


ARTICLE

Applicable Law to Transnational Personal Data: Trends and Dynamics

Jie (Jeanne) Huang* 

(Accepted 27 May 2020)

Abstract

The recent COVID-19 outbreak has pushed the tension of protecting personal data in a transnational context to an apex. Using a real case where the personal data of an international traveler was illegally released by Chinese media, this Article identifies three trends that have emerged at each stage of conflict-of-laws analysis for *lex causae*: (1) The EU, the US, and China characterize the right to personal data differently; (2) the spread-out unilateral applicable law approach comes from the fact that all three jurisdictions either consider the law for personal data protection as a mandatory law or adopt connecting factors leading to the law of the forum; and (3) the EU and China strongly advocate deAmericanization of substantive data protection laws. The trends and their dynamics provide valuable implications for developing the choice of laws for transnational personal data. First, this finding informs parties that jurisdiction is a predominant issue in data breach cases because courts and regulators would apply the law of the forum. Second, currently, there is no international treaty or model law on choice-of-law issues for transnational personal data. International harmonization efforts will be a long and difficult journey considering how the trends demonstrate not only the states' irreconcilable interests but also how states may consider these interests as their fundamental values that they do not want to trade off. Therefore, for states and international organizations, a feasible priority is to achieve regional coordination or interoperation among states with similar values on personal data protection.

Keywords: COVID-19; applicable law; transnational; personal data; conflict of laws

A. Introduction

The recent COVID-19 outbreak has pushed the tension of protecting personal data in a transnational context¹ to an apex. This is because COVID-19 spreads fast with the international travel of people.² Many countries require international travelers to disclose their personal information—such as name, gender, date of birth, travel history, and purpose of travel and residence—and

*Jie (Jeanne) Huang, Associate Professor at University of Sydney Law School. The author is very grateful for the anonymous reviewer's comments and the grant support provided by the University of Sydney Law School and the Indian Development Fund. All errors remain my own. Jeanne.huang@sydney.edu.au.

¹In this Article, “personal data” and “personal information” are used interchangeably. “Personal data breach” means accidental or unlawful destruction, loss, alteration, disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Personal data is transnational when, for example, it involves foreign data subjects, or is collected, saved, or processed in different jurisdictions.

²*What You Need to Know about Coronavirus (COVID-19)*, AUSTRALIAN GOV'T DEP'T HEALTH, <https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert/what-you-need-to-know-about-coronavirus-covid-19> (last visited Apr. 1, 2020).

impose quarantine requirements accordingly.³ In late March 2020, Chinese media widely reported an Australian lady with Chinese origin who breached the home quarantine requirement by jogging without wearing a mask in the residential complex where she was temporarily living in Beijing.⁴ A Chinese policeman required her to stay at home.⁵ The lady refused and alleged she was abused by the policeman.⁶ Chinese media released her photo,⁷ age, flight information, name,⁸ nationality, and temporary home address in Beijing. The Chinese and Australian universities she graduated from and the years of her graduation, her employment history and positions, and her current employer and salary were also released.⁹ Her employer was the Chinese subsidiary of German pharmaceutical giant Bayer.¹⁰ Bayer China quickly made an announcement and fired this lady for breaching the Chinese quarantine requirement.¹¹ Because her Chinese visa was sponsored by Bayer, the Chinese government revoked her visa and deported her after Bayer terminated her employment contract.¹² Clearly, the lady violated the COVID-19 mandatory self-quarantine regulation in China. Her conduct threatened the public health. However, did her offense justify releasing her detailed personal information online? Based on the released information, her identity can be easily ascertained. She is an Australian citizen and arrived in China just one day before the incident occurred. Therefore, she was unlikely to obtain a habitual residence in China in such a short period.¹³ She was a senior director working for Bayer China, which was owned by Bayer Germany, though news reports did not indicate whether she was hired by Bayer Germany and whether her personal employment information was processed in Germany. This incident is not a unique case. It is typical and demonstrates the tension between preventing COVID-19 and protecting transnational personal data: Which law should be applied to the personal data of an international traveler who violates a local quarantine law?

Protecting personal data in the transnational context is important and necessary. In modern society—where individuals often travel across borders¹⁴—technology such as the Internet and the cloud is inherently transnational,¹⁵ and online service providers also actively make their service

³Nicole Mills, *Coronavirus quarantine rules will force international arrivals into two-week quarantine in hotels and caravan parks*, ABC NEWS (Mar. 27, 2020, 2:12 AM), <https://www.abc.net.au/news/2020-03-27/coronavirus-quarantine-laws-force-international-arrivals-hotels/12097312>; *Travel and COVID-19*, AUSTRALIAN GOV'T DEP'T AGRIC. WATER & ENV'T, <https://www.agriculture.gov.au/travelling/to-australia/advice-to-travellers/human-health/coronavirus> (last visited Apr. 1, 2020).

⁴Nectar Gan, *A Chinese Australian Woman breached coronavirus quarantine in Beijing to go for a Jog—and lost her job*, CNN (Mar. 20, 2020, 7:46 AM), <https://edition.cnn.com/2020/03/20/asia/beijing-coronavirus-woman-fired-intl-hnk/index.html>.

⁵*Id.*

⁶*Id.*

⁷Some Chinese media mosaicked her face and some did not.

⁸The media released her Chinese surname and the last Chinese character in her name.

⁹*The Jogging Woman Liang X Yang Was Deported: Australia Locked Down and Rejecting Her Return! How Will She Make a Living?*, SOHU, https://www.sohu.com/na/383768197_120018507?scm=1002.45005a.15d015e01a3.PC_NEW_ARTICLE_REC&spm=smpc.content%2Fnew.fd-d.8.1585353600026oXoZw5N (last visited Apr. 1, 2020); *Rich and Ill-tempered "Australian Jogging Woman" Graduated from Famous Universities and Earned One Million*, ZHIHU, <https://zhuanlan.zhihu.com/p/115002155> (last visited Apr. 1, 2020).

¹⁰*That Australian Who Jogged without Wearing a Mask and Shouted for Help Was Fired!*, SINA, <https://cj.sina.com.cn/articles/view/6115560351/16c840b9f01900o0dd> (last visited Apr. 1, 2020).

¹¹*Id.*; cf. *Other New Reports Indicate that This Lady May Go to Germany and Work for Bayer*, SOHU, https://www.sohu.com/a/383204342_334936?scm=1002.44003c.fe017c.PC_ARTICLE_REC&spm=smpc.content.fd-d.2.1585791557071kSJKI7d&trans_=000012_sogou_fl_ty&f=index_pagerecom_2 (last visited Apr. 1, 2020).

¹²*Australian "Jogging Woman," Deported!*, BEIJING DAILY, <http://www.bjd.com.cn/a/202003/19/WS5e732c99e4b01e8b9150a2f8.html> (last visited Apr. 1, 2020). Before this lady was deported, she had no confirmed case of COVID-19. She had not faced any judicial proceedings in China.

¹³Based on the media reports, it is unclear whether this lady had lived in China long enough in previous years that she had already obtained a residence under Chinese law before this incident.

¹⁴See Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 EUR. J. INT'L L. 441 (2010).

¹⁵Georg Haibach, *Cloud Computing and European Union Private International Law*, 11 J. PRIV. INT'L L. 252, 253–54 (2015).

accessible around the world.¹⁶ Domestic regulators have also become more serious about protecting personal data in the transnational context.¹⁷ The EU implemented the General Data Protection Regulation (GDPR).¹⁸ The California state government adopted the California Consumer Privacy Act.¹⁹ China incorporated the right to personal data into the Chinese General Rules of the Civil Law.²⁰ Australia is robustly creating the Consumer Data Right.²¹ Nonetheless, the contents of domestic laws for personal data protections are not the same. For example, Chinese media published the employment—both current and past employers—and education information of the international traveler who violated the COVID-19 quarantine requirement. In the EU, such personal information would be protected under the GDPR according to the Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak adopted by the European Data Protection Board.²² In Australia, some states may release the flight information and places where an international traveler infected by COVID-19 visited, but his or her full name, employment position and salary, and education information are never released, unless this information is necessary to lessen or prevent a serious and imminent threat to the health of the Australian public.²³

The different domestic responses to protecting personal data in combating COVID-19 demonstrate the need to identify the applicable law to transnational personal data. According to conflict of laws, in finding *lex causae*, there are three stages: First, characterize the issue into one of the established choice of law classifications by identifying the nature of the subject matter. Second, select the rule of conflict of laws which lays down a connecting factor for the issue in question. Third, identify the system of law which is tied by the connecting factor found in stage two to the issue characterized in stage one.²⁴ There are valuable national studies or comparative scholarship

¹⁶Michael D. Simpson, Comment, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 669, 670–73 (2016).

¹⁷Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L ECON. L. 245 (2018).

¹⁸Regulation 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, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

¹⁹The California Consumer Privacy Act passed on September 23, 2018, and became effective on January 1, 2020. CAL. CIV. CODE § 1798.198 (West 2020) [hereinafter CCPA]. California is estimated to make up about 13% of the US marketplace. The International Association of Privacy Professionals estimated that the Act will affect at least 500,000 US businesses. Jeewon Kim Serrato et al., *Covered Entities*, NORTON ROSE FULBRIGHT: CAL. CONSUMER PRIVACY ACT BLOG SERIES (Aug. 16, 2018), <https://www.dataprotectionreport.com/2018/08/california-consumer-privacy-act-blog-series-covered-entities/>.

²⁰Minfa Zongze [General Rules of the Civil Law of China] (promulgated by the Twelfth Nat'l People's Cong., Mar. 15, 2017, effective Oct. 1, 2017), <http://www.court.gov.cn/zixun-xiangqing-37832.html> [hereinafter General Rules of the Civil Law of China].

²¹*Treasury Laws Amendment (Consumer Data Right) Bill 2019*, PARLIAMENT AUSTRAL., https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6370 (last visited Sept. 10, 2019). The third reading of the Bill was agreed to on August 1, 2019.

²²*Statement by the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak*, EUROPEAN DATA PROT. BD. (Mar. 16, 2020), https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en (indicating that “the EDPB would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subject”) [hereinafter *Statement by the EDPB Chair*].

²³In New South Wales, Australia, personal information is defined under the *Privacy and Personal Information Protection Act 1998* (NSW) s 4 (Austl.) [hereinafter PPIPA] as information or an opinion—including those forming part of a database and whether or not recorded in a material form—about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. The NSW government agency may disclose the relevant personal information to the general Australian public, including those outside of NSW jurisdiction, or to an Australian Commonwealth agency. The relevant agency is allowed to do so if such a disclosure is reasonably believed by the NSW government agency to be necessary to lessen or prevent a serious and imminent threat to the health of the Australian public, according to s 19(2)(f) of PPIPA. The *Public Health Act 2010* (NSW) (Austl.) also allows the government to release certain personal information so the general public can keep its distance from the home address or the places that a patient has visited.

²⁴*Macmillan Inc. v. Bishopsgate* [1996] 1 WLR 387 (Eng.).

exploring personal data protection.²⁵ Yet, little conflict-of-laws literature has compared how China, the US, and the EU characterize the right to personal data, what connecting factors they consider, and which law they eventually apply to protect personal data. These issues are important, especially in the context of COVID-19, where states strictly monitor international travelers. Going beyond combating COVID-19, exploring these issues can inform domestic legislators of the convergence and divergence of different national laws. It also helps technology companies design their global service. It further provides useful references for international organizations who plan to propose treaties or model laws to coordinate national laws.

This Article is divided according to the three stages of conflict-of-laws analysis. The first section argues that China, the US, and the EU characterize the right to personal data in very different ways. The EU highlights it as a fundamental human right, the US deems it a civil liberty, and China considers the right to personal data as a personality right. The second section analyzes the connecting factors used in the three jurisdictions. All three jurisdictions make the territorial scope of their personal information protection law broad enough to ensure the application of *lex fori*. Alternatively, they consider the personal data protection law as a mandatory law and as a curtailment of party autonomy. The consequence is the spread-out unilateral applicable law approach in contracts, torts, and equity. Based on the *lex fori* approach discussed in the second section, the third section analyzes the substantive law for personal data protection in the US, the EU, and China. It argues that the global trend for the substantive law is shifting from Americanization to deAmericanization. The first three sections of the Article present three trends at each stage of conflict-of-law analysis: The multi-faceted legal nature of the right to personal data, the spread-out unilateral applicable law approach, and the de-Americanization of substantive personal data protection law. The fourth section explores the dynamics among these trends. It argues that the widely adopted unilateral applicable law approach in contracts, torts, and equity cases of personal data breach has almost eliminated the need for conflict of laws analysis in transnational data breaches. In contrast, the gaps between the substantive domestic law for personal data protection are widening with the deAmericanization movement. The fifth section concludes the Article.

