The Conceptual Barrier to Comparative Study and International Harmonisation of Data Protection Law

Li YANG[*] and Min YAN[**]

Although cross-border data flows are becoming increasingly important and prevalent, there is not yet an international legal framework for data protection. The current lack of international legal harmonisation on data protection has created compliance burdens and risks for companies that rely on cross-border data to operate and may also erode the effectiveness of data protection systems that have been established in jurisdictions like the European Union. This article draws attention to a conceptual barrier to comparative study and international harmonisation of data protection law, namely the divergent conceptions of privacy across different societies and the intricate relations between data protection and privacy. Considering the complications and difficulties caused by the conceptual barrier, this article suggests that data protection and privacy are better understood as interrelated but distinct concepts for the sake of comparative legal research. Such a distinction not only provides the possibility for comparative researchers to construct a relatively ideologically and culturally neutral theoretical framework for understanding data protection law, thereby facilitating the widely desired international harmonisation of data protection standards, but also gives data protection legal discourse the flexibility to consider and to address broader values that are imperilled by ubiquitous data processing in today's information age.

1. Introduction

In today's information age, cross-border data access, usage and exchange are essential to economic development.[1] Almost every sector — from technology to finance and from manufacturing and service to retail — relies on data and its transborder flow.[2] Together with the advancement of data-intensive technologies, such as cloud computing, artificial intelligence (AI),

[*] *Dr Li Yang* is a Postdoctoral Researcher at the Dickson Poon School of Law, King's College London, UK.
[**] Corresponding author. *Dr Min Yan* is an Associate Professor in Business Law and Director of *BSc. Business with Law Programme* at Queen Mary University of London, UK; he is also a Jinshan Distinguished Visiting Professor of Law at Jiangsu University, China. Email: m.yan@qmul.ac.uk. The authors wish to thank the anonymous reviewers for their helpful comments on the earlier version of this paper. The usual disclaimers apply.

[1] Paul M Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law" (2017) 106 *Georgetown Law Journal* 115, 117. It is stated that international data transfers are "the life blood of the digital economy".
[2] See Joshua P Meltzer and Peter Lovelock, "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia" (2018) 113 *Global Economy and Development Working Paper*. Paul M Schwartz, "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment" *The Privacy Projects Org* (2009). McKinsey Global Institute, "Global Data Flows in a Digital Age: How Trade, Finance, People and Data Connect the World Economy" (April 2014), available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Globalization/Global%20flows%20in%20a%20digital%20age/Global_flows_in_a_digital_age_Full_report%20March_2015.pdf (accessed 1 June 2021).

the internet of things and blockchain, the importance of cross-border data flows is increasing.[3] Moreover, unlike decades ago when data flows happened in the form of "point-to-point transmissions" and via senders' explicit intent, today's transborder data flows often "occur as part of a networked series of processes" involving multiple partners and sometimes even without the sender being aware of the transfer.[4]

Given the prevalence and growing importance of cross-border data flows, since the mid-2000s, several entities in both the private and the public sectors have called for an international legal framework for data protection. For example, in 2005, the 27th International Conference of Data Protection and Privacy Commissioners issued the "Montreux Declaration", which advocated that governments and international organisations develop a universal convention for protection of individuals' personal data. Among others, it highlighted the concern that "the absence of data protection safeguards in some places undermines effective global data protection".[5] A similar appeal was also made at the United Nations-sponsored World Summit on the Information Society in 2005 and the 30th International Conference of Data Protection and Privacy Commissioners in 2008.[6] The European Union (EU)'s Article 29 Data Protection Working Party expressly echoed these appeals in 2009. It acknowledged, in an official document, that, given the fact that transborder data flows "are becoming the rule rather than exception", "global standards regarding data protection are becoming indispensable" for facilitating transborder data flows and "ensuring a high level of protection of data when they are transferred and proceed in third countries".[7] More recently, in the World Economic Forum in Davos in 2019, German Chancellor Angela Merkel specifically stressed the importance of "international oversight of data usage".[8] Some private sector entities also made similar appeals. For instance, Peter Fleischer, Google's Global Privacy Counsel, publicly pleaded for the establishment of global privacy standards.[9] Similarly, John Suffolk, the Global Cyber Security and Privacy Officer of Huawei, a China-headquartered multinational technology company, stated: "… [T]he more we can agree international standards, the more we can agree a common

---

3 The World Economic Forum, "A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy" (June 2020), available at https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy (accessed 1 June 2021).

4 For example, the internet of things (such as personal wearable devices and smart home appliances) routinely involves international transfer of data to manufacturers and application providers without the direct involvement of a human being. Likewise, the architecture of cloud computing means that even a transfer to a party in the same country may result in the message or file transiting to other countries. Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013) pp 2–3.

5 International Conference of Data Protection and Privacy Commissioners, "The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities" (Montreux Declaration) (16 September 2005), available at https://www.refworld.org/docid/435914f74.html (accessed 1 June 2021).

6 Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects" (2009) 4 *Computer Law & Security Review* 307, 307–308.

7 Article 29 Data Protection Working Party, "The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data" (1 December 2009) 10, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf (accessed 1 June 2021).

8 See Keith Bradsher and Katrin Bennhold, "World Leaders at Davos Call for Global Rule on Tech" *The New York Times* (23 January 2019), available at https://www.nytimes.com/2019/01/23/technology/world-economic-forum-data-controls.html (accessed 1 June 2021). Noteworthy, in the same forum, China's Vice President Wang Qishan agreed the need for more coordination in oversight of the tech sector, but "did not mention personal privacy" at all.

9 See Peter Fleischer, "Call for Global Privacy Standards" *Google Public Policy Blog* (14 September 2007), available at http://googlepublicpolicy.blogspot.co.uk/2007/09/call-for-global-privacy-standards.html (accessed 1 June 2021).

approach to verification, the more we'll collectively drive through the challenges that we all have with cyber security".[10]

Despite the shared desire for harmonisation, there is, as yet, no international legal framework for data protection.[11] The current lack of harmonisation on data protection standards creates an enormous compliance burden and uncertainty for companies and also risks eroding the effectiveness of advanced data protection systems such as the EU's data protection law.[12] This article draws attention to an understated conceptual barrier to the comparative legal research on data protection: the unbridgeable divergence on the conceptions of privacy across different societies and the intricate relations between data protection and privacy.

