THE UNIVERSITY OF SYDNEY

The University of Sydney Law School

Legal Studies Research Paper Series

No. 20/23

April 2020

COVID-19 and Applicable Law to Transnational Personal Data: Trends and Dynamics

Jeanne Huang

COVID-19 and Applicable Law to Transnational Personal Data:

Trends and Dynamics

Associate Professor Jie (Jeanne) Huang, Sydney Law School

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 traveller was illegally released by Chinese media, the paper identifies that three trends have emerged at the 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 de-Americanisation 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 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 organisations, 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

Table of Contents

The recent COVID-19 outbreak has pushed the tension of protecting personal data in a transnational context[1] to an apex. This is because COVID-19 spreads fast with the international travel of people.[2] Many countries require international travellers to disclose their personal information such as the name, gender, date of birth, travel history, the purpose of travel and residence, etc, and 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 she temporarily lived in Beijing.[4] A Chinese policeman required this lady to stay at home.[5] This lady refused and alleged she was abused by the policeman.[6] Chinese media released this lady's photo,[7] her age, her flight information, her name,[8] her nationality, her

[1] In this paper, "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 e.g. it involves foreign data subjects, or is collected, saved or processed in different jurisdictions.
[2]What You Need to Know about Coronavirus (COVID-19)? 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 April 1, 2020).
[3] Coronavirus Quarantine Rules will Force International Arrivals into Two-week Quarantine in Hotels and Caravan Parks, https://www.abc.net.au/news/2020-03-27/coronavirus-quarantine-laws-force-international-arrivals-hotels/12097312 (last visited April 1, 2020). Travel and COVID-19, https://www.agriculture.gov.au/travelling/to-australia/advice-to-travellers/human-health/coronavirus (last visited April 1, 2020).
[4] An Australian Woman Breached Coronavirus Quarantine in Beijing to Go for a Jog—And Lost Her Job, https://edition.cnn.com/2020/03/20/asia/beijing-coronavirus-woman-fired-intl-hnk/index.html (last visited April 1, 2020).
[5] *Id.*
[6] *Id.*
[7] Some Chinese media mosaicked her face but some not. Bayer Fired the Woman who Refused to be Quarantined and Went Jogging, https://m.weibo.cn/search?containerid=231522type%3D1%26t%3D10%26q%3D%23%E6%8B%9C%E8%80%B3%E8%BE%9E%E9%80%80%E6%8B%92%E7%BB%9D%E9%9A%94%E7%A6%BB%E5%A4%96%E5%87%BA%E8%B7%91%E6%AD%A5%E5%A5%B3%E5%AD%90%23&extparam=%23%E6%8B%9C%E8%80%B3%E8%BE%9E%E9%80%80%E6%8B%92%E7%BB%9D%E9%9A%94%E7%A6%BB%E5%A4%96%E5%87%BA%E8%B7%91%E6%AD%A5%E5%A5%B3%E5%AD%90%23&luicode=10000011&lfid=231522type%3D1%26t%3D10%26q%3D%23%E6%BE%B3%E7%B1%8D%E5%8D%8E%E4%BA%BA%E5%A5%B3%E5%AD%90%E8%BF%94%E4%BA%AC%E6%8B%92%E7%BB%9D%E9%9A%94%E7%A6%BB%E8%A2%AB%E8%BE%9E%E9%80%80%23 (last visited April 1, 2020).
[8] Her name has three Chinese characters and the media released the first Chinese character-being the surname and the last Chinese character. Some Chinese media released her full English name. Bayer Australian Employee

temporary home address in Beijing, the Chinese and Australian universities she graduated and the years of her graduation, her employment history and positions, her current employer and her salary, etc.[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 Chinese quarantine requirement.[11] Because her Chinese visa was sponsored by Bayer in China, Chinese government revoked her visa and deported her after Bayer terminated her employment contract.[12] Clearly, this lady violated the COVID-19 mandatory self-quarantine regulation in China. Her conduct threatened the public health and should be condemned. However, does her offense justify releasing her detailed personal information online? Based on the released information, this lady's identity can be easily ascertained. This lady is an Australian citizen and she arrived at China just for one day before the incident occurred. Therefore, she is unlike 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

---

Ms Liang Resume and Photo, Should the Company Compensate this Woman? https://www.gucheng.com/hot/2020/3875795.shtml (last visited April 1, 2020).

[9] The Jogging Woman Liang X Yang Was Deported: Australia Locked Down and Rejecting her Return! How Will She Make a Living? 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 April 1, 2020). Rich and Ill-tempered "Australian Jogging Woman" Graduated from Famous Universities and Earned One Million, https://zhuanlan.zhihu.com/p/115002155 (last visited April 1, 2020).

[10] That Australian Who Jogged without Wearing a Mask and Shouted for Help was Fired!, https://cj.sina.com.cn/articles/view/6115560351/16c840b9f01900o0dd (last visited April 1, 2020).

[11] *Id.* cf. Other new reports indicates that this lady may go to Germany and work for Bayer, https://www.sohu.com/a/383204342_334936?scm=1002.44003c.fe017c.PC_ARTICLE_REC&spm=smpc.content.fd-d.2.1585791557071kSlKl7d&_trans_=000012_sogou_fl_ty&_f=index_pagerecom_2 (last visited April 1, 2020).

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

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

transnational personal data: which law should be applied to the personal data of an international traveller who violates a local quarantine law.

Protecting personal data in the transnational contexts is important and necessary. This is because in modern society where individuals often travel across borders,[14] technology such as the Internet and the cloud is inherently transnational,[15] and online service providers also actively make their service accessible around the world.[16] Domestic regulators have also become more serious about protecting personal data in the transnational contexts.[17] The EU implemented the General Data Protection Regulation (hereinafter "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] However, 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 traveller 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

[14] See Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 EUR. J. INT. LAW 441–456, 441 (2010).
[15] Georg Haibach, *Cloud Computing and European Union Private International Law*, 11 J. PRIV. INT. LAW 252–266, 253–54 (2015).
[16] Michael D. Simpson, *All Your Data are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy Casenote and Comments*, 87 UNIV. COLO. LAW REV. 669–710, 670–73 (2016).
[17] Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT. ECON. LAW 245–272, 245–272 (2018).
[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L119/1.
[19] California Consumer Privacy Act passed on 23 September 2018 and effective on 1 January 2020, https://www.isipp.com/resources/full-text-of-the-california-consumer-privacy-act-of-2018-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 business. California Consumer Privacy Act blog series: Covered Entities, https://www.dataprotectionreport.com/2018/08/california-consumer-privacy-act-blog-series-covered-entities/.
[20] General Rules of the Civil Law of China [Minfa Zongze], promulgated on 15 March 2017 and effective on 1 October 2017, http://www.court.gov.cn/zixun-xiangqing-37832.html (last visited 10 September 2019).
[21] "Treasury Laws Amendment (Consumer Data Right) Bill 2019", https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6370 (last visited 10 September 2019). The third reading of the Bill was agreed on 1 August 2019.