B. Multi-Faceted Right to Personal Data

There is no uniformity to characterize the right to personal data in the US, EU, and China. This is because this right is considered a fundamental human right in the EU, a civil liberty in the US, and a personality right in China.²⁶ Although apparently both the US and China can protect the right to personal data as a consumer right or a property right, their laws differ in nature.²⁷

²⁵For country or comparative studies on applicable law for personal data, see, for example, Chenguo Zhang, *China's New Regulatory Regime Tailored for the Sharing Economy: The Case of Uber under Chinese Local Government Regulation in Comparison to the EU, US, and the UK*, 35 *COMPUTER L. & SECURITY REV.* 462 (2019); Michael Ng, *Choice of Law for Property Issues Regarding Bitcoin Under English Law*, 15 *J. PRIV. INT'L L.* 315 (2019); Tobias Lutz, *Internet Cases in EU Private International Law—Developing a Coherent Approach*, 66 *INT'L & COMP. L.Q.* 687 (2017); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 *GEO. L.J.* 115 (2017); Andrew Keane Wood, *Against Data Exceptionalism*, 68 *STAN. L. REV.* 729, 730–88 (2016); Dan Jerker B. Svantesson, *Jurisdiction in 3D—“Scope of (Remedial) Jurisdiction” as a Third Dimension of Jurisdiction*, 12 *J. PRIV. INT'L L.* 60 (2016); Jennifer Daskal, *The Un-Territoriality of Data*, 125 *YALE L.J.* 326 (2015); Maja Brkan, *Data Protection and European Private International Law: Observing a Bull in a China Shop*, 5 *INT'L DATA PRIVACY L.* 257 (2015); Rita Matulionyte, *Calling for Party Autonomy in Intellectual Property Infringement Cases*, 9 *J. PRIV. INT'L L.* 77, 77–97 (2013); Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 *EMORY L.J.* 677 (2014); Salil K. Mehra & Marketa Trimble, *Secondary Liability, ISP Immunity, and Incumbent Entrenchment*, 62 *AM. J. COMP. L.* 685 (2014); Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 *AM. BUS. L.J.* 413 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 *WASH. L. REV.* 385, 386–418 (2013); Gregory E. Maggs, *Regulating Electronic Commerce*, 50 *AM. J. COMP. L.* 665 (2002).

²⁶See *infra* Section B.I.

²⁷See *infra* Sections B.II and B.III.

I. Human Right

In the EU, a data subject's right to his or her personal data is characterized as a "right to privacy with respect to the processing of personal data."²⁸ Such a right is considered to be a fundamental one and cannot be outweighed by other values.²⁹ Protection of personal data is founded upon human rights treaties within the EU.³⁰ Under the heading "Right to respect for private and family life," Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: "Everyone has the right to respect for his private and family life, his home and his correspondence."³¹ The European Charter for Fundamental Human Rights goes a step further, providing in Article 8(1) that "[e]veryone has the right to the protection of personal data concerning him or her."³² Article 8(2) of the Charter authorizes the processing of personal data if certain conditions are satisfied—providing that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."³³ Additionally, a right to data protection is also protected by Article 16 of the Treaty on the Functioning of the European Union.³⁴

The US is not a party to the European Convention for the Protection of Human Rights and Fundamental Freedoms or the European Charter for Fundamental Human Rights. In the US, the right to privacy is defined as the "right to be alone."³⁵ It is a civil liberty protected by the Constitution of the US.³⁶ The Fourth Amendment protects personal information from unreasonable searches and seizures of the government.³⁷ As such, it has limited implications for most scenarios involving transnational personal data, where a data breach was conducted by a data company, media, or an individual, rather than a government.³⁸ In *Roe v. Wade*, the Supreme Court of the US held that the right of privacy is "founded in the Fourteenth Amendment's Concept of personal liberty and restrictions on state action."³⁹ Other cases have been less deferential to information privacy as a protectable civil liberty interest,⁴⁰ and the right remains uncertain.⁴¹

²⁸GDPR, *supra* note 18, at art. 1.2; see Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1(1), 1995 O.J. (L 281) 31 [hereinafter EU Data Protection Directive].

²⁹Schwartz & Peifer, *supra* note 25, at 123.

³⁰David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 ICON 220, 223 (2016).

³¹The European Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, became effective in 1953. For an official text, see Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

³²Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 1. The Charter is a constitutional document of the EU. Article 8.1 contains an explicit right to data protection, indicating: "[e]veryone has the right to the protection of personal data"

³³*Id.* art. 8(2).

³⁴Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU].

³⁵Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890).

³⁶US Privacy Act, 5 U.S.C. § 552 (2018); Alan Charles Raul, Tasha D. Manoranjan & Vivek Mohan, *United States, in THE PRIVACY, DATA PROTECTION, AND CYBERSECURITY LAW REVIEW* 268, 269 (Alan Charles Raul ed., 2014).

³⁷U.S. CONST. amend. IV.

³⁸Dan Swinhoe, *The Biggest Data Breach Fines, Penalties and Settlements So Far*, CSO (Jan. 31, 2020, 4:28 AM), <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>.

³⁹*Roe v. Wade*, 410 U.S. 113, 153 (1973). In *Whalen v. Roe*, although the Supreme Court of the United States identified a general right to "information privacy" in the Fourteenth Amendment, the Court upheld a New York statute requiring identification of physicians and patients in dangerous legitimate drug prescription records. 429 U.S. 589, 605–06 (1977).

⁴⁰Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 789, 791 (D.C. Cir. 1997) (expressing "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information . . .").

⁴¹Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 574–82 (1995); Schwartz & Peifer, *supra* note 25, at 133.

In contrast, the Constitution of the US firmly establishes the free flow of information by the First Amendment's free speech clause,⁴² which may be more likely to be considered as a fundamental human right in the US.⁴³ For example, *Sorrell v. IMS Health Care* is concerned with a Vermont law that prohibits pharmacies from disclosing or otherwise allowing prescriber-identifying information to be used for marketing.⁴⁴ The Supreme Court of the US held that this law should be subject to heightened judicial scrutiny because it was "content- and speaker-based" and "burden[ed] disfavored speech by disfavored speakers."⁴⁵ Vermont contended that its law was necessary to protect medical privacy.⁴⁶ The Court rejected this argument because this law allowed pharmacies to share prescriber-identifying information with anyone for any reason except for marketing.⁴⁷ The state also contended that this law advanced important public policy goals by lowering the costs of medical services and promoting public health. The Court held that while these policy goals may be proper, the law did not advance them in a permissible way.⁴⁸ The Court concluded that "the 'fear that people would make bad decisions if given truthful information' cannot justify content-based burdens on speech."⁴⁹ The law was set aside because it violated the First Amendment.⁵⁰

In China, the right to personal data is considered a personality right. There are two reasons. First, unlike the EU, Chinese legislators do not consider the right to personal information a fundamental human right. This is not because they cherish the free flow of information like the US. Instead, an individual's right to personal information should be limited because it should not interfere with the authority of the Chinese government, as the largest data controller, to collect, process, save, and use personal information.⁵¹ It may be true that in highly decentralized distributed systems established in a democratic society, "there is no central controller of information" and "almost everyone connected to the network is a 'controller' of personal data."⁵² However, this statement does not describe the Chinese situation. Although the Internet is decentralized, the Chinese government is still the ultimate controller because it controls the Internet connections between its territory and the outside world.⁵³ For example, China has built an Internet Great Fire Wall to censor the information flow across its border and prosecuted people who used or provided VPNs.⁵⁴ The Chinese government controls and accesses personal data of users of Chinese Internet service providers, such as Wechat.⁵⁵ Although the Chinese Constitution limits government access to Chinese citizens' correspondence to the circumstances of national security

⁴²44 *Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 503, 116 S. Ct. 1459 (Opinion of Stevens, J.) ("The First Amendment directs us to be especially sceptical of regulations that seek to keep people in the dark for what the government perceives to be their own good.").

⁴³*Schwartz & Peifer, supra note 25*, at 134; Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CALIF. L. REV. 751, 758, 770 (1999) (arguing that "Americans are more likely to cherish the principles embodied in the First Amendment—which favors a free flow of information—as fundamental human rights.").

⁴⁴*Sorrell v. IMS Health Care*, 564 U.S. 552, 561 (2011). The law is the Vermont Prescription Confidentiality Law. VT. STAT. ANN. tit. 18, § 4631 (West 2007).

⁴⁵*Sorrell*, 564 U.S. at 565.

⁴⁶*Id.* at 572.

⁴⁷*Id.*

⁴⁸*Id.* at 577.

⁴⁹*Id.*

⁵⁰*Id.* at 580.

⁵¹Zhang Xinbao, *From Privacy to Personal Information: The Theory and System to Re-balance Interest*, 3 *ZHONGGUO FAXUE* (CHINA LEGAL SCI.) 38, 39 (2015).

⁵²Samuelson, *supra note 43*, at 761.

⁵³Samuel Woodhams, *The Rise of Internet Sovereignty and the End of the World Wide Web?*, *GLOBE POST* (Apr. 23, 2019), <https://theglobepost.com/2019/04/23/internet-sovereignty/>.

⁵⁴Benjamin Haas, *Man in China sentenced to five years' jail for running VPN*, *GUARDIAN* (Dec. 21, 2017, 11:59 PM), <https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn>.

⁵⁵*WeChat Shares Consumer Data with Chinese Government*, *PYMNTS* (Sept. 25, 2017), <https://www.pymnts.com/safety-and-security/2017/wechat-hands-over-user-data-to-chinese-government-amid-privacy-concerns/>.

and criminal investigations,⁵⁶ other Chinese laws have gone beyond this constitutional limit. For example, Article 25 of the Chinese Ecommerce Law allows government departments to require e-commerce operators to provide e-commerce data—which includes personal information, privacy, and business secrets—according to provisions of laws and administrative regulations, and the ecommerce operators shall provide this information as required.⁵⁷ E-commerce Law does not provide any grounds or remedy for e-commerce operators to reject the government information request.

Second, the Chinese Constitution provides very limited protection for an individual's right to personal information. The Constitution provides that the residence of Chinese citizens is inviolable, and that freedom and privacy of correspondence of Chinese citizens are protected by law.⁵⁸ These provisions have limited implications on personal data protection in China. Literally speaking, these constitutional provisions are for residence and correspondence. Personal data protection concerns far more information than an individual's address and other contact information. It is unclear whether these constitutional provisions can cover all other personal data. More importantly, these constitutional provisions are about protecting privacy; however, in China, protecting personal data is not the same as protecting privacy. The General Rules of the Civil Law, a fundamental law for civil rights and obligations in China, was enacted in 2017.⁵⁹ It prescribes privacy and personal data protection in different articles. Article 110 provides that “natural persons have the right to life, body, health, name, portrait, reputation, honour, privacy, marriage autonomy and others.”⁶⁰ Article 111 indicates that:

[T]he personal information of natural persons is protected by law. Any organization or individual who needs to obtain personal information of others shall obtain and ensure the security of the information according to law, and shall not illegally collect, use, process, or transmit the personal information of others, and may not illegally buy, sell, or disclose the personal information of others.⁶¹

There are two opinions regarding the relationship between Article 110 and Article 111. The first is that Article 110 is *lex generalis* and Article 111 is *lex specialis*: Protecting personal information—Article 111—is to enhance the protection of privacy—Article 110—in the digital economy. The second opinion is that Article 111 is not *lex specialis*, as opposed to Article 110, because personal information is different from privacy. This second opinion is endorsed by the recently enacted Chinese Civil Code.⁶² Enacted on May 28, 2020, this unprecedented Civil Code is considered a significant milestone of the rule of law and a profound symbol of the prosperity of China.⁶³ Article 1032 of the Chinese Civil Code defines privacy as “the tranquility of the private life of a natural person, and the private space, private activities, and private information that he is

⁵⁶XIANFA art. 40 (1982) (China).

