is suspected that because when Mango TV broadcasted the first Semi-Final of the 2018 Eurovision Song Contest on its website in China, it removed two performances. In one performance, the content shows LGBT; in the other, the singer and his accompaniment band are with too many tattoos.[87] Moreover, when broadcasting, Mango TV also blurred the LGBT flags waved by the audience in the crowd. In a press release, the EBU said: "This is not in line with the EBU's values of universality and inclusivity and our proud tradition of celebrating diversity through music."[88] Consequently, Mango TV will not be permitted to broadcast the second Semi-Final or the Grand Final in China. Since 2016, China State Administration of Press, Publication, Radio, Film and Television (hereinafter "CPPRFT") has banned broadcasting depiction of LGBT on TV.[89] In January 2018, it imposed new standards requiring that programs should not feature actors with tattoos (or depict) hip-hop culture, sub-culture (non-mainstream culture) and dispirited culture (decadent culture).[90] These regulations are applied to both Chinese and foreign programs broadcasted in China. Although filmed in Europe, the broadcasting of the Eurovision Song Contest took place in China, it should comply with the CPPRFT regulations. Moreover, all programs broadcasted in China should be approved by relevant Chinese government agencies, which is not only a mandatory law in China but also its public policy.[91] This is demonstrated by *USA Productions and Tom Hulett & Associates v China Women Travel Agency.*[92] In this case, the

[87]Eurovision 2018: China Removes Albania and Ireland from Semi-final 1 Broadcast, http://esctoday.com/165905/eurovision-2018-china-removes-albania-ireland-semi-final-1-broadcast/.

[88]EBU Terminates This Year's Partnership with Mango TV. https://www.broadbandtvnews.com/2018/05/14/ebu-terminates-this-years-partnership-with-mango-tv/.

[89]China Bans Depictions of Gay People on Television, https://www.theguardian.com/tv-and-radio/2016/mar/04/china-bans-gay-people-television-clampdown-xi-jinping-censorship. China Tightens Censorship of Online Dramas, http://chinafilminsider.com/china-tightens-censorship-of-online-dramas/.

[90]China State Administration of Press, Publication, Radio, Film and Television Issued New Standards for Programs, http://ent.sina.com.cn/tv/zy/2018-01-19/doc-ifyquptv7935320.shtml.

[91]The differences between mandatory law and public policy exception is significant as demonstrated in the recognition and enforcement of arbitral awards and judgments. Awards and judgments that violate the mandatory law of the requested state may still be recognized and enforced. But if they violate its public policy, the requested state will not recognize and enforce them.

[92]*USA Productions and Tom Hulett & Associates v China Women Travel Agency* (Reply of the Supreme People's Court to a Request for Instructions on the Non-Recognition and Non-Enforcement of an Arbitration Award Concerning *USA Productions and Tom Hulett & Associates v China Women Travel Agency* (26 December 1997, Supreme People's Court)).

two plaintiffs concluded a "Contract and Performance Agreement" to hire American actors to perform in China. The Agreement clearly stipulated: "[t]he actors should do their best to observe Chinese law and policies and achieve the best entertainment result of their performance." The two plaintiffs also concluded an annex to the Agreement, which provided that the China Ministry of Culture had the right to review and approve the details of the actors' performances. According to the Agreement and the Annex, the two plaintiffs signed a Contract with China Women's Travel Agency for performances in China in 1992. However, the U.S. actors breached the Contract and performed not according to the performance contents approved by the China Ministry of Culture. Instead, they performed a "heavy metal song." The Ministry considered that the performance was not suitable for China's national conditions and violated the social and public interests of China. Considering the bad impacts resulted from the performance, the Ministry decided to ban their performances in China. Consequently, the profits from the performances decreased. But this is caused by the U.S. actors' serious breach. The Supreme People's Court held that the arbitral award rendered by the China International Economic and Trade Arbitration Commission ignored the above facts and was completely wrong. If the People's Court enforces this arbitral award, it will undermine China's social and public interests. Therefore, the Supreme People's Court rejects the recognition and enforcement of the award. Although *USA Productions and Tom Hulett & Associates* is a case decided almost three decades ago, its holding still reflects the law in China. The public policy exception is available for Chinese parties who work with foreign partners, such as EBU, to ensure their online broadcasting or performance business in China complying with Chinese law.