Personal Data in the Context of the COVID-19 Outbreak adopted by European Data Protection Board.[22] In Australia, some states may release the flight information and places where an international traveller 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: characterise the issue into one of the established choice of law classifications by identifying the nature of the subject matter, select the rule of conflict of laws which lays down a connecting factor for the issue in question, and 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 is valuable national studies or comparative scholarship exploring personal data protection.[25] However, little conflict-of-laws

[22] Statement by the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak, 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").

[23] In New South Wales Australia, personal information is defined under S 4 Privacy and Personal Information Protection Act 1998 (NSW) (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 be reasonably be ascertained from the information or opinion. The NSW government agency may disclose the relevant personal information to the general Australian public (i.e. including those outside of NSW jurisdiction) or to an Australian Commonwealth agency. It is allowed to do 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 s19(2)(f) of PPIPA. The Public Health Act 2010 (NSW) also allows the government to release certain personal information so the general public can keep distance with the home address or the places that a patient has visited.

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

[25] For country or comparative studies on applicable law for personal data, see e.g. 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 COMPUT. LAW SECUR. REV. 462, 462–475 (2019); Michael Ng, *Choice of Law for Property Issues regarding Bitcoin under English Law*, 15 J. PRIV. INT. LAW 315, 315–338 (2019); Tobias Lutzi, *Internet Cases in EU Private International Law---Developing a Coherent Approach*, 66 INT. COMP. LAW Q. 687–721, 687–721 (2017); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEORGETOWN LAW J. 115, 115–178 (2017); Andrew Keane Wood, *Against Data Exceptionalism*, 68 STAN 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. LAW 60, 60–76 (2016); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE LAW J. 326, 326–399 (2015); Maja Brkan,

literature has compared how China, the US, and the EU would characterise the right to personal data, what connecting factors they would consider, and which law they would eventually apply to protect personal data. These issues are important especially in the contexts of COVID-19 where states strictly monitor international travellers. 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 organisations who plan to propose treaties or model laws to coordinate national laws.

This Paper is divided according to the three stages of conflict-of-laws analysis. The first Section argues that China, the US and the EU characterise 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 considered the right to personal data is a personality right. The second Section analyses 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 curtail 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 analyses 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 Americanisation to de-Americanisation. The first three sections of the

---

'Data Protection and European Private International Law: Observing a Bull in a China Shop' (2015) 5 International Data Privacy Law 257, 257–278; Rita Matulionyte, *Calling for Party Autonomy in Intellectual Property Infringement Cases*, 9 J. PRIV. INT. LAW 77, 77–97 (2013); Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY LAW J. 677, 677–739 (2014); Salil K. Mehra & Marketa Trimble, *Secondary Liability, ISP Immunity, and Incumbent Entrenchment*, 62 AM. J. COMP. LAW 685, 685–705 (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. LAW J. 413, 413–482 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design The Disclosure Crisis: Essay*, 88 WASH. LAW REV. 385, 386–418 (2013); Gregory E. Maggs, *Regulating Electronic Commerce*, 50 AM. J. COMP. LAW 665, 665–685 (2002).

paper present three trends at each stage of conflict-of-law analysis: the multi-faceted legal nature of right to personal data, the spread-out unilateral applicable law approach, and the de-Americanisation 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 of conflict of laws analysis in transnational data breach. In contrast, the gaps between the substantive domestic law for personal data protection are widening with the de-Americanization movement. The Fifth Section concludes the paper.

1. Multi-faceted right to personal data

There is no uniformity to characterise the right to personal data in the US, EU and China. This is because this right is considered as 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]

1.1. Human right

In the EU, a data subject's right to his or her personal data is characterised as a person's "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

[26] See *infra* Section 1.1.
[27] See *infra* Section 1.2 and 1.3.
[28] Art. 1.2 of GDPR. See Article 1(1) of EU Data Protection 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 (hereinafter "EU Data Protection Directive").
[29] Schwartz and Peifer, *supra* note 25 at 123.

data is founded on 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 authorises 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 data breach was conducted by

[30] David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INTERNATIONAL JOURNAL OF CONSTITUTIONAL LAW 220, 223 (2016).
[31] The European Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, effective in 1953, for an official text, see https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.
[32] Charter of Fundamental Rights of the European Union, 2000 O.J C 364/10: a constitutional document of the EU. Art. 8.1 contains an explicit right to data protection, indicating: "[e]veryone has the right to the protection of personal data ...."
[33] Art. 8(2) of the EU Charter.
[34] Art. 16 of Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. C 326/47.
[35] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. LAW REV. 193–220, 195–96 (1890).
[36] US Privacy Act, 5 U.S.C. § 552. 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).
[37] U.S. CONST. amend. IV.

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] In contrast, the Constitution of the US firmly establishes free flow of information by the First Amendment's free speech clause,[42] which may be more likely to be considered as fundamental human rights in the US.[43] For example, *Sorrell v IMS Health Care* is concerned with a Vermont law which 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

[38] Dan Swinhoe, *the Biggest Data Breach Fines, Penalties and Settlements So Far*, CSO ONLINE (2019), https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html (last visited Sep 10, 2019).
[39] *Roe v. Wade*, 410 U.S. 113, 153 (1973). In *Whalen v Roe*, although the Supreme Court of the US identified a general right to "information privacy" in the Fourteenth Amendment, the Court upholds a New York statute requiring identification of physicians and patients in dangerous legitimate drug prescription records. *Whalen v Roe*, 429 U.S. 589, 605-06 (1977).
[40] *American Fed. Of Gov't Employees, AFL-CIO v. Dep't of Hous. And 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").
[41] Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States,* 80 Iowa L. Rev. 553, 574-82 (1995). Schwartz and Peifer, *supra* note 25 at 133.
[42] ''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.'' *44 Liquormart, Inc. v. Rhode Island,* 517 U.S. 484, 503, 116 S.Ct. 1459 (Opinion of Stevens, J.)
[43] Schwartz and 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. LAW REV. 751, 758 and 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] 564 U.S. 552, 561 (2011). The law is § 4631(d) Vermont Prescription Confidentiality Law (2007)
[45] 564 U.S. 552, 565 (2011).
[46] *Id.* at 572.
[47] *Id.* at 572.