⁵⁷Dianzi Shangwu Fa [Chinese E-commerce Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 31, 2018, effective Jan. 1, 2019), art. 25, <https://npcobserver.com/legislation/e-commerce-law/>.

⁵⁸XIANFA art. 40 (1982) arts. 39–40.

⁵⁹General Rules of the Civil Law of China, *supra* note 20.

⁶⁰*Id.* art. 110.

⁶¹*Id.* art. 111.

⁶²Minfa Dian [Chinese Civil Code] (promulgated by the Thirteenth Nat'l People's Cong., May 28, 2020, effective Jan. 1, 2021), <http://www.npc.gov.cn/npc/c30834/202005/1247ca1d376e47e9b02a3053dd438e2d.shtml> [hereinafter Proposed Chinese Civil Code]. The Chinese Civil Code will replace all existing laws concerning civil law issues, including the General Rules of the Civil Law of China, *supra* note 20. However, the Chinese Civil Code will be effective on January 1, 2021, so it is not applicable to the COVID-19 pandemic in 2020.

⁶³See *China National People's Congress and National Political Consultative Conference's Notes on the "Civil Code of the People's Republic of China (Draft)"*, XINHUANET (May 22, 2020, 9:47 PM), http://www.xinhuanet.com/politics/2020lh/2020-05/22/c_1126021017.htm; *Civil Code Annotates China's New Territories*, NAT'L PEOPLE'S CONG. CHINA (May 24, 2020, 8:52 AM), <http://www.npc.gov.cn/npc/c30834/202005/8c3340275e6b4d418721ed5f8b015c09.shtml>.

unwilling to be known to others”; and Article 1033 provides that the right to privacy should be protected as *erga omnes*.⁶⁴ Articles 111 and 1034–37 address personal data, but, focus on collection and processing of personal data according to principles of legality, proportionality, and necessity.⁶⁵ Namely, the provisions for privacy focus on non-instruction of privacy, while those for personal data highlight how to legally use personal data. Therefore, the right to privacy and the right to personal data are distinguishable.

The second opinion has also gained wide support from Chinese scholars.⁶⁶ Their arguments can be summarized as follows.⁶⁷ First, privacy focuses on protection of *an individual’s personal information*.⁶⁸ In contrast, personal data protection in the digital economy emphasizes protection of *personal data of a collective of individuals*.⁶⁹ This is because the digital economy relies on big data, which requires a collective of individuals’ information rather than on an individual’s information.⁷⁰ Second, being a protector is the main role for a state regarding an individual’s privacy. In contrast, big data of personal information is a valuable resource for a state to develop its digital economy, maintain social stability, and safeguard national security.⁷¹ Therefore, a state not only protects personal data but also has an interest in accessing, collecting, and analyzing personal information.⁷² Third, data collectors—for example, data companies—contribute to the value of personal information, because if personal data is not collected and processed, it has no value.⁷³ In contrast, the right to privacy is against collecting and processing, and its value lies in “being left alone.”⁷⁴ As a conclusion, personal data protection is not an absolute right like privacy or property ownership, and its protection is comparatively weaker.⁷⁵

Distinguishing personal data from privacy can also find support in other Chinese legislation and judicial practice. For example, the Provisions of the Supreme People’s Court on Several Issues about Applicable Law in Civil Cases of Using Information Network to Infringe Personal Rights and Interests (SPC Provisions on Applicable Law for Personal Rights Infringement) also suggest that not all personal data can be considered as privacy.⁷⁶ Article 12.1 provides that Internet users or network service providers shall not use the Internet to disclose personal privacy *and other*

⁶⁴*Id.* art. 1033 provides limited exceptions—for example, circumstances prescribed by law and consented by a right holder—to intrusion of privacy.

⁶⁵*Id.* arts. 111, 1034–37. Article 1034 provides that private information in personal data shall be governed by the provisions on privacy right. Where there are no provisions, the provisions on the protection of personal information shall apply. The Civil Code does not specify the type of personal data that should be considered as private information.

⁶⁶E.g., Mei Xiaying, *The Legal Properties of Data and the Position of Data in Civil Law*, 9 ZHONGGUO SHEHUI KEXUE (CHINA SOC. SCI.) 164, 175 (2016).

⁶⁷Xinbao, *supra* note 51, at 45–49.

⁶⁸Liming Wang, *Lun Geren Xinxi Quan de Falv Baofu—Yi Geren Xinxi Quan yu Yinsi Quan de Jiefen wei Zhongxin (Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy)*, 35 XIANDAI FAXUE (MOD. L. SCI.) 62, 66 (2013).

⁶⁹Jianhua Xiao & Fangmo Chai, *An Analysis of Data Rights and Transaction Regulation*, 1 ZHONGGUO GAOXIAO SHEHUI KEXUE (SOC. SCI. CHINESE U.) 83, 86–87 (2019).

⁷⁰*Id.*

⁷¹Weiguan Wu, *Da Shuju Jishu xia Geren Shuju Xinxi Siqian Baohu Lun Pinpan (Critique of Personal Data Information Privacy Protection under Big Data Technology)*, 7 ZHENGZHI YU FALV (POL. & L.) 116, 129–31 (2016).

⁷²*Id.*

⁷³Bo Cao, *On Competition and Interoperation of Responsibility Rules and Property Rules in Personal Information Protection [Lun Geren Xinxi Baohu zhong Zeren Guize yu Caichan Guize de Jingzheng ji Xietiao]*, 5 HUAN QIU FALV PINLUN (GLOBAL L. REV.) 86, 100 (2018).

⁷⁴Wang, *supra* note 68, at 66–67.

⁷⁵Cheng Xiao, *Da Shuju Shidai de Geren Xingxi Quan Baofu (Personal Data Rights in the Era of Big Data)*, 3 ZHONGGUO SHEHUI KEXUE (CHINA SOC. SCI.) 102, 115–16 (2018).

⁷⁶Zuigao Remin Fayuan Guanyu Shengli Liyong Xingxi Wangluo Qinghai Renshen Quanyi Minshi Jiufeng Anjian Shiyong Falv Luogang Wenti de Guiding [Provisions of Supreme People’s Court on Several Issues about Applicable Law in Civil Cases of Using Information Network to Infringe Personal Rights and Interests] (promulgated by Supreme People’s Court, Aug. 21, 2014, effective Oct. 10, 2014), 2014 FA SHI no. 10 (China) [hereinafter SPC Provisions on Applicable Law for Personal Rights Infringement].

personal information.⁷⁷ Article 87 of the E-commerce Law also provides that “if a State functionary . . . sells or illegally provides others with *the personal information*, privacy and trade secrets that come to his knowledge in the performance of his duties, he shall be subject to legal liability according to law.” If personal data were to be equal to privacy, the italicized part of this provision would be redundant.

Ye Zhu v. Baidu, the first case on privacy protection concerning cookie technology,⁷⁸ sheds light on the differences between privacy and personal data.⁷⁹ Baidu.com—China’s largest Internet search engine—employs Cookie technology to record and track the search keywords used by a customer, and provide tailor-made advertisements for this customer.⁸⁰ Zhu alleged that Baidu.com invaded her privacy; Baidu, without her permission, recorded keywords she searched, such as “breast enhancement,” “weight loss,” and “abortion,” and used these keywords to provide advertisements to her. Baidu argued that Cookie technology was a lawful, basic, and neutral technology, and had been used by Google, Yahoo, Amazon, and other Internet service providers. Further, the Cookies collected by Baidu did not include any identifiable personal information—that is, as a search provider, Baidu would not be able to locate a specific individual who used its service. The advertisement relating to the search keywords that Zhu used appeared only on Zhu’s computer and was not published by Baidu to other parties. Baidu, therefore, contended that it did not infringe on Zhu’s privacy. The Nanjing Intermediate People’s Court, as the appellate court, agreed with Baidu and held that there was no invasion of privacy for three primary reasons. First, the information collected by Baidu was not personal because it could not identify Zhu. Cookie technology identified a particular browser rather than a certain user. Thus, when the same user used a different browser to search the Internet, Baidu identified this user as a different user. Second, Baidu did not publish Zhu’s personal information because Cookie technology conducted machine-to-machine communication rather than machine to human. Third, the Baidu user’s agreement allowed users to freely opt out of using Cookies. However, Zhu did not do so. The court also held that Cookie technology was widely used, and even if the Baidu user’s agreement did not explain what Cookies were, an average person—like Zhu—should be assumed to understand this technology.

Ye Zhu helps us to understand how Chinese courts distinguish privacy from personal information. The court held that the records of keyword searches of an Internet user could reflect the user’s activity history and Internet browsing preferences, so they were considered to be privacy attributes. However, if separated from the data subject, they could not identify the data subject, so they were not personal data. The court seems to suggest that if a piece of privacy information, used individually, cannot identify a data subject, this privacy information is not a piece of personal information. This is so even if the relevant piece of privacy information, combined with other information collected by a website, may be able to identify a data subject. For example, searching “weight loss” is an activity conducted by Zhu. Zhu does not want others to know of this activity, which should be considered as her privacy. However, “weight loss,” as a searched keyword, is not personally related to Zhu and cannot identify Zhu. Therefore, keyword searches are not personal data. Yet, the court does not consider whether Baidu may have collected other information from

⁷⁷*Id.* art. 12.1.

⁷⁸Sherry Gong & Nolan Shaw, *Chinese Appellate Court Provides Guidance for Lawful Use of Cookies*, HOGAN LOVELLS (Aug. 3, 2015), <https://www.hldataprotection.com/2015/08/articles/international-eu-privacy/chinese-appellate-court-provides-guidance-for-lawful-use-of-cookies/>.

⁷⁹Beijing Baidu Wangxun Keji Youxian Gongsu yu Bei Shangsu Ren Zhu Ye Yingsi Quan Jiufeng An [*Ye Zhu v. Baidu*], 2014 NING MIN ZONG ZI no. 5028 (Nanjing Interm. People’s Ct. 2014) (China).

⁸⁰This case relates to the usage of cookies, a widely used Internet technology. When an Internet user uses a browser to conduct searches on Baidu.com, cookie information automatically sent by Baidu will be saved on the user’s browser. Through the connection established by the cookie, Baidu is able to identify the browser and predict the user’s interest, and thus provide tailor-made advertisements.

Zhu, such as her location or her search habits. The court improperly ignores that the accumulated information may be combined to identify Zhu.

There are three different definitions of personal data co-existing in Chinese law. The first is provided in the Provisions on the Protection of Personal information of Telecommunications and Internet Users (Provisions), enacted by the China Ministry of Industry and Information Technology in September 2013. Article 4 defines a “user’s personal data” as “(1) the user name, date of birth, ID number, address, telephone number, account number, and password that can be used alone or in combination with other information to identify an individual user, and; (2) the time, place, and the like of the user’s use of the service.” Article 4 does not require “the time, place, and the like of the user’s use of the service” to identify an individual user. Nevertheless, the *Ye Zhu* court dismissed the application of Article 4 without a clear reason.

The second definition of personal data can be found in Article 67(5) of the Chinese Cybersecurity Law. It provides that personal data refers to various information—recorded by electronic or other means—that can be used alone or in combination with other information to identify an individual natural person, including but not limited to the person’s name, birthday, personal identification number, biometric information, address, and phone number. The Chinese Cybersecurity Law was enacted by the Standing Committee of National People’s Congress and came into effect in June 2017. This was after *Ye Zhu* was decided. The definition of personal data in *Ye Zhu* is inconsistent with the Chinese Cybersecurity Law, as personal data is the information, alone or jointly with other information, that can be used to identify a data subject.

The third definition can be found in the Information Security Technology—Personal Information Security Specification (Personal Information Security Specification), made jointly by the State Administration of Quality Supervision, Inspection and Quarantine, and the China National Standardization Administration.⁸¹ It came into effect in May 2018. Article 3.1 defines “personal data as various information recorded electronically or otherwise that can identify a particular natural person or reflect the activity of a particular natural person, either alone or in combination with other information.” This definition does not limit personal data to those pieces of information able to identify a particular natural person.