It is commonly accepted that the right to privacy is the foundational, if not the sole, value for data protection laws to protect.[13] The EU Data Protection Directive, for example, declares at the outset: "[T]he object of the national laws on the processing of personal data is to protect fundamental rights and freedom, notably the right to privacy".[14] The US approach seems more straightforward as it directly includes the term "privacy" in the title of the statutes.[15] In a similar vein, many other jurisdictions, such as New Zealand,[16] Hong Kong[17] and Australia,[18] all named their law for data protection as either the "Privacy Act" or "Information Privacy Act". Moreover, European Courts, in particular the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), have repeatedly referred to a fundamental right to privacy when deciding cases concerning protection of individuals' personal data.[19]

Such a prevailing understanding equating data protection with privacy protection might, however, cause serious confusion and difficulties to comparative legal research on data protection law, since the concept of privacy might be interpreted differently in different societies. Without acknowledging and addressing such conceptual divergences, legal transplant or global

---

10 While the article used the term "cyber security" in the title, John Suffolk's talk and the content of the video go beyond cybersecurity and mention several times protection of customers' data. See John Suffolk, "Huawei Calls for Common International Cyber Security Standards" *Huawei.com* (13 October 2013), available at https://www.huawei.com/uk/about-huawei-tobedeleted/cyber-security/related-content/hw_310623 (accessed 10 March 2019).

11 W Gregory Voss, "Cross-Border Data Flows, the GDPR, and Data Governance" (2020) 29 *Washington International Law Journal* 485, 489–493.

12 *Ibid*. See also Christopher Kuner, "The European Union and the Search for an International Data Protection Framework" (2014) 2 *Groningen Journal of International Law* 55, 55–56. It is noted that "companies are frustrated by the lack of harmonisation", whereas data protection authorities must allocate some of their limited resources to deal with complex questions that occur in other regions. Bo Zhao and Weiquan Chen, "Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Exterritorial Application in China" (2019) 16 *US-China Law Review* 97, 103. It is indicated that, despite the good intentions of GDPR and wide extraterritorial jurisdiction in theory, "the harsh reality is that the EU law cannot protect EU citizens' personal data in most important jurisdictions outside the EU".

13 All the norms and similar rules later emerging in Europe were to be formally designated as constituting "data protection" laws and officially ascribed to the objective of serving, primarily, something called "privacy". Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014) pp 21–54. Likewise, Bennett noted that all English-speaking nations have retained the word privacy to add appeal to statutes that essentially perform the same functions as the European data protection laws. Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992) p 13.

14 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 (EU Data Protection Directive 1995), Recital 10.

15 Privacy Act of 1974 (US).

16 Privacy Act 1993 (New Zealand).

17 Personal Data (Privacy) Ordinance 1995 (Hong Kong).

18 Privacy Act 1988 (Australia).

19 See Lee A Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties" (1998) 6 *International Journal of Law and Information Technology* 247; Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action" in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009) pp 3–44.

harmonisation of data protection law would be very difficult, if not impossible. Moreover, by constantly grouping the concepts of privacy and data protection with the ideology and institutions of liberal democracy, the prevailing view in the West may also create resistance from governments without the typical democratic political system. The impeding effect of the conceptual and ideological barriers is particularly acute in the case of China. This is not only because China is a non-Western society governed by a one-party government (thus suffering from a double impediment), but also because, as an emerging superpower and the world's second-largest economy, China is less likely to make compromises to "Brussels effects" and to adopt a regulatory model which it conceives as unfit or even dangerous for its own social and political environments. Hence, this article discusses transnational divergences on the concept of privacy, investigating their implications on the comparative legal research and international harmonisation of data protection law. This article will use China, probably the most affected jurisdiction, as an example to illustrate such conceptual barriers.

The remainder of the article is organised as follows. Section 2 considers the complications and difficulties for comparative legal research caused by the unbridgeable divergences on conceptions of privacy across different societies. Even within the Western liberal-democratic sphere, there are persistent disagreements and controversies regarding the concept of privacy. Section 3 therefore focuses on the conceptual divergence between the EU and the United States, as well as the intricate relationship between privacy and data protection in EU law. After that, Section 4 uses China as a case to illustrate the conceptual barrier and its implication on data protection development in a non-Western society. Section 5 then highlights the ideological collision between China and the West regarding data protection law, and thereby the importance of an ideologically neutral theoretical framework for understanding data protection law. The concluding remarks are provided in Section 6.

2. Conceptual Dilemmas in General

While privacy is widely regarded as the foundational value underpinning data protection legislation, the conception of privacy varies greatly among different societies, which leads to scepticism about the transferability of data protection laws. Accordingly, despite the EU's continued efforts to promote its data protection model worldwide, it is questionable whether the same legal model can be adopted to protect a conception of privacy that is formed in a very different social, political and cultural context.[20]

As Charles Ess pointed out, in order to set up a concrete common basis for global comparison and communication regarding privacy, comparative researchers "must develop a careful and detailed understanding of both similarities and distinctive differences between

[20] For example, some Chinese scholars have argued that the "tensions" between "Western theories of privacy" and the societal "reality" that the Chinese legal system faces are "particularly problematic" for privacy laws, because "both forces are based on strong, and sometimes conflicting value systems". See Tiffany Li, Zhou Zhou and Jill Bronfman, "Saving Face: Unfolding the Screen of Chinese Privacy Law" (2018) *Journal of Law, Information, and Science* 1, 12. Likewise, American scholar James Whitman has commented that, given the fact that Americans and Europeans have different cultures of privacy and different intuitive sensibilities about privacy violations, it is "hogwash" to declare that "American privacy law has 'failed' while European privacy law has 'succussed'". James Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004) *113 Yale Law Journal* 1151, 1160.

Western and Eastern conceptions and assumptions".[21] Likewise, Ronald Krotoszynski contends that it is essential to first reach an agreement "on the discrete interests that fall under the rubrics of privacy" before seeking to establish a global framework for privacy protection.[22] Indeed, if privacy is understood as the foundational or sole value underlying data protection law, a transnational consensus on the concept of privacy would be a prerequisite for international harmonisation of data protection regulation.[23]

Yet it is extremely difficult to identify all the similarities and differences concerning different concepts of privacy across various societies, let alone develop a universally applicable concept of privacy for comparative studies. For example, Ess states that Western concepts of privacy are quite alien to China, Japan, Thailand and other Asian countries, due to the different cultural, historical, religious and philosophical traditions.[24] It is not only mistaken but also "dangerously misleading" to assume that "'privacy' in Asian contexts directly translates Western notions".[25] Ess therefore urges more comparative research on the concept of privacy. In his opinion, this is at the heart of global comparison and communication of data protection law.[26]