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 of violating the First Amendment.[50]

In China, the right to personal data is considered as a personality right. There are two reasons. First, different from the EU, Chinese legislators do not consider the right to personal information is a fundamental human right. This is not because they cherish 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 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 Chinese situation. Although the Internet is decentralized, Chinese government is still the ultimate controller because it controls the Internet connections between its territory with the outside the 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 VPN.[54] Chinese government controls and accesses personal data of users of Chinese Internet service providers such as

[48] *Id.* at 577.
[49] *Id.*
[50] *Id.* at 580.
[51] Zhang Xinbao, *From Privcay to Personal Information: The Theory and System to Re-balance Interest*, 3 CHINA LEG. SCI. ZHONGGUO FAXUE 38, 39 (2015).
[52] Samuelson, *supra* note 43 at 761.
[53] Samuel Woodhams, The Rise of Internet Sovereignty and the End of the World Wide Web?, https://theglobepost.com/2019/04/23/internet-sovereignty/ (last visited April 2, 2020).
[54] Man in China Sentenced to Five Years' Jail for Running VPN, https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn (last visited April 2, 2020).

Wechat.[55] Although Chinese Constitution limits the government access to Chinese citizens' correspondence to the circumstances of national security and criminal investigations,[56] other Chinese laws have gone beyond this constitutional limit. For example, Article 25 of Chinese E-commerce 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 e-commerce 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, 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 information far more than an individual's address and other contact information. It is unclear whether these constitutional provisions can cover all other personal data. More important, these constitutional provisions are about protecting privacy; however, in China, protecting personal data is not the same as protecting privacy. 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.

---

[55] Wechat Shares Consumer Data with Chinese Government, https://www.pymnts.com/safety-and-security/2017/wechat-hands-over-user-data-to-chinese-government-amid-privacy-concerns/ (last visited April 2, 2020).
[56] Art. 40 of Chinese Constitution [Xian Fa], adopted at the Fifth Session of the Fifth National People's Congress and promulgated for implementation by the Announcement of the National People's Congress on December 4, 1982, most recently amended on March 11, 2018.
[57] Art. 25 of Chinese E-commerce Law [Dianzi Shangwu Fa], promulgated by the Standing Committee of the National People's Congress on August 31, 2018 and effective on January 1, 2019, Order No. 7 of the President of the People's Republic of China.
[58] Arts 39 and 40 of Chinese Constitution.
[59] General Rules of the Civil Law of China [Minfa Zongze], promulgated on March 15, 2017 and effective on October 1, 2017, http://www.court.gov.cn/zixun-xiangqing-37832.html (last visited November 9, 2019).

Article 110 provides that "natural persons have the right to life, body, health, name, portrait, reputation, honour, privacy, marriage autonomy, etc."[60] Article 111 indicates that:

> "the 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 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. The second opinion is endorsed by the Proposed Chinese Civil Code (third draft) (hereinafter "the Proposed Chinese Civil Code").[62] If enacted, the Proposed Chinese Civil Code will replace all existing laws concerning civil-law issues.[63] Article 811 of the Proposed Chinese Civil Code defines privacy and Article 812 provides that the right to privacy should be protected as *erga omnes*.[64] Articles 813 to 817 address personal data, however, focusing on collection and process of personal data according to principles of legality, proportionality and necessity.[65] Namely, provisions for privacy focuses 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

---

[60] *Id.,* art. 110.
[61] *Id.,* art. 111.
[62] The Proposed Chinese Civil Code (third draft) was submitted to review at the 15th Meeting of the 13th Standing Committee of the National People's Congress on December 23, 2020. The official draft of the Proposed Chinese Civil Code can be found at http://www.npc.gov.cn/npc/c35174/mfdgfbca.shtml.
[63] *Id.,* art. 1260.
[64] *Id.,* article 812 provides limited exceptions (i.e. circumstances prescribed by law and consented by a right holder) to intrusion of privacy.
[65] *Id.,* arts 813 to 817.

Chinese scholars.[66] Their arguments can be summarized as follows.[67] Firstly, privacy focuses on protection of *an individual's personal information*.[68] However, personal data protection in the digital economy emphasizes protecting *personal data of a collective of individuals*.[69] This is because digital economy relies on big data which requires a collective of individuals' information rather than on individual's information.[70] Secondly, being a protector is the main role for a state regarding an individual's privacy. In contrast, big data of personal information is valuable resource for a state to develop digital economy, maintain social stability and safeguard national security.[71] Therefore, a state not only protects personal data but also has interest in accessing, collecting, analysing, etc personal information.[72] Third, data collectors (e.g. 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, 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 supports in other Chinese legislation and judicial practice. For example, the Provisions of the Supreme People's Court on Several

---

[66] E.g. Mei Xiaying, *The Legal Properties of Data and the Position of Data in Civil Law*, 9 SOC. SCI. CHINA ZHONGGUO SHEHUI KEXUE 164, 175 (2016).
[67] Xinbao, *supra* note 51 at 45–49.
[68] Liming Wang, *Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy [Lun Geren Xinxi Quan de Falv Baofu---Yi Geren Xinxi Quan yu Yinsi Quan de Jiefen wei Zhongxin]*, 35 MOD. LAW SCI. XIANDAI FAXUE 62, 66 (2013).
[69] Jianhua Xiao & Fangmo Chai, *An Analysis of Data Rights and Transaction Regulation*, 1 SOC. SCI. CHINA UNIV. [ZHONGGUO GAOXIAO SHEHUI KEXUE] 83, 86–87 (2019).
[70] *Id.*
[71] Weiguan Wu, *Critique of Personal Data Information Privacy Protection under Big Data Technology [Da Shuju Jishu xia Geren Shuju Xinxi Siquan Baohu Lun Pinpan]*, 7 POLIT. LAW ZHENGZHI YU FALV 116, 129–31 (2016).
[72] *Id.*
[73] Bo 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 GLOB. LAW REV. [HUAN QIU FALV PINLUN] 86, 100 (2018).
[74] Wang, *supra* note 68 at 66–67.
[75] Cheng Xiao, *Personal Data Rights in the Era of Big Data [Da Shuju Shidai de Geren Xingxi Quan Baofu]*, 3 SOC. SCI. CHINA [ZHONGGUO SHEHUI KEXUE] 102, 115–116 (2018).