Among the three definitions, the one provided by the Chinese Cybersecurity Law is the most authoritative. The Chinese Cybersecurity Law was enacted by the Standing Committee of National People’s Congress, which retains more stature and influence compared with the bodies that enacted the other two regulations. The Chinese Cybersecurity Law is also a more recent piece of legislation compared with the Provisions. The Personal Information Security Specification was made later in time compared with the Chinese Cybersecurity Law. But the Personal Information Security Specification is not a law. It serves as guidance of best practices for the industry. Its foreword provides that, if these Specifications contradict with law, the latter should prevail. Therefore, the definition under the Cybersecurity Law—which requires that personal information, alone and in combination with other information, should be able to identify a particular natural person—represents the prevailing view in China.

II. Consumer Right

The US law considers that the data subject’s personal information may be used to exchange for Internet service—as opposed to the EU, where personal data is a fundamental right which cannot be traded.⁸² At the state level, for example, the California Consumer Privacy Act of 2018 explicitly

⁸¹STATE ADMIN. OF QUALITY SUPERVISION, INSPECTION & QUARANTINE & CHINA NAT’L STANDARDIZATION ADMIN., INFORMATION SECURITY TECHNOLOGY—PERSONAL INFORMATION SECURITY SPECIFICATION (GB/T 25069-2010) (2018). The State Administration of Quality Supervision, Inspection and Quarantine is a government agency in China.

⁸²WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORK WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 5 (2012), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf> (“[P]ersonal data fuels an advertising marketplace that brings many online services and sources

provides that “it is the intent of the Legislature to further Californian’s right to privacy by giving consumers an effective way to control their personal information.”⁸³ Satisfying requirements under the law, a business can offer financial incentives to consumers for the collection and sale of their personal data.⁸⁴ At the federal level, the primary privacy enforcement agency is the Federal Trade Commission, whose jurisdiction is limited to regulate privacy violations by organizations who conduct “deceptive” or “unfair” information practices.⁸⁵ Therefore, commentators conclude that the US Privacy Act is a system of broad consumer protection laws that have “been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.”⁸⁶

Like the US, in China, consumer law also allows personal information to be traded.⁸⁷ Chinese consumer law requires data companies to clearly indicate the purpose, manner, and scope of the collection and use of information, and seek the consent of the consumers.⁸⁸ The personal information collected by the data companies must be kept strictly confidential and not be disclosed, sold, or illegally provided to others.⁸⁹ Chinese consumer law also offers explicit remedies for personal data breaches. For example, Article 50 provides that if a business operator infringes upon the consumer’s personal data, the operator shall stop the infringement, restore the reputation, eliminate the influence, apologize, and compensate the loss. Article 56 also indicates that in cases where business operators infringe upon consumers’ personal information, the Administrative Department for Industry and Commerce or other relevant administrative departments shall order corrections, and may—according to the circumstances of the case—impose warnings, confiscate illegal income, and levy fines.⁹⁰ If the circumstances are serious, the operator shall be ordered to suspend business for rectification and revoke the business license.⁹¹

However, the difference between Chinese consumer law and its US counterpart is that the former is much more ambiguous than the latter regarding the competence, necessity, and proportionality to collect personal data. For example, in November 2019, a Chinese professor brought a case against Hangzhou Safari Park in the Hangzhou Huyang District People’s Court.⁹² The professor alleges that the Safari Park would like to mandatorily collect his facial features without his consent.⁹³ The professor bought an annual pass for the Safari Park for the period of April 2019 to April 2020.⁹⁴ In October 2019, without asking the professor’s consent, the Park informed him that

of content to consumers for free.”). Sally Chapman, *Consumer Data Privacy in a Networked World*, HOMELAND SECURITY DIGITAL LIBRARY: ON THE HOMEFRONT BLOG (Feb. 23, 2012), <https://www.hsdl.org/c/consumer-data-privacy-in-a-networked-world/>.

⁸³CCPA at § 2(i). The rights include: (1) The right of Californians to know what personal information is being collected about them; (2) the right of Californians to know whether their personal information is sold or disclosed and to whom; (3) the right of Californians to say no to the sale of personal information; (4) the right of Californians to access their personal information; and (5) the right of Californians to equal service and price, even if they exercise their privacy rights.

⁸⁴*Id.* § 1798.125(b).

⁸⁵Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2018).

⁸⁶Shawn Marie Boyne, *Data Protection in the United States*, 66 AM. J. COMP. L. 299, 301 (2018); Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. L. (July 1, 2016), <https://content.next.westlaw.com/6-502-0467?transition%Type=Default&contextData=>.

⁸⁷Xiaoheizhe Quanyi Baofu Fa [Chinese Consumer Law] (promulgated by the Standing Comm. Nat’l People’s Cong., Oct. 31, 1993, last amended Oct. 25, 2013), art. 29, http://www.gov.cn/flfg/2013-10/25/content_2516547.htm.

⁸⁸*Id.*

⁸⁹*Id.*

⁹⁰*Id.* art. 56.

⁹¹*Id.* Article 56 also provides that, except for the corresponding civil liability, if other relevant laws and regulations have provisions on which government departments should take punishment measures and which measures should be taken, they shall be implemented in accordance with the provisions of the laws and regulations.

⁹²Beijing Youth Daily, *The First Facial Recognition Case in China, A Zoo in Hangzhou is Sued*, XINHUANET (Nov. 4, 2019, 8:35 AM), http://www.xinhuanet.com/legal/2019-11/04/c_1125188289.htm.

⁹³*Id.*

⁹⁴*Id.*

the annual pass system was updated and the old system was abolished; now, visitors must record their facial features at the Park, and the Park will use a facial recognition system to verify visitors' identities.⁹⁵ If a visitor refuses to record his or her facial features, the annual pass cannot be used, and a refund will not be issued.⁹⁶ The Park explains that using the facial recognition system will speed up the Park admission process and save consumers' waiting time.⁹⁷ What is stunning in this case is that the only way for the safari park to provide admission is to collect and use facial features of customers. Facial features are personal biometric information. They are with the natural person for his or her lifetime and cannot be changed. Facial features are more sensitive than fingerprints and other personal data because they are mostly exposed. For public safety and national security, government law enforcement departments, such as the border control and traffic regulation department, can collect this information. Hangzhou Safari Park is not a government department and collects facial features for commercial purposes. Even if it can ensure the collected information will be well protected, saving consumers' waiting time cannot justify the necessity and proportionality to collect such information. This case shows that while Chinese facial recognition technology is widely used, the law to regulate the competence, necessity, and proportionality to collect personal data is insufficient.

III. Property Right

Characterizing personal data as “property” derives from scientific research on the physical reality of information.⁹⁸ It reflects the need to delimit the ownership of data within the booming digital trade where personal data is treated as a product.⁹⁹ It is also appealing for data controllers to claim independent or shared property rights with the data subjects, especially when the controllers process information that is generated by machines based on anonymized personal data.¹⁰⁰

In 1905, the Supreme Court of the US held that data can be considered as property.¹⁰¹ Moreover, the modern digital trade in transferring, licensing, and selling personal data has further fostered the view that personal data should be characterized as property.¹⁰² Property scholars argue that “[p]roperty rights in information focus on identifying the right of a company or individual to control disclosure, use, alternation and copying of designated information.”¹⁰³ In China, the People's Court Daily positively reported a judgment issued by the Hangzhou Internet Court in November 2019.¹⁰⁴ In this case, the plaintiffs operated an online database called Lvzhuang Wang, or “female clothing net.” The defendant manages a competing online database called Zhongfu

⁹⁵*Id.*

⁹⁶*Id.*

⁹⁷*Id.*

⁹⁸Rolf Landauer, *Information is Physical*, 44 PHYSICS TODAY 23–29 (1991).

⁹⁹Kenneth C. Laudon, *Markets and Privacy*, 39 COMM. ACM 92 (1996) (proposing property rights in personal data as a way to protect privacy).

¹⁰⁰For example, this includes non-personal data or value-added data created by data companies from basic data collected from data subjects.

¹⁰¹*Bd. of Trade of Chicago v. Christie Grain & Stock Co.*, 198 U.S. 236, 251 (1905) (“If, then, the plaintiff's collection of information is otherwise entitled to protection, it does not cease to be so, even if it is information concerning illegal acts. The statistics of crime are property to the same extent as any other statistic, even if collected by a criminal who furnishes some of the data.”).

¹⁰²Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, DUKE L. TECHNOL. REV. 220, 221 (2017).

¹⁰³Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INT'L J.L. & INFO. TECH. 3, 5–7 (1993); see Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1 (2011) (arguing that individuals should have an “enforceable property right” over their own personal information).

¹⁰⁴*One Company in Zhejiang Is Ordered to Pay 350,000 RMB in a Judgment*, PEOPLE'S COURT NEWS (Nov. 5, 2019), http://rmfyb.chinacourt.org/paper/html/2019-11/05/content_161872.htm?div=-1; *Use the “Crash Library” to Log In to Peer Websites Thousands of Times to Obtain Information*, ZHEJIANG LEGAL NEWS (Nov. 11, 2019, 10:09 AM), http://www.zjsfgkw.cn/art/2019/11/1/art_56_18812.html.

Wang, or “China clothing net.” Many users who registered with the plaintiffs also registered with the defendant. Twenty-four users of the defendant’s database authorized the defendant’s staff to use their IDs and passwords to access their accounts on the defendant’s website. Because many users may use the same IDs and passwords on different websites, the defendant’s staff used the “crashing the library” technology to log into the twenty-four users’ accounts on the plaintiff’s website.¹⁰⁵ Consequently, the defendant downloaded information valuable to clothing dealers from the plaintiffs’ website. The plaintiffs brought an unfair competition claim against the defendant. The defendant argued that the plaintiffs’ user agreement did not specify who was the owner of the users’ IDs and passwords; even if the defendant misused the users’ IDs and passwords, it should be the users, not the plaintiffs, to claim the right to the users’ IDs and passwords. The court rejected this argument, holding that the users’ IDs and passwords were property and should be protected. Furthermore, the court held that the IDs and passwords were highly correlated with the users’ identity authentication, and the property right generated by this information was like that of computer information system data, so the rights of the users’ IDs and passwords should belong to the website—in this case, the plaintiffs.

The property right argument is deeply problematic. In the above case, it is doubtful that a data controller can obtain absolute property rights over data collected from data subjects. This is because the data controller has to use personal data strictly according to the agreements with the data subjects. Moreover, the data controller does not exclusively possess personal data. Data subjects can provide the same piece of personal data to other data controllers. Nevertheless, the data controllers invest time, money, and energy in compiling, organizing, or processing personal data. Alternatively, personal data may be generated while data subjects use the Internet service provided by the data controllers. Therefore, the data controllers have legitimate interests in the personal data they collect. However, this legitimate interest is not a property interest in personal data. Rather, it is a property interest that lies with the data controller, who invested in the process of gathering personal data under the guise that they would not be taken advantage of by other competing data controllers.

Further, in the American context, the property right theory is criticized because there are strong policy reasons, such as First Amendment civil liberty, against marking all personal information as property.¹⁰⁶ However, in China, the property right argument is doomed to fail for a reason not existing in the American context. The property right argument can enhance every data subject’s right of self-determination and control of his or her data. Yet, such self-determination and control are inconsistent with the Chinese government’s digital surveillance measures that rely on gathering a huge amount of personal data.¹⁰⁷ These data are collected under an over-comprehensive concept of national security without proper judicial review and public transparency supervision. Although the Chinese Civil Code provides that the collection and processing of personal information is subject to the principles of legality, proportionality, and necessity,¹⁰⁸ there are not many genuine opportunities for Chinese consumers to say no and find convenient alternatives for many basic services in China. For example, Chinese consumers are required to use facial recognition as a

¹⁰⁵“Crashing the library” means that the hacker generates the corresponding dictionary table by collecting the account and password information that has been leaked on the Internet, and tries to log in to other websites in batches to obtain a series of users’ accounts that can be accessed. Many users use the same account password on different websites, so the hacker can try to log in to Website B by obtaining the user’s account on Website A.