However, given the immense discrepancies in the concept of privacy across different societies, this article is sceptical that a successful resolution can be reached through comparative work on the issue. For instance, a Thai scholar has pointed out that most scholars agree that the Western concept of privacy is not applicable to Thai social reality, as Thailand's society is deeply shaped by the ideologies of collectivism, "face" culture, Buddhism and social hierarchy.[27] Specifically, whereas the concept of privacy was ostensibly assimilated into Thai culture in the nineteenth century, this concept is collectivistic rather than individualistic, as the privacy is "shared by intimate members of the same household" rather than being individual.[28] Also, the main justification in favour of privacy in Thailand is the traditional value of "saving face";[29] accordingly, interference in "private affairs" is acceptable, and even welcome, when conducted with the purpose of "saving face".[30] Researches focusing on Thai people's awareness of privacy in digital contexts have made similar observations. One study shows that, interviewees mostly regard privacy as "a luxury for the upper social status" even in the more urban parts of the country.[31] In the latest research in 2021, the author concedes that many participants "still do not fully understand just what information privacy is about".[32]

Likewise in Japan, it is acknowledged that the concept of privacy contains "only some aspects of the Western concept of privacy" and does not include "the 'individualistic' perspective that ascribes privacy to the dignity of the person".[33] Moreover, this partially

---

21 Charles Ess, "'Lost in Translation'? Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)" (2005) 7 *Ethics and Information Technology* 1, 5.
22 Ronald Krotoszynski, *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (OUP, 2016) p 2.
23 *Ibid*.
24 *Ess* (n 21 above) p 4.
25 *Ibid*., p 5.
26 *Ibid*., p 6.
27 Krisana Kitiyadisai, "Privacy Rights and Protection: Foreign Values in the Modern Thai Context" (2005) 7 *Ethics and Information Technology* 17, 17.
28 *Ibid*., p 18.
29 "Face" represents one's social and professional position, reputation and self-image in a group or society; in the collective culture, "a loss of face is to be prevented and avoided at all costs". *Ibid*.
30 *Ibid*., p 19.
31 Pirongrong Ramasoota and Sopark Panichpapiboon, "Online Privacy in Thailand: Public and Strategic Awareness" (2014) 23 *Journal of Law, Information and Science* 97, 114.
32 Charnsak Srisawatsakul and Waransanang Boontarig, "An Assessment of Privacy Concerns on Personal Health Information: Thailand Case Study" (2021) 21 *Current Applied Science and Technology* 774, 786.
33 Rafael Capurro, "Privacy: An Intercultural Perspective" (2005) 7 *Ethics and Information Technology* 37, 46.

imported concept of privacy is blended in a very complicated way with the Buddhist tradition of *musi* ("denial of subjectivity")[34] and traditional values such as the notion of *aida* ("in-between human beings").[35] Consequently, individual privacy can be easily overridden by other traditional values of Japanese society. A study in Japan reveals that the publication of homicide victims' extremely detailed private information is acceptable,[36] because it is considered necessary for the community to have a better understanding of the meaning of the homicide and the network of relationships (emphasised in the notion of *aida*).[37] Also, the privacy novel is a very popular genre in Japan, as it is believed that to intentionally express or betray one's sinful inner mind, that is, to voluntarily surrender one's privacy, is a way to self-purify and to be saved by Buddha.[38]

Apart from conceptual discrepancies regarding privacy in the Western–Asian context, privacy as a notion also does not function in African philosophical thinking.[39] *Ubuntu*, a sophisticated set of life philosophies and dominant world view in Africa, sees the welfare of a group or community as more important than the welfare of any single individual.[40] This stands in sharp contrast to Western cultures, which emphasise individualism and personal autonomy.[41] Consequently individual privacy, a key ethical value in Western countries, is not a priority for either individuals or communities in African societies.[42] A study with a specific focus on Ethiopia's privacy protection affirms this conclusion.[43]

The aforementioned transnational discrepancies and complications concerning the concept of privacy can be further complicated by considering the dynamics of a society's perception of privacy.[44] No wonder that Luciano Floridi remarked: "No one would find it

---

34 While the self in the Western world is considered the most precious thing people have and thus requires protection, in Japan, the self is something that "should be denied, not protected". *Ibid*., p 42.

35 *Ibid*., pp 38–46. It is argued that as Japanese morality stresses the value of community and the dimension of in-between human beings (*aida*), the Japanese conception of privacy is "community oriented"; furthermore, due to the influence of *musi*, private things are widely considered as less worthy than public things in Japan.

36 Makoto Nakada and Takanori Tamura, "Japanese Conceptions of Privacy: An Intercultural Perspective" (2005) 7 *Ethics and Information Technology* 27, 30. The two Japanese scholars concluded that "one thing is clear: privacy is not something like 'intrinsic good' … for us".

37 *Ibid*., p 35.

38 *Ibid*., p 30.

39 Hanno Olinger, Johannes Britz and Martin Olivier, "Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa" (2007) 39 *The International Information & Library Review* 31–43; Alex Boniface Makulilo, "Privacy and Data Protection in Africa: A State of the Art" (2012) 2 *International Data Privacy Law* 163, 172.

40 Olinger, Britz and Olivier (n 39 above) pp 34–35.

41 *Ibid*., p 34. The strong collective thinking of Ubuntu means that individuals "cannot imagine ordering their lives individualistically without the consent of their family, clan or tribe". To respond to the new information technologies that impose risks on the crowd as opposed to identifiable individuals, some Western scholars have, in recent years, added a new collective/group dimension to the traditional understanding of privacy that focuses on individuals. For example, see Linnet Taylor, Luciano Floridi and Bart Van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer, 2016). However, this Western collective privacy that aims to expand and strengthen the protection for individual privacy must not be confused with collective cultures which privilege communities and groups over individuals.

42 Olinger, Britz and Olivier (n 39 above) pp 35–36. It is argued that "the culture of transparency and openness in Ubuntu would not understand the need for privacy or be able to justify it"; on the contrary, privacy in Ubuntu societies would be interpreted as "the Ubuntu individual is trying to hide something", adversely implicating "the good of the community".

43 Although there are some legislations in Ethiopia relating to privacy, "it would be by no means an exaggeration to claim that there does not seem to exist much interest in privacy in Ethiopia". Kinfe Micheal Yilma, "Data Privacy Law and Practice in Ethiopia" (2015) 5 *International Data Privacy Law* 177, 179.