Issues about Applicable Law in Civil Cases of Using Information Network to Infringe Personal Rights and Interests (hereinafter "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 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 italicised part would be redundant.

Ye Zhu v. Baidu, the first case on privacy protection concerning cookie technology,[78] sheds a 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 due to Baidu, without her permission, recording of keywords she searched such as "breast enhancement", "weight loss", "abortion" and using of 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 and Amazon and other Internet service providers. Further, the Cookies collected by Baidu did not include any

[76] 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 [Zuigao Remin Fayuan Guanyu Shengli Liyong Xingxi Wangluo Qinghai Renshen Quanyi Minshi Jiufeng Anjian Shiyong Falv Luogang Wenti de Guiding] (hereinafter "SPC Provisions on Applicable Law for Personal Rights Infringement"), promulgated on 21 August 2014 and effective on 10 October 2014, Fa Shi [2014] No. 10.
[77] Art. 12.1 of SPC Provisions on Applicable Law for Personal Rights Infringement.
[78] Chinese Appellate Court Provides Guidance for Lawful Use of Cookies, HL CHRONICLE OF DATA PROTECTION (2015), https://www.hldataprotection.com/2015/08/articles/international-eu-privacy/chinese-appellate-court-provides-guidance-for-lawful-use-of-cookies/ (last visited Sep 10, 2019).
[79] *Ye Zhu v. Baidu [Beijing Baidu Wangxun Keji Youxian Gongsi yu Bei Shangsu Ren Zhu Ye Yingsi Quan Jiufeng An]*, Nanjing Intermediate People's Court (2014) Ning Min Zong Zi No. 5028.
[80] This case relates to the usage of Cookie, a widely used Internet technology. When an Internet user uses a browser to conduct searches on Baidu.com, a cookie information automatically sent by Baidu will be saved on the user's browser. Through the connection established by cookie, Baidu is able to identify the browser and predict the user's interest and thus provide tailor-made advertisements.

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 only appeared on Zhu's computer and were not published by Baidu to other parties. Baidu therefore contended that it did not infringe on Zhu's privacy. 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. Firstly, 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. Resultantly, when the same user used a different browser to search the Internet, Baidu identified this user as a different user. Secondly, Baidu did not publish Zhu's personal information since Cookie technology conducted machine-to-machine communication rather than machine to human. Thirdly, 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 search keywords of an Internet user could reflect the user's activity history and Internet browsing preferences, so they were of 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 if a piece of privacy information, used individually, cannot identify a data subject, this privacy information is not a personal information; even if combined with other information collected by a website, this piece of privacy information 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 this activity, which should be considered as her privacy. However, "weight loss", as a searching keyword, is not personally related to Zhu and cannot identify Zhu. Therefore, searching keywords are not personal data. However, the court does not consider whether Baidu may have collected

other information from Zhu, such as her location, her search habit, etc. The court improperly ignores 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 Provisions on the Protection of Personal information of Telecommunications and Internet Users (hereinafter "Provisions") enacted by China Ministry of Industry and Information Technology in September 2013. Its Article 4 of defines "user's personal data" as (1) the user name, date of birth, ID number, address, telephone number, account number and password, etc 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" can identify an individual user. However, the *Ye Zhu* court dismisses the application of Article 4 without a clear reason. The second definition of personal data can be found in Article 67 (5) of 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, phone number, etc. Chinese Cybersecurity Law was enacted by the Standing Committee of National People's Congress and came into effect in June 2017. This is after *Ye Zhu* was decided. The definition of personal data in *Ye Zhu* is inconsistent with Chinese Cybersecurity Law, as personal data is the information, alone or jointly with other information, can be used to identify a data subject. The third definition can be found in Information Security Technology---Personal Information Security Specification (hereinafter "Personal Information Security Specification") made jointly by the State Administration of Quality Supervision, Inspection

and Quarantine and China National Standardization Administration.[81] It came into effect in May 2018. Its 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 be able to identity a particular natural person. Among the three definitions, the one provided by the Chinese Cybersecurity Law is the most authoritative. The Chinese Cybersecurity Law is enacted by the Standing Committee of National People's Congress, which is at a much higher hierarchy compared with the bodies enacted the other two regulations. Chinese Cybersecurity Law is also a more recent legislation compared with the Provisions. Personal Information Security Specification is made later in time compared with Chinese Cybersecurity Law. However, Personal Information Security Specification is not a law. It serves as guidance of best practice for the industry. Its foreword provides that, if these Specifications contradict with law, the latter should prevail. Therefore, the definition under the Cybersecurity Law--- that requires personal information, alone and in combination with other information, should be able to identify a particular nature person---represents the prevailing view in China.

1.2. 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, California Consumer Privacy Act of 2018 explicitly provides that "it is the intent of the Legislature to further Californian's right to

[81] Information Security Technology---Personal Information Security Specification made jointly by the State Administration of Quality Supervision, Inspection and Quarantine and China National Standardization Administration, GB/T 25069-2010.
[82] White House, Consumer Data Privacy in a Networked World, page 5 (Feb. 2012) indicates "personal data fuels an advertising marketplace that brings many online services and sources of content to consumers for free." Sally Chapman, *Consumer Data Privacy in a Networked World*, HOMELAND SECURITY DIGITAL LIBRARY (2012), https://www.hsdl.org/c/consumer-data-privacy-in-a-networked-world/ (last visited Sep 10, 2019).

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 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 to personal data breach. 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 case that a business operator infringes consumers' personal information, the Administrative Department for Industry and Commerce or other

[83] Title 1.81.5, the California Consumer Privacy Act of 2018, section 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; (5) The right of Californians to equal service and price, even if they exercise their privacy rights.
[84] California Consumer Privacy Act of 2018, 1798.125 (b).
[85] Federal Trade Commission Act, 15 U.S.C. §§ 41–58.
[86] Shawn Marie Boyne, *Data Protection in the United States*, 66 AM. J. COMP. LAW 299–343, 301 (2018). Ieuan Jolly, *Data Protection in the United States: Overview*, Thompson Reuters Practical law (July 1, 2016), https://content.next.westlaw.com/6-502-0467?transition Type=Default&contextData= (last visited November 9, 2019).
[87] Art. 29 of Chinese Consumer Law [Xiaofeizhe Quanyi Baofu Fa], promulgated by the Standing Committee of the National People's Congress on 31 October 1993 and most recently amended on 25 October 2013.
[88] *Id.*
[89] *Id.*

relevant administrative departments shall order corrections, and may, according to the circumstances of the case, impose warnings, confiscate illegal income, and impose a fine.[90] If the circumstances are serious, the operator shall be ordered to suspend business for rectification and revoke the business license.[91]