¹⁰⁶See, e.g., Pamela Samuelson, *Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?* 38 CATH. U.L. REV. 365, 366 (1988).

¹⁰⁷See PAUL M. SCHWARTZ & JOEL R. REIDENBERG, *DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION* 39 (1996) (arguing gathering personal data “to weaken the individual capacity for critical reflection and to repress any social movements outside their control”).

¹⁰⁸Proposed Chinese Civil Code at art. 1035.

precondition to receive mobile phone and banking services in China.¹⁰⁹ There is no alternative for them except providing their facial features. If there is no genuine consent, how can the legality of collecting facial biometric information be decided? If consumers do not know what facial information is collected, how to process it, and where to store it, it is hard to determine proportionality. Moreover, the most common justification for granting property rights is to enable efficient and effective allocations of scarce resources. This does not seem to apply to facial biometric information or personal data, because in digital society, “[w]hat is scarce is information privacy, not personal data.”¹¹⁰ Therefore, the rhetoric of property law is also inconsistent with the right to personal data as a personality right in China.

The limitation of applying property law to personal data raises the question whether personal data can be considered as a copyright in the context of intellectual property protection? Personal data may not satisfy the threshold in becoming an original work, trademark, or patent.¹¹¹ For example, “female” as a gender is an important piece of personal information for an individual but cannot be regarded as an original and creative work under the copyright law.¹¹² In *Shanghai Hantao Information Consultation Co. v. Aibang Juxin (Beijing) Technology Co.*, the No. 1 Intermediate People’s Court in Beijing held that if a comment provided by an individual customer expresses his or her original thoughts, character, emotions, and experiences, this comment would be considered as a work under the Chinese Copyright law. However, the plaintiff in this case failed to prove that every comment on its platform satisfied the originality and creativity requirement under the Chinese Copyright Law.¹¹³ *Shanghai Hantao Information Consultation Co.* is like *Feist Publ’ns, Inc. v. Rural Telephone Serv. Co.*, where the Supreme Court of the US also concluded that it is difficult to justify copyright protection unless sufficient creativity exists in the development of databases of factual information.¹¹⁴

C. Spread-Out Unilateral Applicable Law Approach

The second stage of conflict-of-laws analysis involves identifying connecting factors. The US, EU, and China either adopt connecting factors leading to the law of the forum or consider their data protection laws as mandatory law. Consequently, they predominantly apply *lex fori* to data disputes in torts, contracts, and equity, with little consideration of the conflicting foreign laws that transnational personal data may involve.

I. Lex Fori Based on Connecting Factors and Mandatory Law of the Forum

2019 has witnessed numerous seminars on topics such as “GDPR 18 Months On: Insights on Enforcement and Compliance for Non-EU Agencies” and the like.¹¹⁵ The connecting factors adopted by the EU GDPR go beyond the traditional ones for natural persons, such as habitual residence or active citizenship. Article 3.2 of the GDPR provides that it applies to the offering of free or paid goods or services to the data subject who is in the EU.¹¹⁶ This condition is fulfilled

¹⁰⁹China Due to Introduce Face Scans for Mobile Users, BBC (Dec. 1, 2019), <https://www.bbc.com/news/world-asia-china-50587098>; Meng Jing, *From Travel and Retail to Banking, China’s Facial Recognition Systems are Becoming Part of Daily Life*, SOUTH CHINA MORNING POST (Feb. 8, 2018, 6:00 AM), <https://www.scmp.com/tech/social-gadgets/article/2132465/travel-and-retail-banking-chinas-facial-recognition-systems-are>.

¹¹⁰Samuelson, *supra* note 43, at 1138.

¹¹¹E.g., Gianclaudio Malgieri, “Ownership” of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, 20 J. INTERNET L. 3, 3–6 (2016).

¹¹²*Id.*

¹¹³Shanghai Hantao Information Consultation Co. v. Aibang Juxin (Beijing) Technology Co., 2010 HAI MIN CHU ZI no. 4253 (Beijing Haidian People’s Ct. 2010) (China).

¹¹⁴*Feist Publ’ns, Inc. v. Rural Telephone Serv. Co.*, 499 U.S. 340, 363 (1991).

¹¹⁵For example, a panel discussion happened at the IAPP ANZ Summit 2019, which was held on October 29–30 in Sydney, Australia.

¹¹⁶GDPR, *supra* note 18, at art. 3.2.

if the controller or processor envisages offering goods or services to data subjects in the EU, such as using a language or currency generally used in one or more EU member states, or targeting EU customers.¹¹⁷ The GDPR also applies if the data subject's behavior is monitored, so far as their behavior takes place in the EU.¹¹⁸ This broad territorial scope enables the GDPR to be applied as a mandatory law to a large number of data subjects who are non-EU residents or citizens.¹¹⁹

In the US, data protection law also has a broad territorial scope. A foreign business that collects, holds, transmits, processes, or shares a US resident's personal information is subject to US federal data protection laws and may also be subject to relevant state-based laws in the state where the data subject resides.¹²⁰ The newly-enacted California Consumer Privacy Act applies to companies collecting personal information from California residents who satisfy at least one of three requirements, indicating the requisite nexus with California: (1) Having over \$25 million in annual gross revenue; (2) buying, receiving, selling, or sharing for commercial purposes the personal information of 50,000 or more Californian consumers, households, or devices; or (3) deriving 50 percent or more of their revenue from the sale of California consumers' personal information.¹²¹ Commentators have criticized that the thresholds of the nexuses are so low so as to cover not only big companies but also many small- and medium-sized businesses.¹²² Nevertheless, this low threshold ensures that more California resident consumers can benefit from the Consumer Privacy Act.

The Chinese Cyber Security Law provides for personal data protection.¹²³ Article 2 states that the construction, operation, maintenance, and use of networks, as well as the supervision and management of networks in China, shall be subject to this law.¹²⁴ The Provisions on Online Protection of Children's Personal Information provides that it shall apply to the collection, storage, use, transfer, disclosure, and other activities relating to children's personal information that are conducted online within the territory of China.¹²⁵ The Safety Assessment Guide for Data Transferred Outside of China, Draft for Public Comments in 2017, provides that it applies to a foreign data controller or processor that is not registered in China but provides products or services to people in China.¹²⁶ The factors to determine whether a foreign data controller or processor operates in China or provides products or services to people in China include, but are not limited to, advertising in Chinese, using Chinese currency, and providing logistics service to

¹¹⁷*Id.* at rec. 23.

¹¹⁸*Id.* at art. 3.2. Monitoring means tracking a natural person on the Internet—by using data processing techniques such as profiling—to analyse or predict her or his personal preferences, behaviors, and attitudes. *See id.* at rec. 24.

¹¹⁹PAUL VOIGT & AXEL VON DEM BUSSCHE, SCOPE OF APPLICATION OF THE GDPR 21–22 (Paul Voigt & Axel von dem Bussche eds., 2017).

¹²⁰Steven Chabinsky & F. Paul Pittman, *USA: Data Protection 2020*, ICLG (June 7, 2020), <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>; *Watson v. Employer Liability Corp.*, 348 U.S. 66, 72 (1954) (holding that a state “may regulate to protect interests of its own people, even though other phases of the same transactions might justify regulator legislation in other states”).

¹²¹CCPA at § 1798.140(c).

¹²²Brenda Stoltz, *A New California Privacy Law Could Affect Every U.S. Business—Will You Be Ready?*, FORBES (Sept. 7, 2019, 7:52 PM), <https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy-act-could-affect-your-business/>.

¹²³Zhonghua Renmin Gongheguo Wangluo Anquan Fa [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), arts. 41–44, CLL1.283838 (EN) (Lawinfochina) [hereinafter Chinese Cybersecurity Law].

¹²⁴*Id.* art. 2.

¹²⁵[Provisions on Online Protection of Children's Personal Information] (promulgated by the Cyberspace Admin., Aug. 22, 2019, effective Oct. 1, 2019), art. 3, <https://perma.cc/2RJZ-XN98>.

¹²⁶NAT'L INFO. SECURITY STANDARDIZATION TECH. COMM., SAFETY ASSESSMENT GUIDE FOR DATA TRANSFERRED OUTSIDE OF CHINA (SECOND DRAFT FOR PUBLIC COMMENTS) arts. 3.2, 3.6 (2017).

China.¹²⁷ The Safety Assessment Guide for Personal Data Transferred Outside of China, Draft for Public Comments in 2019, explicitly indicates that it applies to companies registered outside of China but collecting personal information of people in China via the Internet.¹²⁸ Like their US and EU counterparts, these connecting factors enable these Chinese data protection laws to cover a broad territorial scope.

Moreover, data protection laws may be considered as mandatory law and directly apply to foreign-related civil relations without the guidance from the conflict rules. In China, the connecting factor to determine the applicable law for the personality right is a person's habitual residence.¹²⁹ In 2012, the Supreme People's Court issued a judicial interpretation that defines mandatory law as "provisions of the laws and administrative regulations that involve the social public interest of China, that the parties concerned cannot exclude their application through an agreement, or that are directly applicable to foreign-related civil relations without the guidance from the conflict rules."¹³⁰ The judicial interpretation provides that the following situations are mandatory law: Involving the protection of the interests of labors; involving food or public health safety; involving environmental safety; involving financial safety such as foreign exchange administration; involving anti-monopoly or anti-dumping; or other situations that should be recognized as mandatory provisions.¹³¹ In the context of COVID-19, if a law for public health safety requires the releasing of personal information, this law should be applied because it is a mandatory law and consequently, foreign laws should be excluded. Applying this interpretation to the COVID19 case discussed in the first paragraph of this Article, although that lady's habitual residence is Australia, Australian law should not be applied because Chinese law for COVID-19 is a mandatory law. On February 4, 2020, the China Central Cyber Security and Informatization Commission issued a Notification on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control of Disease.¹³² Therefore, this Notification should be applied to international travelers whose habitual residences are not in China. Yet, if a law for personal information protection has nothing to do with protecting public health, the question arises whether this law is a mandatory law. The answer depends on whether this law involves the social public interest of China.¹³³ Personal data protection laws, such as the Chinese Cyber Security Law, The Provisions on Online Protection of Children's Personal Information, and Consumer Law, address the social public interest of China. Therefore, they should be considered as mandatory laws.

II. Curtailing Party Autonomy

The user's agreement between a data subject and a data controller is a consumer contract; so unsurprisingly, party autonomy regarding the law to protect personal data is usually restricted by the mandatory law discussed in Section I, *Lex Fori* Based on Connecting Factors and

¹²⁷*Id.* at Article 3.6 provides that "processing" means any operations involving personal information and important data, including collecting, saving, accessing, revising, transferring, publishing, anonymizing, de-labeling, retrieval, erasure, destruction, or other operations.

¹²⁸CYBERSPACE ADMIN., SAFETY ASSESSMENT GUIDE FOR PERSONAL DATA TRANSFERRED OUTSIDE OF CHINA (DRAFT FOR PUBLIC COMMENTS IN 2019) (2019).

¹²⁹[Law of the Application of Law for Foreign-related Civil Relations of China] (promulgated by the Eleventh Nat'l People's Cong., Oct. 28, 2010, effective Apr. 1, 2011), art. 15, <https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn173en.pdf>.

¹³⁰[Interpretation of the Supreme People's Court on Certain Issues Concerning the Application of the "Law of the People's Republic of China on the Application of Laws to Foreign-Related Civil Relations"] (promulgated by the Jud. Comm. Supreme People's Court, Dec. 28, 2012, effective July 1, 2013), 2012 FA SHI no. 24, art. 10, <http://cicc.court.gov.cn/html/1/219/199/201/679.html> [hereinafter Interpretation on the Law on the Application of Laws].

¹³¹*Id.*

¹³²CHINA CENTRAL CYBER SECURITY & INFORMATIZATION COMM'N, NOTIFICATION ON PROTECTING PERSONAL INFORMATION AND USING BIG DATA TO SUPPORT JOINT PREVENTION AND CONTROL OF DISEASE (2020) [hereinafter NOTIFICATION ON PROTECTING PERSONAL INFORMATION].

¹³³Interpretation on the Law on the Application of Laws, *supra* note 130, art. 10.

Mandatory Law of the Forum. The contract between a data controller and a processor is not a consumer contract. Yet, party autonomy for the applicable law is also restricted in the contract between the data controller and the processor.