44 Lee A Bygrave, "Privacy and Data Protection in an International Perspective" (2010) 56 *Scandinavian Studies in Law* 165, 174.

reasonable to compare, for example, Eastern and French cuisine",[45] implying that the transnational comparison of the concept of privacy would be at least as baffling and intricate as comparing the cuisine of two countries. Not surprisingly, despite its vital importance, little progress has been made on developing a globally acceptable concept of privacy. Krotoszynsk attempted to facilitate the creation of "a global system of privacy protection" by examining the constitutional protection of privacy in different jurisdictions.[46] Yet four of the five jurisdictions considered in Krotoszynsk's book share "common legal genealogies" and all five jurisdictions share broadly similar commitments to Western liberal democracy.[47] Moreover, while intending to assist the development of a global data protection system, the book did not answer this key question: What should, or could, the concept of privacy be in the global context?[48] Likewise, Graham Greenleaf's influential monograph on Asian data protection laws, though admitting the relevance of local cultural values, does not discuss the differences between Western and Asian concepts of privacy and states that the book "is not a sociological study".[49]

Floridi suggests adopting a more constructive approach to the concept of privacy in a transnational context, looking for "those common and invariant traits that unify all humanity at all times and in all places", as opposed to the unbridgeable discrepancies.[50] This suggestion appears valid: it seems reasonable to posit that we can identify at least some elements or levels of privacy in almost all societies, such as sexual intimacy, coverage of genitals, safeguarding of the home and sealing of personal correspondence. In fact, much ethnographic literature has affirmed this presumption. For example, it is argued that at least the desire for some level of privacy is a "panhuman trait".[51] Likewise, one study indicated that even in societies with minimal privacy, such as in the Mehinacu and Javanese cultures, there exist certain mechanisms to control interaction with others, which may imply that some desire for privacy regulation is universal.[52]

Yet Floridi's seemingly constructive and evidence-based suggestion overlooks another crisis confronting data protection law: jurists in Western jurisdictions, especially the EU, have made admirable efforts to stretch the concept of privacy to include as many data protection problems as possible, which otherwise would fall outside its scope.[53] According to the decisions made by the ECtHR and CJEU, the traditional notion of privacy defined as intimacy has been expanded significantly to embrace "development of interpersonal relationship", "certain facts occurred in public sphere" and some data subject rights.[54] In other words, while there are voices that suggest, from a transnational perspective, downplaying the discrepancies among different concepts of privacy to increase the chance of transnational consensus, the data protection legal discourse in Western jurisdictions has been heading in the opposite direction. In this sense, comparative research on data protection law is now between a rock and a hard place. On the one

---

45 Luciano Floridi, "Four Challenges for a Theory of Informational Privacy" (2006) 8 *Ethics and Information Technology* 109, 113.
46 Krotoszynski (n 22 above).
47 Joe Purshouse, "Privacy Revisited: A Global Perspective on the Right to Be Left Alone. By Ronald J. Krotoszynski, Jr" (2017) 76 *Cambridge Law Journal* 449, 449.
48 *Ibid*.
49 Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (OUP, 2014) p 18.
50 Floridi (n 45 above).
51 Barrington Moore, *Privacy: Studies in Social and Cultural History: Studies in Social and Cultural History* (Routledge, 1984) p 276.
52 Irwin Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33 *Journal of Social Issues* 66, 84.
53 The tendency in Western legal discourse to deliberately expand the concept of privacy to tackle data protection issues has its own problems. See Paul De Hert and Serge Gutwirth. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power" (2006) *Privacy and the Criminal Law* 61, 91.
54 De Hert and Gutwirth (n 19 above) pp 15–20.

hand, if, for the sake of international data protection coordination and harmonisation, research downplays the differences among markedly divergent concepts of privacy in different countries and cultures, this would hamper the efforts of Western jurisdictions to stretch the elasticity of privacy to tackle increasingly complicated data protection issues. On the other hand, if it follows the current trend of expanding the concept of privacy in a transnational context, a Western-formulated and broadly defined concept of privacy may not be acceptable or applicable in non-Western societies.

To sum up, whereas privacy is conventionally considered as the foundational value underlying data protection law, concepts of privacy in Asian and African cultures diverge significantly from those of the West in terms of subject, scope and underlying justification. Moreover, privacy in the non-Western context is often regarded as alien and of relatively low priority, when compared to other traditional values.[55] Such conceptual divergences not only raise questions regarding the transferability of Western data protection experiences (in particular, the EU data protection model) but also indicate a gloomy future for the international harmonisation of data protection law.[56] Admittedly, some non-Western countries have already followed the EU and are on track to enact EU-style data protection laws, despite the conceptual divergences.[57] Yet the problem in those cases is that if the public only has a narrow perception and limited interest in privacy,[58] and the legislatures only have a vague comprehension of the concept of privacy (ie, the foundational value underpinning the data protection law), can they ensure that such legal institution will be genuinely accepted and implemented,[59] rather than becoming just a piece of handsome legislation on paper?[60]

---

55 It is argued that privacy and individualism "remain outside of the lists of the most important values for Japanese". Nakada and Tamura (n 36 above) p 31.

56 As Krotoszynski conceded, while understanding how different societies conceptualise and define privacy would seem "a necessary prerequisite to prosing a global system of privacy protection", "significant differences in both local understandings and practices will make finding a global consensus on privacy rights very difficult to achieve—perhaps even impossible". Krotoszynski (n 22 above) p xi.

57 See Michael D Birnhack, "The EU Data Protection Directive: An Engine of a Global Regime" (2008) 24 *Computer Law & Security Review* 508, 520.

58 Ess (n 21 above) p 4; Capurro (n 33 above) p 46. It is argued that Eastern countries and many African cultures "give privacy at least partly a negative connotation". For more discussion, see Section 2 above.

59 As Arora argued, "The notion of GDPR as a golden and global standard is commendable. However, regulations are meaningless without enforcement. … We cannot serve a global data regulation without a shared privacy culture". Payal Arora, "General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South" (2019) 17 *Surveillance & Society* 717, 724.

60 While several Asian jurisdictions have adopted data protection legislation following the enactment of the EU Data Protection Directive in 1995, much of the legislation is either deficiently drafted or not properly enforced. For example, "the Philippines" Act is "enacted as 'window dressing'" for foreign-trade consumption, rather than having much to do with improving the human rights of Filipinos; the Malaysian Act "has very limited scope, and an extremely defective and limited method of enforcement" and the Act in Singapore is characterised by "the excessively limited scope and generally minimalist content". Greenleaf (n 49 above) pp 352, 334 and 315. Hong Kong, as "Asia's leader in data privacy", is characterised by "strong principles" but overly "cautious enforcement". See Graham Greenleaf, "Hong Kong Data Privacy 2015: Cautious Enforcement, Strong Principles" (2015) 138 *Privacy Laws & Business International Report* 21, 23; Anne SY Cheung, "An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995–2012)" (2013) 3 *International Data Privacy Law* 29, 31. More recently, in January 2019, the European Commission adopted its adequacy decision on Japan, recognising Japan's newly reformed Act on the Protection of Personal Information as providing an "equivalent" level of protection to the EU GDPR. However, the enforceability and effectiveness of the laws remains to be seen. In effect, it is indicated that despite the adequacy decision, "disparate concepts of data privacy" determine that the Japanese data protection law mainly "emphasizes the economic importance of data as an economic commodity and protects a narrower range of personal information". See Flora Y Wang, "Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan Adequacy Agreement" (2020) 33 *Harvard Journal of Law & Technology* 661, 668–669. Likewise, Greenleaf has criticised the EU's Adequacy Decision on Japan, stating that it lacked sufficient justification; among other problems, Greenleaf highlighted that Japan's enforcement and redress seem to only exist on paper and are not demonstrated in practice. Further, the supplementary rules of the law that offer a higher level of protection apply only to