However, what differs Chinese Consumer Law and its US counterparts 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 at 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 of 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 the annual pass system was updated, and the old system was abolished, now visitors should record their facial features at the Park, and the Park would 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 no refund will be made.[96] The Park explains that using facial recognition system can speed up the Park admission process and saves consumers' waiting time.[97] What is stunning in this case is that a safari park can collect and use facial features of customers as the only way for park admission. Facial features are personal biometric information. They are with a nature person for his or her lifetime and

[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 department should take punishment measures and what measures should be taken, they shall be implemented in accordance with the provisions of the laws and regulations.
[92] The First Facial Recognition Case in China, A Zoon in Hangzhou is sued, available at http://www.xinhuanet.com/legal/2019-11/04/c_1125188289.htm (last visited November 9, 2019).
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*

cannot be changed. Facial features are more sensitive than fingerprints and other personal data because they are exposed outside. For public safety and national security, government law enforcement departments such as the border control and traffic regulation 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.

1.3. Property right

Characterising "personal data" as "property" derives from scientific research on the physical reality of information.[98] It reflects the need to delimitate 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 anonymised 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

[98] Rolf Landauer, *Information is Physical*, 44 Physics Today 23-29 (1991).
[99] Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92 (proposing property rights in personal data as a way to protect privacy).
[100] E.g. 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 ("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.").

further fostered the view that personal data should be characterised 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 operate an online database called "Lvzhuang Wang (female clothing net)". The defendant manages a competing online database "Zhongfu Wang (China clothing net)". Many users who register with the plaintiffs also register with the defendant. Twenty-four users of the defendant 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 valuable clothing dealers' information from the plaintiffs' website. The plaintiffs brought an unfair competition claim against the defendant. The defendant argued that, 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, the IDs and passwords were highly correlated with the

[102] Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, DUKE LAW TECHNOL. REV. 220–277, 221 (2017).
[103] Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property,* 1 Int'l J. L. & Info. Tech. 3, 5-7 (1993- 1994). See Jamie Lund, *Property Rights to Information,* 10 Nw. J. Tech. & Intell. Prop. *1, passim* (2011) (arguing individuals should "enforceable property right" over their own personal information).
[104] One Company in Zhejiang Is Ordered to Pay 350,000 RMB in a Judgment, http://rmfyb.chinacourt.org/paper/html/2019-11/05/content_161872.htm?div=-1, http://www.zjsfgkw.cn/art/2019/11/1/art_56_18812.html (last visited November 9, 2019).
[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 logged in. Many users use the same account password on different websites, so the hacker can try to log in to the B website by obtaining the user's account on the A website.

users' identity authentication, and the property rights 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 (i.e. plaintiffs).

The property-right argument is deeply problematic. In the above case, it is doubtable that a data controller can obtain absolute property rights of 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 subject can provide the same piece of personal data to other data controllers. Nevertheless, the data subjects 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 in protecting the resource that the data subject invested in the process of gathering personal data will not be taken advantage by other competing data controllers.

Further, in the American contexts, the property right theory is criticized because there are strong policy reasons, such as First Amendment civil liberty, against propertizing all personal information.[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. However, such self-determination and control are inconsistent with the Chinese government's digital surveillance

[106] *See, 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).

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 property judicial review and public transparency supervision. Although the proposed Chinese Civil Code provides that the collection and procession 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 to have many basic services in China. For example, Chinese consumers are required to use facial recognition as a 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 to decide the legality of collecting facial biometric information? If consumers do not know what facial information is collected, how to process and where to store, 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.

Because of the limitation of applying property law to personal data, can personal data be considered as a copyright in the contexts 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

---

[107] See 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.")
[108] Arts. 813 to 817 of the Proposed Chinese Civil Code.
[109] China Due to Introduce Face Scans for Mobile Users, https://www.bbc.com/news/world-asia-china-50587098 (last visited April 2, 2020). From Travel and Retail to Banking, China's Facial Recognition Systems are Becoming Part of Daily Life, https://www.scmp.com/tech/social-gadgets/article/2132465/travel-and-retail-banking-chinas-facial-recognition-systems-are, (last visited April 2, 2020).
[110] Samuelson, *supra* note 43 at 1138.
[111] e.g. Gianclaudio Malgieri, *"Ownership" of Customer (big) Data in the European Union: Quasi-Property as Comparative Solution?*, 20 J. INTERNET LAW N. Y. 3, 3–6 (2016).

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 U.S. also concluded that it is difficult to justify copyright protection unless sufficient creativity exists in the development of databases of factual information.[114]

2. Spread-out unilateral applicable law approach

After finishing characterization, the first stage of conflict-of-laws analysis, we should move to the second stage which is to identify connecting factors. The US, EU, and China either adopts connecting factors leading to the law of the forum or considers its data protection law as a 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.

[112] *Id.*
[113] *Shanghai Hantao Information Consultation Co v Aibang Juxin (Beijing) Technology Co*., Beijing Haidian People's Court, (2010) Hai Min Chu Zi No. 4253.
[114] *Feist Publ'ns, Inc. v Rural Telephone Serv. Co*., 499 U.S. 340, 363 (1991).

2.1. *Lex fori* based on connecting factors and mandatory law of the forum

The year of 2019 has witnessed numerous seminars on topics "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 goes beyond the traditional ones for natural persons such as habitual residence or active citizenship. Article 4.2 of the GDPR provides that it applies if the offering of free or paid goods or services to the data subject who is in the EU.[116] This condition is fulfilled if the controller/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 target EU customers.[117] The GDPR also applies if the data subject's behaviour is monitored so far as their behaviour takes place in the EU.[118] This broad territorial scope enables 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 Californian 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

[115] E.g. A panel discussion at IAPP ANZ Summit 2019, 29-30 October Sydney Australia.
[116] Art. 3.2 of the GDPR.
[117] *Id.*, Recital 23.
[118] *Id.*, art. 3.2 of the GDPR. 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.*, Recital 24.
[119] Paul Voigt and Axel von dem Bussche, *Scope of Application of the GDPR* (Paul Voigt and Axel von dem Bussche eds, Springer International Publishing 2017) 21–22.
[120] Deborah Thoren-Peden and Catherine Meyer, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa. *Watson v Employer Liability Corp*. 348 U.S. 66 (1954) 72 (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.")