In the EU, a data controller and a processor can conclude data-processing contracts.¹³⁴ However, parties are not allowed to use contractual choice of law clauses to diminish the personal data protection provided by the GDPR. This is for two reasons.

First, for the contractual relationship between a data controller and a data processor, if a controller or a processor is established in the EU, the GDPR applies to the processing of personal data in the context of its activities.¹³⁵ It does not matter whether the processing takes place in the EU or not.¹³⁶ The leading authority for defining “in the context of the activities of an establishment” is the *Weltimmo* case.¹³⁷ *Weltimmo* was registered in Slovakia¹³⁸ and managed a property dealing website concerning Hungarian properties. It had no registered office or branch in Hungary. However, the owner of *Weltimmo* lived in Hungary and the website was written exclusively in Hungarian. *Weltimmo* had also opened a bank account in Hungary for the recovery of its debts and had a letter box for everyday business affairs. It hired a representative in Hungary to negotiate the settlement of its unpaid debts with its advertisers. The Court of Justice of the EU (CJEU) held that “in the context of the activities of an establishment” should be broadly interpreted.¹³⁹ More specifically, the concept of “establishment” emphasizes the effective and real exercise of activity through stable arrangements. Within this construction, the legal form of such an establishment—for example, an entity with or without a legal personality—is not determinative.¹⁴⁰ The “establishment” extends to any real and effective activity based on the stable arrangements.¹⁴¹ Accordingly, the CJEU held that *Weltimmo* pursued a real and effective activity in Hungary. The Court further held that the operation of loading personal data on an Internet page should be considered to be “processing.”¹⁴² Therefore, Hungarian law should be applied to *Weltimmo*. Another leading authority is the *Google Spain* case.¹⁴³ In this case, the processing of the relevant personal data took place exclusively in California by Google US. Google Spain possessed a separate legal personality and provided support to the Google group’s advertising activity. The activity of Google Spain was separate from the search engine service in California. The CJEU held that Directive 95/46, the predecessor of the GDPR, should be applied as the processing of data in the US was carried out in the context of the activities of Google Spain. The activity of Google Spain was inextricably linked with the search service provided by Google US because without the advertising space, the search engine would not be economically profitable and may not be able to perform.¹⁴⁴

Second, there is a question of whether a data controller can disclose personal data to an overseas processor and contract for a law providing a lower standard of privacy protection than the law of the controller’s place of registration. The answer is negative in the EU. The personal information collected in the EU can be disclosed only to overseas processors located in a jurisdiction recognized by the EU as a jurisdiction that offers equivalent data protection laws. In the case of

¹³⁴GDPR, *supra* note 18, at rec. para. 40; EU Data Protection Directive, *supra* note 28, at art. 26.

¹³⁵GDPR, *supra* note 18, at art. 3.1.

¹³⁶*Id.*

¹³⁷Case C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639 (Oct. 1, 2015), <http://curia.europa.eu/juris/liste.jsf?num=C-230/14>.

¹³⁸*Weltimmo* did not carry out any activity in its place of registration and often changed its registered office from one state to another.

¹³⁹Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317 (May 13, 2014), para. 53, <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.

¹⁴⁰EU Data Protection Directive, *supra* note 28, at rec. 19 of the preamble; *Google Spain SL*, Case C-131/12 at para. 48.
¹⁴¹*Weltimmo*, Case C-230/14.

¹⁴²Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, ECLI:EU:C:2003:596 (Nov. 6, 2003), para. 25, <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01>; *Google Spain SL*, Case C-131/12 at para. 26.

¹⁴³*Google Spain SL*, Case C-131/12.

¹⁴⁴*Id.*

outsourcing to a country without equivalent data protection laws to the EU's laws, the GDPR requires the controller to apply adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.¹⁴⁵ Therefore, parties are not allowed to select a law providing a lower standard of protection. This conclusion is also supported by judicial practice. In the German case *Facebook v. Independent Data Protection Authority of Schleswig Holstein*,¹⁴⁶ the general terms and conditions of Facebook contained a clause according to which, for German users, German law applied. The German court pointed out that, according to the Rome I Regulation, it was in principle possible to make an agreement on applicable law for the contract but not on data protection law. This was on account of the provisions on data protection—falling within the concept of overriding mandatory provisions—within the meaning of Article 9 of the Rome I Regulation, making it impossible for the parties to make an agreement on applicable law in this regard.

Different from the EU, Chinese law does not generally limit party autonomy in the choice of applicable law for contracts between a data controller and a processor. However, Chinese law does not allow a data controller to disclose personal data of a child to an overseas processor and contract for a law providing a lower standard of privacy protection than Chinese law. The Provisions on Online Protection of Children's Personal Information provides that if a network operator transfers personal information of children to a third party, it shall conduct its own safety assessment, or engage an independent organization to conduct the same.¹⁴⁷ If a network operator entrusts a third party to process personal information of children, it should also conduct a security assessment of the entrusted party.¹⁴⁸ The entrustment contract between the network operator and the entrusted party shall provide that, among others, personal information of children shall be handled according to Chinese law and the entrusted party is not allowed to transfer the commission.¹⁴⁹

The purpose in restricting party autonomy in the contract between a data controller and a processor is to protect data subjects. There is often no direct contractual relationship between the data subject and the data processor, because the latter may not directly collect personal data from the former and, instead, the latter often obtains the data from a data controller. However, the right of the data subject against the data processor is derived from the contract between the data subject and the data controller. The contract between the data controller and the data processor should not impose any obligations on the data subject, and it should ensure that the data subject's information is well protected. Namely, the data subject is the third-party beneficiary of the contract between the data controller and the data processor. Restricting party autonomy in the contract between a data controller and a processor is consistent with the mandatory nature of personal information law to protect data subjects.

III. Applying *Lex Fori* in Equity Cases

Besides torts and contracts, a personal data breach may also be pursued as a breach of confidence claim in the UK and other commonwealth countries. The *lex fori* approach leads to the application of forum law—the same result as applying mandatory law and curtailing party autonomy discussed in previous sections. For example, in *Giller v. Procopets*, the Court of Appeal of the Supreme Court of Victoria in Australia awarded equitable compensation for “distress arising from

¹⁴⁵GDPR, *supra* note 18, at art. 46; EU Data Protection Directive, *supra* note 28, at art. 26.2.

¹⁴⁶Bundesverwaltungsgericht [BVerwG] [Federal Administrative Court] Feb. 25, 2016, 1 C 28.14, <https://www.bverwg.de/en/250216B1C28.14.0>. For a comment of the decision, see, for example, Carlo Piltz, Facebook Ireland Ltd. v. Independent Data Protection Authority of Schleswig-Holstein, Germany—*Facebook Is Not Subject to German Data Protection Law*, 3 INT'L DATA PRIVACY L. 210 (2013).

¹⁴⁷Provisions on Online Protection of Children's Personal Information, *supra* note 125, art. 17.

¹⁴⁸*Id.* art. 16.

¹⁴⁹*Id.*

a breach of personal privacy that was framed as a breach of confidence claim.”¹⁵⁰ Traditionally, both the principle and the balance of AngloAustralian authority favored the general application of *lex fori* in equity cases.¹⁵¹ Although the leading Australian case, *Murakami v. Wiryadi & Ors*, qualifies this approach by providing an unexhaustive list of exceptions, it never replaced the traditional *lex fori* approach.¹⁵² Similarly, this approach was upheld by the Court of Appeal in the UK in *Douglas v. Hello!*. This case concerned the unauthorized publication of the Douglas’ wedding photos in the UK. Subsequent to Michael Douglas and Catherine Zeta-Jones’s wedding in New York, a member of the paparazzi took unauthorized photos of this wedding and sold them to Hello! Magazine. The couple brought a claim for breach of confidence in the UK. Though Hello! Magazine argued that the proper law should be the law of New York—where the unjust enrichment occurred¹⁵³—this argument was effectively rejected by the Court of Appeal, who instead applied the English law of confidence to protect individual privacy.¹⁵⁴ Although the place of intrusion was New York, the court held that it was the English law of confidence that provided the remedy. This was consistent with the longstanding tradition of courts of equity using public policy concerns of the forum to exclude the operation of foreign law.¹⁵⁵ Scholars have advocated for other conflict of laws rules in breach of confidence cases.¹⁵⁶ However, it is undeniable that *lex fori* is the general rule for breach of confidence claims, which is most relevant in data breach cases.

D. De-Americanization of Substantive Data Protection Law

The nature of the right to personal data is characterized differently in the EU, the US, and China. Due to the mandatory nature of personal data protection law and the connecting factors leading to the law of the forum, the applicable law for transnational personal data depends on a race to courthouses or regulators.¹⁵⁷ Meanwhile, the domestic substantive data protection laws are experiencing a de-Americanization movement. The relationship between Internet data corporate giants and states needs to be reconsidered. The conventional wisdom is that Internet companies act, only to a small extent, in the shadow of state law.¹⁵⁸ Appearances, however, can be deceptive. These giants have to comply with the law of their domiciles, which is often US law. The developmental trend to regulate the Internet industry—especially the part of that industry concerned with data—has moved from Americanization to deAmericanization. This was triggered by the combination of legislative and nonlegislative approaches in the EU and China. Iconic examples include the passing of the GDPR in the EU, the Christchurch Call initiated by New Zealand and France, the Huawei ban, and the COVID-19 online propaganda that divide China and the US/EU.

¹⁵⁰*Giller v Procopets* (2008) 24 VR 1, 29 [133] (Ashley JA) (Austl.).

¹⁵¹*National Commercial Bank v Wimborne* (1978) 5 BPR [97 423], 24 (Holland J) (Austl.).

¹⁵²*Murakami v Wiryadi & Ors* [2010] NSWCA 7 (Austl.).

¹⁵³*Douglas v Hello!* [2006] QB 125, 160 (Lord Phillips for the Court) (Austl.); Regulation 864/2007, of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-contractual Obligations (Rome II), 2007 O.J. (L 199) 40 (EC).

¹⁵⁴In this case, the Court also considered whether the action should be characterized as a tort and acknowledged that it was “shoehorning” the claim into an equity claim.

¹⁵⁵Ben Chen, *Historical Foundations of Choice of Law in Fiduciary Obligations*, 10 J. PRIV. INT’L L. 171, 187 (2014).

¹⁵⁶E.g., Michael Douglas, *Characterisation of Breach of Confidence as a Privacy Tort in Private International Law*, 41 U. N.S.W. L.J. 490, 509 (2018).

¹⁵⁷See Houston Putnam Lowry, *Transborder Data Flow: Public and Private International Law Aspects*, 6 HOUS. J. INT’L L. 159, 170 (1983).

¹⁵⁸See Christopher Whytock, *Litigation, Arbitration, and the Transnational Shadow of Law*, 18 DUKE J. COMP. INT’L L. 449 (2008).

1. Americanization

Professor Jack M. Balkin indicates that “[c]urrently the Internet is mostly governed by the values of the least censorious regime—that of the United States.”¹⁵⁹ From the perspective of conflict of laws, this phenomenon can be explained by the significance of the law of domicile. The main global Internet players are US companies and industry associations registered in the US. Among the top ten Internet companies in the world, six are US companies: Amazon, Google, Facebook, Netflix, Booking, and eBay.¹⁶⁰ The domicile of a data company is significant, sometimes determinative, in identifying the law that would apply to protect personal data collected by the company. The US data regulatory environment features freedom of speech,¹⁶¹ industry self-regulation,¹⁶² the Federal Trade Commission’s consent decrees,¹⁶³ and weak consumer privacy regulations.¹⁶⁴

The domicile of a company is also important for the purpose of judgment recognition and enforcement.¹⁶⁵ Consequently, it is concerned about whether a domestic law on personal data protection can be respected in other jurisdictions. In *LICRA & UEJF v. Yahoo! Inc. & Yahoo France*, Yahoo! was ordered by a French court to block French users from accessing the auction site on Yahoo.com offering Nazi memorabilia in contravention of French law.¹⁶⁶ Yahoo! was domiciled in the US. Unsurprisingly, it went to a US district court and successfully obtained a judgment declaring that the French judgment was not recognizable or enforceable because it violated the First Amendment of the US Constitution.¹⁶⁷ Although the district court judgment was reversed at the appellate level on the grounds of a lack of personal jurisdiction on LICRA & UEJF and the “ripeness” of the enforcement claim, it nevertheless demonstrates that the First Amendment to the US Constitution can potentially be used to protect US-domiciled websites from enforcing foreign judgments.¹⁶⁸ Similarly, in *Google Inc. v. Equustek Solutions Inc.*, Google was required by a Canadian court to block websites violating Canadian law.¹⁶⁹ Google, yet another company with a domicile in the US, obtained a judgment at its home court that rendered the Canadian judgment unenforceable.¹⁷⁰ Furthermore, the US Securing the Protection of our Enduring and Established Constitutional Heritage Act (SPEECH Act 2010) expressly prohibits the recognition and enforcement of foreign defamation judgments against online providers, unless the defendant would have been liable under US law.¹⁷¹

¹⁵⁹Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1206 (2018).