3. Conceptual Disarray in the West

Even when looking only at the Western liberal-democratic sphere, where data protection law first arose, considerable disagreement exists between the EU and the United States regarding the concept of privacy. As James Whitman rightly points out, "We must acknowledge that … there are, on the two sides of Atlantic, two different cultures of privacy … which have produced two significantly different laws of privacy".[61] Likewise, Capurro argued that "we westerners seem to live simultaneously in different worlds according to different traditions that partly overlap and partly contradict themselves . . . this is particularly the case when we take into account the differences between Europe — which is again an oversimplification![62] — and the United States".[63] While it might be tempting to attribute all the differences to the fact that privacy is a notoriously slippery and complicated concept, the EU–US disagreements and ongoing controversies only serve to deepen the confusion of researchers and legislators from non-Western jurisdictions regarding the definition and purpose of privacy.[64]

3.1 Conceptual Divergence between the EU and the United States

While the EU repeatedly emphasises that privacy is a fundamental right, the United States seems to be very sceptical on this point, as many distinguished US scholars have expressed. For instance, Helen Nissenbaum has argued that, although many brilliant works defend privacy as a fundamental right by linking it to other values with long-standing moral, political and legal pedigrees, these works suffer the shortcoming of leaving a "gap" between the "ground" (namely, "interest brawls") and the "heavens" (namely, "universal human values and moral and political principles").[65] That is to say, regarding privacy as a fundamental right does little to help tackle the real challenges, where conflicting acts can also appeal to higher-order values and principles, such as national security, personal autonomy, freedom of speech and free-market economy. Julie Cohen has revealed a paradox of the European concept of fundamental right to privacy, arguing that "if privacy is a fundamental right, it cannot be socially constructed; if privacy is socially constructed, it cannot be a fundamental right".[66] As Peter Swire conceded, "[T]he current dominant position … is that the US rejects the fundamental rights approach".[67]

Certain aspects of privacy are indeed protected under the US constitutional system. For instance, the First Amendment offers protection for anonymous expression, the Third

---

personal data originally obtained from the EU, but not personal data sourced from Japan and other jurisdictions. Graham Greenleaf, "Japan: EU Adequacy Discounted" (2018) 155 *Privacy Laws & Business International Report* 8, 8.

61 Whitman (n 20 above) p 1160.

62 There are, for example, notable differences between the United Kingdom and the other EU member states in terms of their attitudes towards the right to privacy. See Krotoszynski (n 22 above) pp 120–141.

63 Capurro (n 33 above) p 46.

64 Simon Chesterman, "After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012" [2012] *Singapore Journal of Legal Studies* 391, 392. It is argued that the "largely unsuccessful efforts to produce a coherent theory of privacy" were partly "because of distinct visions of privacy" in the United States and European Union; "the lack of a strong theory of what privacy is", in turn, undermines "the coherence of any legal regime" of data protection.

65 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009) pp 9–10.

66 Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012) p 19.

67 Peter Swire, "Peter Hustinx and Three Clichés about EU-US Data Privacy" in Hielke Hijmans and Herke Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust?: Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004–2014)* (Intersentia, 2014) p 195.

Amendment protects against soldiers quartering private homes without consent of the owner during peacetime, the Fourth Amendment safeguards against unreasonable government seizures and searches (including warrantless wiretapping), and the Due Process Clauses of the Fifth and Fourteenth Amendments protect decisional autonomy and, arguably,[68] information privacy.[69] However, the constitutional protection of privacy in the United States is limited in several respects. First, unlike the European fundamental right that has a horizontal effect and is applicable to both government and non-government actors, the US constitutional rights are "characterized by negative rights against the state".[70] This means that the constitutional protections for privacy do not apply to relations that are purely between private entities and individuals.[71] Likewise, US governments, unlike their European counterparts, are not obliged to take positive steps (such as adopting specialised legislations) to secure privacy more broadly in society.[72] Privacy rules against private entities are not mandated by the US Constitution, instead they are considered as a part of consumer protection law and "lower in the American system".[73]

Second, the "deep-seated commitment to the free expression" implies that the constitutional protection for privacy in the United States is further restricted.[74] Admittedly, in Europe, freedom of expression is also explicitly safeguarded by the European Convention on Human Rights (ECHR)[75] and the EU Charter of Fundamental Rights.[76] However, in the United States, freedom of expression is enriched in the First Amendment, which means that it is not subject to proportionality analysis. If a court finds the First Amendment right is at stake, strict scrutiny usually applies.[77] As a result, in US jurisprudence privacy almost always loses out to freedom of expression.[78] It is clear that the EU and the United States have a "different metric" when "accommodating the rights of speech and press, on the one hand, and the right of privacy, on the other".[79] In the United States, privacy is not as prioritised as it is in the EU.[80]

There are also obvious disparities between the United States and Europe concerning the boundary or scope of privacy. As Whitman maintained, there are "unmistakable differences in

---

68 In *Whalen v Roe* 429 US 589 (1977), the Supreme Court recognised that the line of substantive due process cases protects two different kinds of privacy interests, namely, "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions". Then in *Nixon v Administration of General Services* 422 US 425 (1977), the Court concluded that President Nixon had a constitutional privacy interest in records of his private communications with his family but not in records involving his official duty. However, in the next decades, the Supreme Court did little to develop the Constitutional right to information privacy. It is argued that "both its extent and its reach remain uncertain". The Supreme Court's decision in *National Aeronautics and Space Administration v Nelson* 131 SCt 746 (2011) further aggravated the confusion. The Court held that "[w]e assume, without deciding that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*", whereas Justices Thomas and Scalia stated in a concurrence that "[a] federal Constitutional right to 'information privacy' does not exist". See more detail in Daniel Solove and Paul Schwartz, *Information Privacy Law* (Wolters Kluwer, 2011) pp 503–510; Schwartz and Peifer (n 1 above) p 133.

69 Woodrow Hartzog, and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection" (2020) 61 *Boston College Law Review* 1687, 1727.

70 *Ibid*., p 1728.

71 *Ibid*.

72 Schwartz and Peifer (n 1 above) p 132.

73 Hartzog and Richards (n 69 above) pp 1728–1729.

74 *Ibid*.

75 The European Convention on Human Rights 1953 art 10.

76 The Charter of Fundamental Rights of the European Union 2000 art 11.

77 Hartzog and Richards (n 69 above) p 1730.

78 *Ibid*. It is noted that "the Supreme Court's First Amendment jurisprudence … has been consistent in elevating the protection of free speech over privacy interests". Krotoszynski (n 22 above) pp 17, 29.