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 criticised that the thresholds of 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 more California resident consumers can benefit from the Consumer Privacy Act.

Chinese Cyber Security Law provides for personal data protection.[123] Its Article 2 states that the construction, operation, maintenance, and use of networks, as well 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 China.[127] The Safety Assessment Guide for

[121] California Consumer Privacy Act § 1798.140 (c).
[122] Brenda Stoltz, *A New California Privacy Law Could Affect Every U.S. Business—Will You Be Ready?*, FORBES , https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy-act-could-affect-your-business/ (last visited September 10, 2019).
[123] Arts 41 to 44 of China Cyber Security Law, promulgated on 7 November 2016 and effective on 1 June 2017.
[124] *Id.* art 2.
[125] Art. 3 of Provisions on Online Protection of Children's Personal Information, promulgated on 22 August 2019 and effective on 1 October 2019, Decree No. 4 of the Cyberspace Administration of China.
[126] Arts. 3.2 and 3.6 of Safety Assessment Guide for Data Transferred outside of China (Second Draft for Public Comments) published on 25 August 2017 by National Information Security Standardization Technical Committee of Chinese government.
[127] *Id.* art. 3.6 of Safety Assessment Guide for Data Transferred outside of China (Second Draft for Public Comments) provides that "processing" means any operations on personal information and important data, including collecting, saving, accessing, revising, transferring, publishing, anonymizing, de-labelling, retrieval, erasure, destruction, etc.

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 personality right is a person's habitual residence.[129] In 2012, the Supreme People's Court issued a judicial interpretation 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 follow 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 releasing of personal information, this law should be applied because it is a mandatory law and consequently foreign laws should be excluded. Applying to the COVID-19 case discussed in the first paragraph of this paper, although that lady's habitual residence is Australia, Australian law should not be applied because Chinese

[128] The Safety Assessment Guide for Personal Data Transferred outside of China (Draft for Public Comments in 2019) published on 13 June 2019 by Cyberspace Administration of China.
[129] Art. 15 of the Law of the Application of Law for Foreign-related Civil Relations of China, adopted at the 17th session of the Standing Committee of the 11th National People's Congress on 28 October 2010 and effective on 1 April 2011, No. 36 Order of the President of the People's Republic of China.
[130] Art. 10 of the 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 on 28 December 2012 and effective on 1 July 2013, Fa Shi [2012] No. 24.
[131] *Id.*

law for COVID-19 is a mandatory law. On 4 February 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 travellers whose habitual residence are not in China. However, if a law for personal information protection has nothing to do with protecting public health, 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 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.

2.2. 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 2.1. The contract between a data controller and a processor is not a consumer contract. However, 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.

[132] Notification on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control of Disease, promulgated and effective on 4 February 2020 by the China Central Cyber Security and Informatization Commission.
[133] Art. 10 of the 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 on 28 December 2012 and effective on 1 July 2013, Fa Shi [2012] No. 24.
[134] Para 40 of Recital of GDPR. Art. 26 of Data Protection Directive.

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 Slovakia[138] 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 (hereinafter "CJEU") held that "in the context of the activities of an establishment" should be broadly interpreted.[139] More specifically, the concept of "establishment" emphasises the effective and real exercise of activity through stable arrangements. Within this construction, the legal form of such an establishment (e.g. 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

[135] Art. 3.1 of the GDPR.
[136] *Id.*
[137] Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639.
[138] Weltimmo did not carry out any activity in its place of registration and often changed its registered office from one state to another.
[139] C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317, para 53.
[140] Recital 19 of the preamble to Data Protection Directive. Judgment in *Google Spain and Google*, para 48.
[141] *Weltimmo*, Case C-230/14.
[142] C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, EU: C:2003:596, para 25, and *Google Spain and Google*, C-131/12, para 26.
[143] *Google Spain and Google*, C-131/12.

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 the 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, 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 only be disclose to overseas processor located in a jurisdiction recognised by the EU as a jurisdiction to offer equivalent data protection law. In the case of outsourcing to a country without equivalent data protection law to the EU, 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 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

[144] *Id.*
[145] Art. 46 of GDPR. Art. 26.2 of Data Protection Directive.
[146] *Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany.* 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*, (2013) 3 INTERNATIONAL DATA PRIVACY LAW 210, 210-212.

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 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 or engage an independent organization to conduct a safety assessment.[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 entrust party is not allowed to transfer the commission.[149]

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

[147] Art. 17 of the Provisions on Online Protection of Children's Personal Information.
[148] *Id.*, art. 16.
[149] *Id*.

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.

2.3. 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 UK and other common wealth 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 a breach of personal privacy that was framed as a breach of confidence claim'.[150] Traditionally, both principle and the balance of Anglo-Australian authority favoured the general application of the *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 unauthorised publication of the Douglas' wedding photos in the UK. Subsequent to Michael Douglas and Catherine Zeta-Jones' wedding in New York, a member of the paparazzi took unauthorised photos of this wedding and sold them to Hello! Magazine. The couple claimed 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 occurred,[153] this argument was effectively rejected by the Court of Appeal, who instead applied the English

[150] *Giller v Procopets* (2008) 24 VR 1, 29 [133] (Ashley JA).
[151] *Wimborne* (1978) 5 BPR [97 423], 24 (Holland J).
[152] *Murakami v Wiryadi & Ors* [2010] NSWCA 7.
[153] *Douglas v Hello!* [2006] QB 125, 160 (Lord Phillips for the Court). Art. 10 of Rome II Regulation.

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 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.

3. De-Americanisation 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 factor 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-Americanisation movement. The relationship between Internet data corporate giants and states need 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 (especially data) industry has moved from Americanisation to de-Americanisation. This was triggered by the combination of legislative and non-legislative approaches in the EU and China. Iconic

[154] In this case, the Court also considered whether the action should be characterised as a tort and acknowledged that it was "shoehorning" the claim into an equity claim.
[155] Ben Chen, *Historical Foundations of Choice of Law in Fiduciary Obligations*, 10 J. PRIV. INT. LAW 171, 187 (2014).
[156] E.g. Douglas Michael, *Characterisation of Breach of Confidence as a Privacy Tort in Private International Law*, 41 UNSW LAW J. 490, 509 (2018).
[157] See Houston Putnam Lowry, *Transborder Data Flow: Public and Private International Law Aspects*, 6 HOUST. J. INT. LAW 159, 170 (1983).
[158] See Christopher Whytock, *Litigation, Arbitration, and the Transnational Shadow of Law*, 18 DUKE J. COMP. INT. LAW 449, 449–475 (2008).