The Internet has no borders. Why Chinese law focuses on domestic compliance rather than extra-territorial application? An important reason is that the strict censorship system can block illegal contents posted on foreign websites from reaching Chinese Internet users. Chinese data localization policy also limits the chance that Chinese data subject's information flows outside of China. In these contexts, extra-territorial application of Chinese data protection law becomes practically less important.

2. *Internet intermediaries*

Recent years have witnessed many courts apply domestic law extraterritorially to Internet intermediaries. For example, in *LICRA v. Yahoo!,* the Tribunal de Grande Instance de Paris applies French law to Yahoo. Com and orders it to take all possible measures to dissuade and prevent access in France to Yahoo! Auction sites that sell Nazi and related commodities.[93] In *Procureur-General v. Yahoo! Inc.*

[93] *LICRA v. Yahoo!, Inc.*, Tribunal de Grande Instance de Paris [TGI] [High Court of Paris], May 22, 2000, *available at* https://perma.cc/738B-V9BM.

and *Procureur General v. Skype,* Belgian courts apply the Belgian law to Yahoo! and Skype who have no subsidiaries in Belgium, because the law at issue covered "any operator or provider that actively aims its economic activities on [Belgium] consumers."[94] In *Google v. Equustek,* the Canadian Supreme Court issued an injunction to Google, a non-party to a trademark infringement suit, to de-index the defendant's websites through any of its search portals worldwide.[95]

China also tries to achieve a seamless application of its data protection law through Internet intermediaries. Chinese law uses the place of providing service as a connecting factor to apply Chinese law to Internet intermediaries. For example, the Interim Provisions on the Administration of the Development of Public Information Services of Instant Messaging Tools (hereinafter "Provisions on Instant Messaging Tools") applies to companies that provide instant messaging service in the territory of China and such service shall comply with Chinese censorship, namely the requirements of "seven bottom lines" including Chinese laws and regulations, socialist systems, national interests, legitimate interests of citizens, public order, social morality and information authenticity.[96] WeChat (Weixin) is a very popular instant messaging app developed by Tencent Company. It combines calling, messaging, social media and payment functions.[97] With its ios, Android, and web versions, it has over 1 billion monthly active users (902 million daily active users) by 2018.[98] Every WeChat user needs to link his or her WeChat account with a mobile phone number. If the mobile phone number is Mainland, the account will be subject to Chinese law. WeChat adopts a more liberal censorship for users who link their account with a non-Mainland mobile phone number. WeChat poses two choice-of-law issues.

First, the place of providing online service may not be the same as the place of receiving such service. A research shows that when a Weichat user's account,

[94] *Procureur-General v. Yahoo! Inc.*, Hof van Cassatie [Cass.] [Court of Cassation] [Supreme Court of Belgium], Dec. 1, 2015, No. P.13.2082.N (Belg.), *translated in* 13 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REVIEW 156 (2016). *Procureur General v. Skype*, Tribunal de Première Instance [Civ.] [Tribunal of First Instance], Mechelen, Oct. 27, 2016, No. ME 20.4.1 105151-12, ¶¶ 1.2-1.5 (Belg.), *available at* https://perma.cc/C5Z7-EZ9Y.

[95] *Google v. Equustek Solutions*, No. 5:17-cv-04207, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

[96] Art. 2 of the Interim Provisions on the Administration of the Development of Public Information Services of Instant Messaging Tools, promulgated on 7 August 2014 and effective on that date. Other similar regulations include article 2 of Provisions on the Administration of Mobile Internet Applications Information Services, Art. 2 of the Regulations for Internet News Information Service, article 2 of the Regulations of Internet Forum Community Service, and article 2 of the Regulations of Internet Thread Comments Service.

[97] Connecting a Billion People with Calls, Chats, and More, https://www.wechat.com/en/.

[98] Wechat, https://en.wikipedia.org/wiki/WeChat#cite_note-138. Facebook has more than 2.2 billion monthly active users as of January 2018, https://en.wikipedia.org/wiki/Facebook. Twitter has more than 319 million monthly active users as of 2016, https://en.wikipedia.org/wiki/Twitter.