79 W Gregory Voss, "Obstacles to Transatlantic Harmonization of Data Privacy Law in Context" [2019] *University of Illinois Journal of Law, Technology & Policy* 405, 463.

80 It is argued that "even in circumstances when the Frist Amendment would not stand in the way", the US legal and political cultures have been reluctant to provide privacy protections. Krotoszynski (n 22 above) p 22.

sensibility" between Americans and Europeans "about what ought to be kept 'private'".[81] In terms of law, it is noted that the right to privacy in the United States has a significantly narrower scope of application than in EU jurisprudence.[82] For instance, whereas EU jurisprudence has repeatedly acknowledged the principle of being "private while in public", in the United States, when a person voluntarily enters a public space, they are generally considered to lack a reasonable expectation of privacy and thus can hardly claim for legal protection against privacy disclosure.[83] It is also "nonsensical", from an American perspective, that "a reasonable expectation of privacy could exist in a police station or a jail cell".[84] Furthermore, in contrast to EU jurisprudence, which believes that all persons in principle enjoy a right to privacy, in the United States, the status of an individual as a public official, a public figure or a person involved in matters of public concern determines that legal protection of their right to privacy is significantly diminished.[85]

In addition, there is also a transatlantic gulf regarding the justification of privacy. As Whitman famously argued, "[C]ontinental (European) privacy protections are, at their core, a form of protection of a right to respect and personal dignity", whereas "America … is much more oriented towards values of liberty, and especially the liberty against the state".[86] Some scholars have stated that there are more resemblances than divergences between Europe and the United States on the issue. For instance, Francesca Bignami asserts that "privacy law in Europe also protects liberty" in some respects.[87] This argument is undoubtedly valid. However, as Whitman contended, although there are some important resemblances to privacy protection across the Atlantic, it is often the relative differences that matter most in comparative law.[88] Krotoszynski also expressed a similar opinion in his monograph on comparative privacy.[89]

In effect, it can be argued that it is this dominant American understanding of privacy as liberty against the state, together with the influence of neoliberalism in the United States,[90] that largely explains the current lack of data protection regulation in the US private sector. At almost the same time as the European countries enacted their first-generation data protection laws, the US Congress enacted the Federal Privacy Act of 1974 to regulate federal agencies' processing of personal information. However, up until now, the regulation of the private sector in the United States still primarily relies on a collection of narrowly focused sectoral laws and industry self-regulation.[91] This legal *status quo* in the United States can be attributed, at least in part, to the American understanding of privacy as liberty against the state. Accordingly, the major threat to

---

81 Whitman (n 20 above) p 1154.
82 Krotoszynski (n 22 above) p 151.
83 *Ibid*., p 152.
84 *Ibid*., p 153.
85 Lior Jacob Strahilevitz, "Toward a Positive Theory of Privacy Law" (2012) 126 *Harvard Law Review* 2010, 2042.
86 Whitman (n 20 above). See also Lee A Bygrave, "International Agreements to Protect Personal Data" in James Rule and Graham William Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar, 2010) p 16.
87 Francesca Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining" (2007) 48 *Boston College Law Review* 609, 612.
88 Whitman (n 20 above) pp 1151–1221.
89 Krotoszynski (n 22 above) p 36. It is argued that although there has been "a shared commitment" to protect privacy as an important value, "significant cultural and legal differences between the US and Europe" make transatlantic harmonisation very difficult.
90 The influence of neoliberalism entrenches the US legislature's preference for a market-oriented approach to data protection in the private sector. See Paul M Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States" (1995) 80 *Iowa Law Review* 553, 618. Voss (n 79 above) pp 432–439.
91 Ryan Moshell, "And then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection" (2004) 37 *Texas Tech Law Review* 357–432; Shawn Marie Boyne, "Data Protection in the United States" (2018) 66 *American Journal of Comparative Law* 299, 343.

privacy is considered to be the state, as opposed to private-sector enterprises.[92] Many American scholars have asserted that to assign to the state the role of protecting privacy in the private sector is like "entrusting the fox to protect the chicken",[93] whereas a market-based approach and industry self-regulation seem to be a more sensible way to keep the major threat away.[94] Consequently, "the best care for data protection in the United States" is more likely to be found in the public sector as opposed to the private sector, because the state "requires less justification when governing itself than regulating private activities".[95] Likewise, as Krotoszynski noted, even when US legislative bodies enact statutes to offer privacy protection in non-government sectors, "these statutory rights often lack cultural salience and quickly morph into relatively meaningless forms of legal boilerplate".[96]

For some scholars, all these differences simply confirm the well-known fact that privacy is a slippery and complicated concept. Yet, from the perspective of comparative legal research, the EU and US disagreements and ongoing collisions regarding privacy protection[97] inevitably leave non-Western researchers and legislators confused regarding the meaning of privacy in the Western ideological domain. As acutely summarised by Daniel Solove, a leading US privacy scholar, "[P]rivacy seems to be about everything, and therefore it appears to be nothing".[98] Without knowing what privacy is in its original context, how can developing countries transfer a legal institution claimed to be built upon it and ensure consistency in its implementation?

3.2 Conceptual Uncertainty within the EU

Even within the EU, the relationship between data protection and privacy is not as clear and concrete as some believe it to be. Evidence has been presented to show that the concepts of data protection and privacy in Europe have experienced a long and complicated process of "coupling" but are now undergoing the opposite process, "decoupling".[99] This uncertainty and ambiguity regarding the core concepts of EU data protection law makes comparative studies attempting to comprehend or transfer the EU data protection model particularly difficult.[100]

When various European countries started regulating personal data processing in the 1970s, few associated new regulations with anything resembling privacy.[101] Germany, Sweden and France were the data protection pioneers, which first adopted *ad-hoc* legal acts applicable to the processing of information related to individuals. Nevertheless, none of these pioneering acts held privacy protection as their foundational purpose. For instance, in 1970, the German federal state of Hessen promulgated the world's first data protection law. This law introduced the word *Datenschutz* (data protection) without "any explicit link to any other legal notion except with the