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.

3.1. Americanisation

Professor Jack M. Balkin indicates "[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, to identify the law that would apply to protect personal data collected by the company. The US data regulatory environment features in 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*

---

[159] Jack 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* (2019) https://en.wikipedia.org/w/index.php?title=List_of_largest_Internet_companies&oldid=914808498 (last visited September 10, 2019).
[161] Richard Peltz-Steele, *The New American Privacy*, 44 GEO J INTL L 365, 383 (2013).
[162] Rita S. Heimes, *Privacy and Innovation: Information as Property and the Impact on Data Subjects Symposium Issue: What Stays in Vegas*, N. ENGL. LAW REV. 649, 663 (2014).
[163] Boyne, *supra* note 86 at 305.
[164] ANUPAM CHANDER, *THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD TOGETHER IN COMMERCE* 57-58 (Yale University Press, 2013).
[165] UTA KOHL, JURISDICTION AND THE INTERNET: REGULATORY COMPETENCE OVER ONLINE ACTIVITY 201 (2007).

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 recognisable and enforceable in violating 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 (hereinafter "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]

[166] *LICRA & UEJF v Yahoo! Inc & Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000).
[167] *Yahoo! Inc v La Ligue Contre le Racisme et l'Antisemitisme,* 169 F. Supp. 2d 1181 (N.D.Cal. 2001).
[168] Upon the UEJF and LICRA's appeal, the US Court of Appeals for the Ninth Circuit held that the District Court lacked jurisdiction, and it ultimately decided to rehear the case *en banc* and reversed the District Court's judgment, remanded the case with directions to dismiss the action on 12 January 2006. *Yahoo! Inc, v. LICRA and UEJF*, 433 F 3d 1199 (9th Cir. 2006). The Supreme Court of the US denied LICRA's request to issue a certiorari on 30 May 2006. However, Yahoo! has chosen to remove the sale of Nazi memorabilia from its site entirely.
[169] *Equustek Solutions Inc v Jack* (2014) 374 DLR (4th) 537; *Equustek Solutions Inc v Google Inc* (2015) 386 DLR (4th) 224; see also *Google Inc v Equustek Solutions Inc* [2017] 1 SCR 824. Jennifer Daskal, *Google Inc. v. Equustek Solutions Inc.*, 112 AM. J. INT. LAW 727, 727-33 (2018).
[170] *Google Inc v Equustek Solutions Inc.,* 2017 SCC 34.
[171] SPEECH Act 2010, https://www.congress.gov/111/plaws/publ223/PLAW-111publ223.pdf (last visited November 9, 2019).

3.2. De-Americanisation

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

3.2.1. EU

Although subject to criticism, GDPR may commence the Europeanisation of data protection law,[172] and symbolises the global trend of de-Americanisation of data industry regulations.[173]

The EU harmonises 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 harmonised 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 GDRP rather than the E-commerce Directive.[177] Also

[172] Orla Lynskey, *The 'Europeanisation' of Data Protection Law*, 19 CAMB. YEARB. EUR. LEG. STUD. 252, 252–286 (2017).
[173] Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. LAW 411, 460–461 (2011).
[174] Directive 95/46/EC, consideration (9).
[175] Paul 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).
[176] For Italian courts, see Corte di Cassazione, Cass. sez. tre Penale, 3 febbraio 2014, n. 5107/14 (It.). For French courts, see Sophie Stalla-Bourdillon, Data Protection and Intermediary liability: how do the French do it? https://inforrm.org/2017/04/24/data-protection-abd-intermediary-liability-how-do-the-french-do-it-sophie-stalla-bourdillon/ (last visited November 9, 2019).
[177] Art. 83(5) of GDPR.

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 GDPR applies to the processing of personal data in the context of COVID-19.[179] 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 consent of individuals.[180]

Secondly, 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 imposes high-standard data protection law equivalent to the EU.[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 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 entered into legally binding conventions or instruments relating to the protection of personal data.[184] The adequacy decision is not a final decision.

---

[178] Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY J. INT. LAW 297, 371–374 (2018). See *Mosley v. Google Inc*., [2015] EWHC (QB) 59 [45]-[46].
[179] Statement on the Processing of Personal Data in the Context of the Covid-19 Outbreak, adopted by the European Data Protection Board on 19 March 2020.
[180] *Id.*
[181] Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 J. INT. ECON. LAW 769, 775–777 (2018).
[182] Art. 45. 2 (a) of GDPR.
[183] *Id.* art. 45. 2 (b).
[184] *Id.*, art. 45. 2 (c).

The European Commission should conduct a periodic review at least quadrennially,[185] and monitor developments in countries that receive a positive adequacy decision.[186]

Besides 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 live-streamed the massacre at the first mosque on his Facebook page. The attacks killed 51 people.[188] According to § 230 of the Communications Decency Act (hereinafter "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, and 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

---

[185] *Id.*, art. 45. 3.
[186] *Id.*, art. 45. 4.
[187] Christchurch Shootings Mark 'Unprecedented Act of Violence', New Zealand Prime Minister Jacinda Ardern Says, https://www.abc.net.au/news/2019-03-15/christchurch-shootings-unprecedented-pm-jacinda-ardern-says/10904950 (last visited November 9, 2019).
[188] *Id.*
[189] 47 U.S. Code § 230. 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 TULANE J. TECHNOL. INTELLECT. PROP. 1, 3 (2017).
[190] See *Force v Facebook. Inc*., 2019 WL3432818 (2d Cir. July 31, 2019) (in this case, based on CDA §230, the court rejected 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 terrorists').
[191] Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online https://www.christchurchcall.com/ (last visited November 9, 2019).
[192] Christchurch Call Document, https://www.scribd.com/document/410178195/Christchurch-Call-Document#from_embed (last visited November 9, 2019).
[193] *Id.*

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 GDPR and other legislations, the Christchurch Call represents a non-legislative approach, which is increasingly used to obtain compliance of US Internet giants.[196] An important difference between legislations and non-legislative approach is the latter can circumvent the difficulties of enforcing foreign judgments under the SPEECH Act in the US.[197] This is because 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 only enforced in the judgment-rendering state.[199] If it is not recognizable and enforceable in the state where the companies is domiciled (e.g. the US), its efficacy is limited. Its global impact is further limited by the insufficient international mechanism for recognition and enforcement of judgments.[200]

4.2.2. China

[194] Among 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.
[195] E.g. Amazon, Dailymotion, Facebook, Google, Microsoft, Qwant, Twitter, YouTube. 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 LAW REV. 1035, 1041–1045 (2018) (discussing using the non-legislative approach such as code of conduct and blacklist database to seek industrial compliance.)
[197] *Id.* at 1056.
[198] *Id.*
[199] *Id.*
[200] Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters has not come into effect https://www.hcch.net/en/instruments/conventions/status-table/?cid=137; Convention of 30 June 2005 on Choice of Court Agreements has been ratified by 32 countries (most of them are European countries), https://www.hcch.net/en/instruments/conventions/status-table/?cid=98 (last visited April 2, 2020).