which is previously linked with a Mainland phone number, relinks to a non-Mainland number, the account will be still subject to the strict Mainland censorship rather than the more liberal censorship for non-Mainland phone numbers.[99] Suppose that a person emigrates from China to Australia, becomes an Australian citizen and resides in Sydney, he relinks his previous WeChat account to an Australia phone number and uses WeChat in Australia. He will still be subject to the Chinese censorship. Consequently, his online speech that fully complies with Australian law will be blocked because of violation of Chinese Provisions on Instant Messaging Tools. In this case, the place of providing online service is China because Wechat is managed by Tencent, a Chinese company. However, the place of receiving service is in Australia. An argument to justify Wechat's application of Chinese law is that a Wechat user should sign the Agreement on Software License and Service of Tencent Weixin, which indicates that the applicable law to this Agreement is the Provisions on Instant Messaging Tools.[100] However, freedom of speech is considered as a fundamental human right in Australia. It is doubtable whether Chinese law against this fundamental right can be applied to an Australian resident using an App in Australia although this App is developed by a Chinese company. Just like *LICRA v. Yahoo!,* the French court held that the freedom of speech under the U.S. Fourteenth Amendment should not be applied to French residents in France even if Yahoo! is a U.S. company.

Second, WeChat uses where a user's mobile phone number is registered to determine the applicable law (i.e. the level of censorship).[101] This begs questions. A French citizen may have a Mainland phone number linked to WeChat and access WeChat in Iran. A Chinese citizen may have his account bound with a U.S. phone number and use WeChat in China. It is arbitrary that the French citizen will be subject to a stricter censorship than the Chinese citizen simply because of the nationalities of their mobile phone numbers. The data protection law in France, Iran, China and the US are significantly different. WeChat can constantly access a user's geographic information. Is geographic location a better connecting factor for the applicable law? It may be "yes" because at least it helps to avoid the arbitrary application of the law. However, it may lead to a fortuitous application because human beings are mobile. The above discussion shows that the

[99]The research was carried out by the Citizen Lab, a research group at the University of Toronto in 2016 and 2017. For 2016 report, see One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally, https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/; for 2017 report see What Happens When You Try to Send Politically Sensitive Messages on WeChat, https://qz.com/960948/what-happens-when-you-try-to-send-politically-sensitive-messages-on-wechat/.

[100]Art. 8.1.2.1 (11) of the Mainland Agreement on Software License and Service of Tencent Weixin, https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&cc=CN.

[101]*Ibid.*

U.S. and the EU have moved to abolish the geographic location as a connecting factor for the applicable law. Instead, they use citizenship or habitual residence of data subject as a connecting factor. Should WeChat require users to declare their citizenship or habitual residence? How do WeChat know its users' declarations are true? Habitual residence requires factually a person remains in a place continuously for a certain period of time and psychologically this person desires to stay there. The geographic information may help to determine the factual factor, but how to determine the psychological factor? The conundrum of connecting factors is not only an issue for WeChat but also for other social media such as Facebook and Twitter.

C. Conclusion

China personal jurisdiction and applicable law for online data protection are mostly territorial-based. This is not because Chinese legislators adopt the exceptionalist or unexceptionalist view. Rather, this is because territorial-based private international law fits into China's economic-wide data localization policy and the strict censorship system. It can be seen "as a geographic strategy to control people and things by controlling area … the power of topography conceals the topography of power."[102] It is also consistent with the tradition of Chinese private international law, which generally refrains from the extra-territorial application.

China's example has at least two broad international implications. First, the global development of private international law for online data protection is diversified. This is because not every country supporting the free flow of data across borders. Even between the U.S. and the EU where data policy is relative liberal, exists important differences about data protection.[103] Data localization and censorship are not a unique policy in China. It has been adopted by many other countries.[104] Data localization and censorship can avoid some thorny issues about jurisdiction and applicable law regarding data. For example, controversial cases against Google have occurred in France, Belgium, the EU, Canada, etc,[105] but none is in China. This reason is simple: Google is banned in China. However, data localization and censorship also create other difficult private international law issues, as the WeChat example shows. Second, China's example demonstrates that in the Internet era, states have looked for private-international-law tools to advance their public policy claims on data protection.

[102]Zekos (n 11) 8.
[103]D Cole and F Fabbrini, "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders", (2016) 14 *International Journal of Constitutional Law* 220, 220–237.
[104]A Chander and U P Le, "Data Nationalism", (2014) 64 *Emory Law Journal* 677, 679–708.
[105]See *supra* Section 2.2.

Private international law should be developed by responding to non-private law issues such as privacy protection, combating serious crime, national security, and political stability.[106]

Disclosure statement

No potential conflict of interest was reported by the author.

[106]For scholarship discussing that private international law can go beyond its traditional "private" domain to serve global governance, e.g. H Muir Watt and DPF Arroyo, *Private International Law and Global Governance* (OUP, 2014), 2–19.