92 It is argued that "in the United States, we tend to think of privacy rights running against state rather than against each other". Krotoszynski (n 22 above) p 23.
93 *Cf.* Amitai Etzioni, "A Communitarian Perspective on Privacy" (2000) 32 *Connecticut Law Review* 897, 900.
94 Privacy is often seen in the United States as "a pre-existing quality whose protection merely requires an absence of state power". Schwartz (n 90 above) p 615.
95 Schwartz (n 90 above) p 555.
96 Krotoszynski (n 22 above) p 23.
97 Voss (n 79 above) pp 408–411.
98 Daniel J Solove, "A Taxonomy of Privacy" (2006) 154 *University of Pennsylvania Law Review* 477, 479; Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006) p xxii.
99 Fuster (n 13 above) p 269.
100 For example, in a comparative study concerning data protection in Africa, a Tanzanian scholar dedicated almost a third of the article to exploring and clarifying the relationship between data protection and privacy within the EU context, prior to the main theme analysis of data protection developments in Africa. See Makulilo (n 39 above) pp 164–167.
101 Fuster (n 13 above) pp 254–257.

wide formula of the legitimate interests of persons".[102] The same applies to the German Federal Data Protection Act enacted in 1977. This Act expressly protected personal data against misuse, aiming to prevent harm to any personal interests that warrant protection.[103] The first European national law regulating automated data processing, the Swedish Data Act 1973, had no connection with privacy either, declaring that its purpose was to prevent undue invasion of personal integrity (*Personlig integritet*) of individuals whose data were registered in data banks. In the report, titled *Data och integritet 1972*, the Swedish parliamentary commission noted that the importance of personal integrity was primarily intended to ensure trust and confidence between the state and citizens.[104] What is more, the French Data Protection Law 1978, instead of resting on privacy alone, embraced a variety of ethical values ranging from human identity and human rights to privacy/private life and individual or public freedoms. In other words, privacy is merely one of the numerous values underpinning the French Data Protection Law, rather than its foundation.[105] The later "coupling" between data protection and privacy — such as the identification of a right to privacy (in the sense of art 8 of the ECHR) as the prime purpose of data protection law by the EU Data Protection Directive and the Convention 108 — is mostly the result of a series of miscommunications that "neglect the fact that existing national rules on data processing had hardly ever been explicitly designed to pursue such target".[106]

Shifting the spotlight from the distant past to the present, the relationship between privacy and data protection remains unclear and continues to evolve. Just as the European data protection supervisor acknowledged in 2014: "We have seen a growing distinction between 'privacy' and 'data protection' as separate concepts" in the EU context.[107]

This statement can be affirmed by the following three facts. To start with, the EU Charter of Fundamental Rights 2000 (hereafter, "the Charter") has a separate provision for the protection of personal data,[108] in parallel with art 7, the right to privacy. Contrary to conventional belief, the Charter expressly recognises that data protection is an autonomous right and therefore cannot be represented by, or interchanged with, the right to privacy. However, the Charter's explanatory memorandum provides little explanation of the reason for the introduction of this right in addition to the pre-existing right to privacy, and how these two rights should interact. What is more, the CJEU has so far not provided direct and concrete orientation as to what "data protection" does mean, although it has had many opportunities to do so since 2000.[109]

Second, basing the right of privacy as the foundation of the current EU data protection law has given rise to increasing scepticism about the legitimacy of the existing data protection legal regime. For instance, it is argued that "few direct manifestations of intimacy-oriented conceptions of privacy can be found in the provisions of data protection laws" and even

---

102 *Ibid*., p 58. For more analysis of the Hessen Data Protection Act, see Frederik Willem Hondius, *Emerging Data Protection in Europe* (North-Holland Publishing, 1975).

103 German Federal Data Protection Act (Bundesdatenschutzgesetz) 1977 s 1.

104 Fuster (n 13 above) p 58.

105 French Act on Data Processing, Data Files and Individual Liberty 1978 art 1.

106 See Fuster (n 13 above) p 255.

107 Peter Hustinx, "European Leadership in Privacy and Data Protection" *European Data Protection Supervisor* (8 September 2014), available at https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/european-leadership-privacy-and-data_en (accessed 1 June 2021). See also Gloria González Fuster and Serge Gutwirth, "Opening up Personal Data Protection: A Conceptual Controversy" (2013) 29 *Computer Law & Security Review* 531–539. It is noted that lately "it is more and more usual to depict the right to privacy and the right to the protection of personal data as separate notions", and the latter is "often regarded as a spin-off of the former, or even, perhaps more graphically, an unwanted child".

108 The Charter of Fundamental Rights of the European Union 2000 art 8.

109 Fuster and Gutwirth (n 107 above) p 537; Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order" (2014) 63 *International & Comparative Law Quarterly* 569, 574.

broadened privacy concepts are "not of a nature to explain data protection principles such as purpose limitation, data quality or security".[110] Moreover, although the EU data protection law expressly applies to any data related to an identified or identifiable person, the case laws have shown that both the ECtHR and CJEU require additional elements in order for personal information to fall within the governing scope of right to privacy.[111] Further, EU data protection law is notably characterised by a series of data subject rights, ranging from the data subject's right of access to data, the right to rectification, the right to object to automated decision-taking, the right to prevent direct-marketing, to the recently introduced right to be forgotten, and the right to data portability.[112] But the right to privacy can uphold only some, rather than all, of the data subject rights, even after the deliberate expansion.[113]

Last, in the General Data Protection Regulation (GDPR),[114] the recent replacement for the EU Data Protection Directive, the reference to privacy has almost disappeared and been replaced by personal data protection. For example, while the EU Data Protection Directive declares, in the article concerning the object of the Directive, that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data",[115] the parallel article of GDPR does not mention privacy. Instead it states that "this regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data".[116] The concepts previously known as "privacy by design" and "privacy impact assessments" have also been supplanted by "data protection by design" and "data protection impact assessments" in the GDPR.[117] In addition, the GDPR also indicates a variety of individual rights and freedoms that may be endangered by personal data processing and data breaches, such as the right against discrimination, and the rights to personal security and financial security.[118]

It is not surprising that both the historical complications and ongoing uncertainty regarding the relationship between data protection and privacy in the EU context lead to confusion or frustration for comparative researchers from developing jurisdictions. In other words, if data protection is distinct from privacy protection, what then are data protection laws designed to achieve? It seems unwise to transfer a novel legal institution without a clear understanding and certainty about what is it for. Even assuming an EU-style data protection law was transferred and enacted, how could the regulatory authorities of the recipient jurisdictions interpret and apply such law in practice without a basic understanding of its legislative purpose and underlying values? It is doubtful that international harmonisation of data protection can be achieved by simply increasing the number of countries that have enacted an EU-style data protection law.

---

110 De Hert and Gutwirth (n 19 above) p 10. Likewise, Bygrave argued that the concept of privacy "fails to capture the entire remit" with which data protection law is concerned. Lee A Bygrave, *Data Privacy Law: An international Perspective* (OUP, 2014) p 28.

111 Juliane Kokott and Christoph Sobotta. "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" (2013) 3 *International Data Privacy Law* 222–228; Maja Brkan, *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar, 2017) pp 10–31; De Hert and Gutwirth (n 19 above) pp 24–26.