¹⁶⁰*List of Largest Internet Companies*, WIKIPEDIA, https://en.wikipedia.org/w/index.php?title=List_of_largest_Internet_companies&oldid=914808498 (last visited Sept. 10, 2019).

¹⁶¹Richard Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT’L L. 365, 383 (2013).

¹⁶²Rita S. Heimes, *Privacy and Innovation: Information as Property and the Impact on Data Subjects*, NEW ENG. L. REV. 649, 663 (2014).

¹⁶³Boyne, *supra* note 86, at 305.

¹⁶⁴ANUPAM CHANDER, *THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD TOGETHER IN COMMERCE* 57–58 (2013).

¹⁶⁵UTA KOHL, *JURISDICTION AND THE INTERNET: REGULATORY COMPETENCE OVER ONLINE ACTIVITY* 201 (2007).

¹⁶⁶Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, 00/05308 (Fr.).

¹⁶⁷*Yahoo! Inc. v. La Ligue Contre le Racisme et l’Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

¹⁶⁸Upon the UEJF and LICRA’s appeal, the US Court of Appeals for the Ninth Circuit held that the district court lacked jurisdiction. It ultimately decided to rehear the case *en banc* and reversed the district court’s judgment, remanding the case with directions to dismiss the action on January 12, 2006. *Yahoo! Inc. v. LICRA & UEJF*, 433 F.3d 1199 (9th Cir. 2006). The Supreme Court of the US denied LICRA’s request to issue a *writ of certiorari* on May 30, 2006. But, Yahoo! has chosen to remove the sale of Nazi memorabilia from its site entirely.

¹⁶⁹*Equustek Solutions Inc. v. Jack* (2014), 374 D.L.R. 4th 537 (Can.); *Equustek Solutions Inc. v. Google Inc.* (2015), 386 D.L.R. 4th 224 (Can.); *see also Google Inc. v. Equustek Solutions Inc.*, [2017] 1 S.C.R. 824 (Can.); Jennifer Daskal, *Google Inc. v. Equustek Solutions Inc.*, 112 AM. J. INT’L L. 727 (2018).

¹⁷⁰*Google Inc.*, [2017] 1 S.C.R. at 824.

¹⁷¹*Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act of 2010*, 28 U.S.C. §§ 4101–4105 (2018).

II. De-Americanization

The substantive law for personal data protection and, broadly, international regulations is moving from Americanization to de-Americanization. The two main drivers are the EU and China.

1. EU

Although subject to criticism, the GDPR may commence the Europeanization of data protection law¹⁷² and symbolize the global trend of de-Americanization of data industry regulations.¹⁷³

The EU harmonizes data protection law through two means. The first is within the EU. The EU Data Protection Directive allows member states to apply their own law.¹⁷⁴ In contrast, the GDPR established a more harmonized framework, thanks to its direct application in member states.¹⁷⁵ Notably, Recital 21 of the GDPR provides that it “is without prejudice to the application of [the e-Commerce Directive] in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.” Therefore, the GDPR does not replace the intermediary liability rules of the e-Commerce Directive. Before the GDPR became effective, various cases attest to how courts in EU member states applied the e-Commerce Directive to personal information posted online by a third party.¹⁷⁶ However, considering the prohibitive penalty under the GDPR today, in practice, intermediaries would be more inclined to follow the GDPR rather than the e-Commerce Directive.¹⁷⁷ Also considering the long-arm jurisdiction created by the GDPR, courts may also be prone to apply the GDPR.¹⁷⁸ Further, compared with the e-Commerce Directive, the GDPR is especially relevant to protecting personal data in combating COVID-19. The European Data Protection Board has formally announced that the GDPR applies to the processing of personal data in the context of COVID-19.¹⁷⁹ In the processing of personal information by the competent public health authorities and employers, for reasons of substantial public interest in the area of public health, there is no need to rely on the consent of individuals.¹⁸⁰

Second, coordination of substantive law for personal data protection between EU members and non-members is also orchestrated through the European Commission’s adequacy decision, which requires that the state receiving data from the EU impose a highstandard data protection law equivalent to the EU standard.¹⁸¹ Article 45 of the GDPR provides that the transfer of personal data out of the EU is based on the European Commission’s adequacy decision. The Commission will take account of three elements when making the decision: Whether the non-EU country respects human rights and fundamental freedoms by general and sectoral legislation,¹⁸² whether the non-EU country has effectively established an independent supervisory authority for ensuring and enforcing compliance with the data protection rules,¹⁸³ and whether the non-EU country has

¹⁷²Orla Lynskey, *The “Europeanisation” of Data Protection Law*, 19 CAMBRIDGE Y.B. EUR. LEGAL STUD. 252 (2017).

¹⁷³Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 460–61 (2011).

¹⁷⁴EU Data Protection Directive, *supra* note 28, at consideration (9).

¹⁷⁵Paul Lefebvre & Cecilia Lahaye, *EU Data Protection and the Conflict of Laws: The Usual “Bag of Tricks” or a Fight Against the Evasion of the Law?*, 84 DEF. COUNS. J. 1, 2 (2017).

¹⁷⁶For Italian courts, see Cass. Pen., sez. tre., 3 febbraio 2014, n. 5107 (It.). For French courts, see Sophie StallaBourdillon, *Data Protection and Intermediary Liability: How Do the French Do It?*, INFORM’S BLOG (Apr. 24, 2017), <https://inform.org/2017/04/24/data-protection-abd-intermediary-liability-how-do-the-french-do-it-sophie-stalla-bourdillon/>.

¹⁷⁷GDPR, *supra* note 18, at art. 83(5).

¹⁷⁸Daphne Keller, *The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY J. INT’L L. 297, 371–74 (2018); see *Mosley v. Google Inc.* [2015] EWHC (QB) 59 [45]–[46] (Eng.).

¹⁷⁹*Statement by the EDPB Chair*, *supra* note 22.

¹⁸⁰*Id.*

¹⁸¹Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 J. INT’L ECON. L. 769, 775–77 (2018).

¹⁸²GDPR, *supra* note 18, at art. 45.2(a).

¹⁸³*Id.* at art. 45.2(b).

entered into legally binding conventions or instruments relating to the protection of personal data.¹⁸⁴ The adequacy decision is not a final decision. The European Commission should conduct a periodic review at least quadrennially¹⁸⁵ and monitor developments in countries that receive a positive adequacy decision.¹⁸⁶

Besides the GDPR, another important global effort to curtail the impacts of lax US internet regulations is the Christchurch Call. On March 15, 2019, a gunman attacked two mosques in Christchurch, New Zealand.¹⁸⁷ The gunman livestreamed the massacre at the first mosque on his Facebook page. The attacks killed 51 people.¹⁸⁸ According to § 230 of the Communications Decency Act (CDA), an internet intermediary like Facebook is immune from civil liability caused by third-party contents.¹⁸⁹ Therefore, by applying US law, Facebook would have no liability for allowing the gunman to livestream the massacre online.¹⁹⁰ On May 15, 2019, New Zealand Prime Minister Jacinda Arden, French President Emmanuel Macron, heads of many other states, and leaders of technology companies all adopted the Christchurch Call.¹⁹¹ The Call aims to “bring together countries and tech companies in an attempt to bring to an end the ability to use social media to organise and promote terrorism and violent extremism.”¹⁹² Online service providers, including Facebook, have committed to take transparent and specific measures to prevent the uploading of terrorist and violent extremist content, and to stop its dissemination on content-sharing services.¹⁹³ Unlike the GDPR, the Christchurch Call is non-binding. Nevertheless, it has gained wide support in Oceania and the EU, and its soft-law nature may help to promote its popularity in the global community. Thus far, the Call has been signed by seventeen countries, ranging from developing countries like Senegal and India to developed countries such as Japan and Germany.¹⁹⁴ Many big-name US Internet companies have endorsed the Call.¹⁹⁵

Unlike the GDPR and other legislation, the Christchurch Call represents a non-legislative approach, which is increasingly used to obtain compliance of US Internet giants.¹⁹⁶ An important difference between a legislative and non-legislative approach is that the latter can circumvent the difficulties of enforcing foreign judgments under the SPEECH Act in the US.¹⁹⁷ This is because

¹⁸⁴*Id.* at art. 45.2(c).

¹⁸⁵*Id.* at art. 45.3.

¹⁸⁶*Id.* at art. 45.4.

¹⁸⁷*Christchurch Shootings Mark “Unprecedented Act of Violence”, New Zealand Prime Minister Jacinda Arden Says*, ABC NEWS (Mar. 15, 2019, 12:30 AM), <https://www.abc.net.au/news/2019-03-15/christchurch-shootings-unprecedented-pm-jacinda-arden-says/10904950>.

¹⁸⁸*Id.*

¹⁸⁹47 U.S.C. § 230 (2018). This Act is also known as the Cox-Wyden Amendment. For comments on this Act, see Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 3 (2017).

¹⁹⁰*See Force v. Facebook, Inc.*, 934 F.3d 53, 65, 71 (2d Cir. 2019) (rejecting, based on CDA §230, plaintiffs’ argument that Facebook should be liable for “giving Hamas a forum with which to communicate and for actively bringing Hamas’ message to interested parties” as a “material support for terrorism”).

¹⁹¹CHRISTCHURCH CALL TO ELIMINATE TERRORIST AND VIOLENT EXTREMIST CONTENT ONLINE, <https://www.christchurchcall.com/> (last visited Nov. 9, 2019).

¹⁹²*The Christchurch Call to Action*, CHRISTCHURCH CALL, <https://www.christchurchcall.com/christchurch-call.pdf>.

¹⁹³*Id.*

¹⁹⁴Among the signatories to the Call are the European Commission, and the governments of Australia, Canada, France, Germany, Indonesia, India, Ireland, Italy, Japan, Jordan, the Netherlands, New Zealand, Norway, Senegal, Spain, Sweden, and the UK.

¹⁹⁵For example, Amazon, Dailymotion, Facebook, Google, Microsoft, Qwant, Twitter, and YouTube have signed the Call. The US declined to sign the Call because of concerns that compliance with the Call may conflict with free speech protections in its Constitution.

¹⁹⁶*See Danielle Keats Citron, Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1041–45 (2018) (discussing using the non-legislative approach, such as code of conduct and blacklist database, to seek industrial compliance).

¹⁹⁷*Id.* at 1056.

industrial compliance is embodied in the terms of service and can be applied all over the world.¹⁹⁸ In contrast, a court judgment may be enforced only in the judgment-rendering state.¹⁹⁹ If it is not recognizable and enforceable in the state where the company is domiciled—for example, the US—its efficacy is limited. Its global impact is further limited by the insufficient international mechanism for recognition and enforcement of judgments.²⁰⁰

2. China

China is another strong proponent of de-Americanization of data industry regulations. It does so for reasons very different from the EU. The EU promotes de-Americanization because it considers protecting personal data a fundamental human right and the US laissez-faire protection insufficient. For China, the main drive for de-Americanization is national security. This drive has been boosted by two recent incidents.