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

The first is the US Huawei ban.[201] Huawei is a Chinese leading 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 case of non-compliance. Although the Huawei ban was issued by the US government, it has led to a broad snow-ball effect to largely preclude Huawei from the global supply chain. As a

[201] Sean Keane, Huawei Ban: Full Timeline as It Posts Smallest Profit Increases in 3 Years, https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-p40/ (last visited April 2, 2020).
[202] *Id.*
[203] Sonam Sheth, Trump Declares a National Emergency, Which Could Set Up a Huge Blow to China's Huawei, https://www.businessinsider.com.au/trump-national-emergency-china-huawei-2019-5, (last visited November 9, 2019).
[204] Victoria 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, https://www.dailymail.co.uk/sciencetech/article-7057889/EE-switch-5G-network-month-sale-Huawei-devices-paused.html (last visited 2 April 2020).
[205] Huawei: ARM memo tells staff to stop working with China's tech giant, https://www.bbc.com/news/technology-48363772, (last visited November 9, 2019).
[206] Adam Satariano, Raymond Zhong, Daisuke Wakabayashi, Google, Intel and other US companies Stop Supplying Huawei, https://cn.nytimes.com/business/20190521/google-huawei-android/, (last visited November 9, 2019).
[207] Japan just Followed, Two Big Telecommunication Companies Announced Unlimited Postpone of Launchingf Huawei Mobile Phone, https://new.qq.com/omn/20190523/20190523A0RRJU.html (last visited November 9, 2019).

consequence, the Huawei Ban may cause private companies in non-US allies to join the digital sovereign campaigns. Previously, the digital sovereignty claim was mostly promoted by states such as China and Russia rather than private technology companies.[208] It 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 crystalise private companies in non-US allies in order to move towards the digital sovereignty campaigns. This is because it teaches a vivid lesson to them: 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. Therefore, the Huawei Ban will promote the de-Americanisation of data industry regulations.

The second incident is the global pandemic COVID-19. As discussed in Section 2.1, 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 travellers 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

[208] Jack Margolin, *Russia, China, and the Push for "Digital Sovereignty"*, IPI GLOBAL OBSERVATORY (2016), https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/ (last visited August 13, 2019).
[209] Cybersecurity Law of the People's Republic of China [Zhonghua Renmin Gongheguo Wangluo Anquan Fa], as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016, Art. 1.
[210] Notification on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control of Disease, promulgated and effective on 4 February 2020 by the China Central Cyber Security and Informatization Commission.

the consent of the person being collected.[211] Where laws and administrative regulations provide otherwise, they shall be implemented accordingly.[212] The collection 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, home address, etc. without the consent of the person being collected, except for the joint disease defence and control work.[216] All personal information used should be desensitized and anonymized.[217] Therefore, Chinese media violated this Notification in the COVID-19 case discussed in the first paragraph of the paper, 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 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 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 relevant

[211] *Id.* art. 1.
[212] *Id.*
[213] *Id.* art. 2.
[214] *Id.*
[215] *Id.* art. 3.
[216] *Id.*
[217] *Id.*
[218] *Id.* art. 6.

crimes according to law.[219] However, Chinese authority has not done anything to remedy the personal information violation caused to the lady discussed in the first paragraph of this paper. 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 GDPR can cause a fine 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 breach can lead to a fine up to ten times of 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 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 spread to the rest of world, Chinese media have begun to publish articles criticizing the US as the origin of the disease since March 2020.[223] It is not the intention of this paper to discuss what is the origin of COVID-19 and who should be liable. The point is 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.

4. Dynamics among Trends

[219] *Id.*
[220] A list of fines and notices issued under the GDPR can be found at https://en.wikipedia.org/wiki/GDPR_fines_and_notices.
[221] Art. 64 of Chinese Cyber Security Law.
[222] Evidence is Confirmed that Virus is found at Huanan Fish Market, http://finance.sina.com.cn/7x24/2020-01-23/doc-iihnzahk6049908.shtml. Lancet Published Chinese Scholar's Comment: the Relationship between Novel Coronavirus and Consumption Wild Animals, https://m.chinanews.com/wap/detail/zw/sh/2020/02-12/9087971.shtml (last visited April 2, 2020).
[223] E.g. Where does COVID-19 Come from? Chinese Academy of Sciences Published a Paper Telling You the "Truth", https://news.china.com/zw/news/13000776/20200301/37852321_all.html (last visited April 2, 2020).

Three trends have emerged at the 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-Americanisation 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 right to protect personal data fosters the spread-out unilateral applicable law approach. Consequently, de-Americanisation 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 interest 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 block 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-Americanisation.

At the micro level, if we look into each individual trend, what becomes apparent is that the divergent laws adopted by each jurisdiction in that trend are actually not reconcilable. The typical example is the industry self-regulation of personal data in the US that conflicts with the laws in China and the EU which clearly push for more government regulations (i.e. de-

Americanisation). However, in the de-Americanisation 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.

5. Conclusions

As German Chancellor Angela Merkel indicated at the Harvard University 368th Commencement Ceremony on May 30, 2019: "are 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 travellers 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 traveller was illegally released by Chinese media, the paper identifies three trends have emerged at each stage: the multi-faceted legal nature of right to protect personal data, the spread-out unilateral applicable law approach, and the de-Americanisation 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] However, due to the spread-out unilateral applicable law approach and consequent lesser possibility of applying foreign law, the importance of choice of laws significantly decreases in cases of transnational personal data

[224] MARTIN DAVIES, ANDREW BELL & PAUL LE GAY BRERETON, NYGH'S CONFLICT OF LAWS IN AUSTRALIA 306–310 (9th ed. 2014).

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 organisations, a feasible priority is to achieve regional coordination or interoperation among states with similar values on personal data protection.