The first is the US Huawei ban.²⁰¹ Huawei is a leading Chinese 5-G manufacturer and the second-largest smartphone manufacturer in the world.²⁰² On May 16, 2019, President Donald Trump added Huawei to the US blacklist and banned US companies from doing business with them, without first obtaining US government approval,²⁰³ on the allegation that Huawei posed “threats against information and communications technology and services in the US.”²⁰⁴ Due to the ban, companies that stopped supplying Huawei include not only US companies, such as Google and Intel, but also non-US companies, including the UK’s ARM and Vodafone,²⁰⁵ Germany’s Infineon,²⁰⁶ and Japan’s KDDI and Docomo.²⁰⁷ These non-US companies have production lines in the US and are thus concerned over the US sanction in the case of non-compliance. Although the Huawei ban was issued by the US government, it has led to a broad snowball effect to largely preclude Huawei from the global supply chain. The Huawei Ban teaches a vivid lesson to private companies domiciled in China and other countries which are traditionally not allies to the US: Even though they are registered outside of the US, they are still subject to US law by relying on the global supply chain that is dominated by US companies and industry associations. Consequently, they may have to join the internet sovereignty camp. Previously, the internet sovereignty camp was constituted by states such as China and Russia, rather than

¹⁹⁸*Id.*

¹⁹⁹*Id.*

²⁰⁰The Convention of July 2, 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters has not come into effect. *Status Table 41*, HAGUE CONFERENCE ON PRIVATE INT’L LAW, <https://www.hcch.net/en/instruments/conventions/status-table/?cid=137> (last visited July 11, 2020). The Convention of June 30, 2005 on the Choice of Court Agreements has been ratified by 32 countries—most of them are European countries. *Status Table 37*, HAGUE CONFERENCE ON PRIVATE INT’L LAW, <https://www.hcch.net/en/instruments/conventions/status-table/?cid=98> (last visited April 2, 2020).

²⁰¹Sean Keane, *Huawei ban timeline: China may restrict Nokia, Ericsson if EU bans Huawei from 5G networks*, CNET (June 25, 2020, 7:10 AM), <https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-p40/>.

²⁰²*Id.*

²⁰³Sonam Sheth, *Trump declares a national emergency, which could set up a huge blow to China’s Huawei*, BUS. INSIDER AUSTL. (May 16, 2019, 7:09 AM), <https://www.businessinsider.com.au/trump-national-emergency-china-huawei-2019-5>.

²⁰⁴Victoria Bell, *Now EE and Vodafone drop Huawei Phones from their 5G network launch lineup as chip designer ARM distances itself from the company over US ban*, DAILY MAIL (May 22, 2019, 6:59 AM), <https://www.dailymail.co.uk/sciencetech/article-7057889/EE-switch-5G-network-month-sale-Huawei-devices-paused.html>.

²⁰⁵Dave Lee, *Huawei: ARM memo tells staff to stop working with China’s tech giant*, BBC (May 22, 2019), <https://www.bbc.com/news/technology-48363772>.

²⁰⁶Adam Satariano, Raymond Zhong & Daisuke Wakabayashi, *Google, Intel and Other US Companies Stop Supplying Huawei*, N.Y. TIMES (May 21, 2019), <https://cn.nytimes.com/business/20190521/google-huawei-android/>.

²⁰⁷*Japan Just Followed, Two Big Telecommunication Companies Announced Unlimited Postpone of Launching Huawei Mobile Phone*, QQ, <https://new.qq.com/omn/20190523/20190523A0RRJU.html> (last visited Nov. 9, 2019).

private technology companies.²⁰⁸ Internet sovereignty is often considered to be more concerned with national security than private commercial interest. The prominent example is China's 2017 Cybersecurity Law aiming to "safeguard cyber security, protect cyberspace sovereignty and national security."²⁰⁹ However, the Huawei Ban may drag private companies domiciled in non-US allies into the internet sovereignty camp because the US does not treat companies as separate legal entities from the state that they domicile. Therefore, the Huawei Ban will promote the deAmericanization in the data industry.

The second incident is the global pandemic of COVID-19. As discussed in Section I, *Lex Fori* Based on Connecting Factors and Mandatory Law of the Forum, the Notification on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control of Disease is a mandatory law and should be applied to international travelers in China.²¹⁰ This Notification provides that all localities and departments should attach great importance to the protection of personal information; except for those agencies authorized by the State Council's Sanitary and Health Department in accordance with China Cyber Security Law, the Law on Prevention and Control of Infectious Diseases, and Regulations on Public Health Emergencies, no other unit or individual may use personal information on the grounds of epidemic prevention and control or disease prevention without the consent of the person being collected.²¹¹ Where laws and administrative regulations provide otherwise, they shall be implemented accordingly.²¹² The collector of personal information necessary for joint prevention and control should refer to the national standard of Personal Information Security Regulations and adhere to the principle of minimum collection.²¹³ The collection object is limited to key groups—such as diagnosed persons, suspects, and close contacts in principle—and is generally not targeted at specific areas, to prevent de facto discrimination against specific geographic groups.²¹⁴ Personal information collected for epidemic prevention and control and disease prevention shall not be used for other purposes.²¹⁵ No entity or individual may disclose personal information such as name, age, identity card number, phone number, or home address without the consent of the person from whom the data is collected, except for the joint disease defense and control work.²¹⁶ All personal information used should be desensitized and anonymized.²¹⁷ Therefore, the Chinese media violated this Notification in the COVID-19 case discussed in the first paragraph of the Article, because they published that lady's detailed personal information without her consent. The collection and release of her information did not comply with the minimum principle because her employment information, the university from where she graduated, and the year of her graduation have nothing to do with disease prevention and control.

According to the Notification, the Chinese network information department shall promptly deal with the illegal collection, use, and disclosure of personal information, and incidents that cause a large amount of leakage of personal data in accordance with China Cyber Security Law and related regulations.²¹⁸ The police department should severely crack down on relevant crimes according to law.²¹⁹ Yet, the Chinese authorities have not done anything to remedy the

²⁰⁸Jack Margolin, *Russia, China, and the Push for "Digital Sovereignty"*, IPI GLOB. OBSERVATORY (Dec. 2, 2016), <https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/>.

²⁰⁹Chinese Cybersecurity Law at art. 1.

²¹⁰NOTIFICATION ON PROTECTING PERSONAL INFORMATION, *supra* note 132.

²¹¹*Id.* at art. 1.

²¹²*Id.*

²¹³*Id.* at art. 2.

²¹⁴*Id.*

²¹⁵*Id.* at art. 3.

²¹⁶*Id.*

²¹⁷*Id.*

²¹⁸*Id.* at art. 6.

²¹⁹*Id.*

personal information violation caused to the lady discussed in the first paragraph of this Article. This reveals two issues. First, compared with the EU GDPR, the enforcement mechanism of the Notification and other Chinese law for personal data protection is much weaker. Violating the GDPR can result in a fine of up to €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater.²²⁰ Comparatively, the China Cyber Security Law provides that personal data breaches can lead to a fine of up to ten times the illegal income; if there is no illegal income, the fine is less than RMB 1 million.²²¹ Second, Chinese law for personal information protection is subject to China's national interest. This is especially true for COVID-19 online propaganda. In January and early February 2020, Chinese media widely reported that the spread of COVID-19 was due to people who sold and ate wild animals illegally.²²² However, with COVID-19 spreading to the rest of the world, the Chinese media has begun to publish articles criticizing the US as the origin of the disease since March 2020.²²³ It is not the intention of this Article to discuss what is the origin of COVID-19 and who should be liable. The point is that the sharp divide between China and the US regarding the origin of COVID-19 and the relevant state liability will further push China to firmly control online media and Internet companies located in China. De-Americanization is consistent with China's national interest.

E. Dynamics Among Trends

Three trends have emerged at each stage of identifying the applicable law for transnational personal data: (1) The EU, the US, and China characterize the right to personal data differently, (2) the spread-out unilateral applicable law approach comes from the fact that all three jurisdictions either consider the law for personal data protection as a mandatory law or adopt connecting factors leading to the law of the forum, and (3) the EU and China strongly advocate de-Americanization of substantive data protection laws. These trends are developing and interacting with one another. Their dynamics are two-fold.

At the macro level, the trends are consistent with one another. The multi-faceted legal nature of the right to protect personal data fosters the spread-out unilateral applicable law approach. Consequently, de-Americanization has been supported by the EU and China. All the trends embody the fundamental value and national interest of states. However, because these values and interests are so diverse, the trends demonstrate the regulatory competition among states on personal data in transnational contexts. For instance, the US overarchingly values the freedom of speech, thus elucidating their adoption of lax data regulation and blockage of foreign judgments that violate the First Amendment of the US Constitution. Contrarily, in the EU, privacy of personal data is considered a fundamental human right. Therefore, it is unsurprising that the GDPR imposes broad extra-territorial jurisdiction. Chinese data governance derives from the national interest in using personal data as a valuable resource to develop the data industry and maintain social stability. Therefore, China distinguishes the right to personal data from the right to privacy and supports de-Americanization.

At the micro level, if we look into each individual trend, it is apparent that the divergent laws adopted by each jurisdiction in that trend are not actually reconcilable. The typical example is the industry self-regulation of personal data in the US that conflicts with the laws in China and the

²²⁰For a list of fines and notices issued under the GDPR, see *GDPR Fines and Notices*, WIKIPEDIA, https://en.wikipedia.org/wiki/GDPR_fines_and_notices (last updated June 17, 2020).

²²¹Chinese Cybersecurity Law at art. 64.

²²²*Evidence Is Confirmed that Virus Is Found at Huanan Fish Market*, SINA (Jan. 23, 2020, 11:40 PM), <http://finance.sina.com.cn/7x24/2020-01-23/doc-iihnzahnk6049908.shtml>; *Lancet Published Chinese Scholar's Comment: The Relationship between Novel Coronavirus and Consumption Wild Animals*, CHINA NEWS (Feb. 12, 2020, 7:50 AM), <https://m.chinanews.com/wap/detail/zw/sh/2020/02-12/9087971.shtml>.

²²³E.g., Jiang Xiaozhang, *Where Does COVID-19 Come From? Chinese Academy of Sciences Published a Paper Telling You the "Truth"*, CHINA.COM (Mar. 1, 2020, 11:18 AM), https://news.china.com/zw/news/13000776/20200301/37852321_all.html.

EU, which clearly push for more government regulations—in other words, de-Americanization. However, in the de-Americanization camp, the differences existing in the laws adopted by the EU and China exceed nuance. Because the contents of substantive laws adopted by the US, the EU, and China are so different, coordination of substantive law at the regional level by the GDPR adequacy decisions actually leads to a wider gap internationally.

F. Conclusions

As German Chancellor Angela Merkel indicated at the Harvard University 368th Commencement Ceremony on May 30, 2019: “[A]re we laying down the rules for technology, or is technology dictating how we act? Do we prioritize people as individuals with human dignity with all the manifests or do we see them as many consumers, data sources, objects of surveillance?” These questions are especially relevant for protecting personal information of international travelers and combating COVID-19. According to conflict of laws, determining an applicable law in a transnational case requires three stages: characterization, connecting factors, and identifying a legal system. Using the incident where the personal data of an international traveler was illegally released by Chinese media, this Article identifies three trends that have emerged at each stage: the multi-faceted legal nature of the right to protect personal data, the spread-out unilateral applicable law approach, and the de-Americanization of substantive law for personal data protection. The trends and their dynamics provide valuable implications for developing the choice of laws for transnational personal data. First, the choice of laws aims to provide comity, consistency, and predictability to international civil litigations and discourage forum shopping.²²⁴ Nevertheless, due to the spread-out unilateral applicable law approach and the consequent lesser possibility of applying foreign law, the importance of choice of laws significantly decreases in cases of transnational personal data breach. This finding informs parties that jurisdiction is a predominant issue in data breach cases because courts and regulators would apply the forum law. Second, currently there is no international treaty or model law on choice-of-law issues for transnational personal data. International harmonization efforts will be a long and difficult journey considering how the trends demonstrate not only the states’ irreconcilable interests, but also how states may consider these interests as their fundamental values that they do not want to trade off. Therefore, for states and international organizations, a feasible priority is to achieve regional coordination or interoperation among states with similar values on personal data protection.

²²⁴MARTIN DAVIES, ANDREW BELL & PAUL LE GAY BRERETON, *NYGH’S CONFLICT OF LAWS IN AUSTRALIA* 306–10 (9th ed. 2014).