112 Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015) pp 127–129.

113 *Ibid*.

114 Regulation (EU) 2016/679 of the European Parliament and 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 (EU General Data Protection Regulation).

115 The EU Data Protection Directive 1995 art 1(1).

116 EU General Data Protection Regulation art 1(2).

117 Fuster (n 13 above) p 244.

118 EU General Data Protection Regulation, Recital 85.

4. The Case of China

China, an emerging economic superpower with the largest population in the world, has been regularly criticised by international privacy advocates for its lack of personal data protection.[119] There is certainly much truth in these criticisms. Until recently, the Chinese legal regime relating to personal data protection remains fragmentary, incoherent and largely ineffective. However, it would be a mistake to assume that the Chinese government is inherently against the idea of data protection and decisively resists all Western data protection approaches. On the contrary, the Chinese central government initiated a data protection law research project as early as 2003, when it commissioned the Chinese Academy of Social Science (CASS) to conduct comprehensive comparative research on data protection legislations worldwide and propose a draft Personal Information Protection Act for official consideration. The resulting draft Personal Information Protection Act, as its accompanying legislative research report explained, drew lessons from many foreign jurisdictions, in particular the EU.[120] In addition, almost at the same time as the CASS comparative law project, the Chinese government also actively participated in a joint project with the EU, the EU–China information society's project, the main purpose of which was to provide Chinese authorities and scholars with information about the EU's legislative experience on data protection.[121]

Yet, despite the Chinese government's initial interest in the EU data protection model, China's data protection regime has evolved in a largely incremental and reactive manner in the passing decade.[122] It was only in August 2021 that the National People's Congress enacted China's first ever Personal Information Protection Act .[123] While it is not yet clear how the general and abstract rules of the new Act will be implemented in practice,[124]the weaknesses of the current Chinese data protection regime, which features scattered supervisory responsibility, [125] lax regulation for public authorities [126] and incoherent legislative objectives,[127] largely persist. Most notably, no unified supervisory system is required to be

119 China will increasingly have a voice on data protection issues, whereas "its message remains to be deciphered, let alone clearly heard" by Western experts. See Bygrave (n 110 above) p 209.

120 Hanhua Zhou, *Expert-suggestion Draft Law on Personal Information Protection of the People's Republic of China and the Research Report* (Law Press, 2006) (周漢華,《中華人民共和國個人信息保護法專家建議稿及立法研究報告》 (法律出版社 2006 年).

121 Xinbao Zhang, "Status Quo of Prospects for Legislation on Protection of Personal data in China" [2007] 2 *China Law Express* 19, 21 (張新寶, "中國個人數據保護立法的現狀與展望" 《中国法律》2007 年第 2 期, 第 21 頁》).

122 For more details about the historical development of China's data protection regime, see Feng Yang, "The Future of China's Personal Data Protection Law: Challenges and Prospects" (2019) 27 *Asia Pacific Law Review* 62, 69–75. Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way between the US and the EU?" (2020) 8 *Penn State Journal of Law and International Affairs* 49, 66–78.

123 Personal Information Protection Act of the People's Republic of China (《中華人民共和國個人信息保護法》) .

124 The Act has only 74 clauses and is due to take effect from 1st November 2021.

125 Unlike EU data protection law, which establishes independent data protection authorities, the current Chinese data protection regime fragments the supervisory responsibility between various administrative authorities in accordance with the specific areas or sectors they regulate. There is no clear boundary between the competences of different administrative authorities. Consequently, it can be very difficult to identify the competent authority, in many cases, both for the aggrieved individuals and the officials in the delegated authorities. The situation is much more complicated in practice, as data often flow across different sectors. This problem is also compounded by the fact that these authorities mostly lack expertise and resources to deal with increasingly complex and new technologies-related data protection breaches. The result is that many authorities oversee data protection enforcement in China, but in practice, no authority can be held accountable.

126 See the discussions in Section 4(b).

127 As several Chinese professors pointed out, there is neither coherent expression in Chinese legislation nor consensus in Chinese legal discourse regarding the legislative purpose for personal data protection. See Guoping Gao and Wenxiang Wang,

established;[128] instead, the new Act merely imposes an obligation on "ultra-large internet platforms" to establish for themselves an "independent" supervisory body composed of external members.[129] The Personal Information Protection Act seems to continue with the existing Chinese regime's commitment to uphold the government's information and communications technology development strategies and the primacy of national security while providing limited legal protection for individuals.[130] Simply put, the newly enacted law remains very different from the EU model that is characterised by high levels of protection in both private and public sectors, an independent supervisory authority, and diverse and rigorous enforcement mechanisms.[131]

The conceptual problem regarding privacy and data protection has played a considerable, if not a dominant, part in changing China's attitudes towards the EU data protection model and dissuading China from lining up with the EU on the issue of data protection. In other words, the conceptual barrier discussed in the foregoing sections can also be identified in the case of China, which is discussed the following sections.

4.1 Chinese privacy as a relatively alien and underappreciated concept

Unlike the EU, where privacy is widely acknowledged as a fundamental right, privacy in China is often regarded as a relatively alien concept and an underappreciated value. Similar to the situations in many other Asian and African countries explored earlier, the concept of privacy has only limited appeal to the Chinese public. Equating data protection with privacy would undermine the domestic driving force stimulating the Chinese government to take more concrete actions in data protection regulation.

As a leading Chinese legal scholar noted at the 39th International Conference of Data Protection and Privacy Commissioners in 2017, "[T]he concept of privacy is virtually non-existent in China's traditional culture".[132] While certain elements of privacy might be incidentally preserved under traditional Chinese culture and norms, such as Chinese Confucianism's request for "secrecy on couple's matters" (夫妻之事不可言) and "concealment between kinfolks" (親親相容隱), the purpose of these norms was to maintain traditional family ethics and social hierarchy and not to protect individuals' privacy.[133] The concept of privacy only emerged in Mainland China in the late twentieth century. Prior to the mid-1980s, there was little academic discussion on privacy and no legal documents or judicial interpretation using the concept of privacy in China.[134] Instead, the traditional Chinese concept of *Yinsi* (shameful and

---

"The Criminal Boundaries for Sale and Provision of Citizens' Personal Information—from the Perspective of Legal Interests/Values Underlying the Crime of Infringements upon Citizens' Personal Information" [2017] 2 *Political Science and Law* 46, 48 (高富平, 王文祥, "出售或提供公民個人信息入罪的邊界──以侵犯公民個人信息罪所保護的法益為視角"《政治與法律》2017 年第 2 期, 第 48 頁). See also Xinbao Zhang, "From Privacy to Personal Information: The Theory of Interest Re-Balance and Regulatory Framework" [2015] 3 *China Legal Science* 38, 44 (張新寶, "從隱私到個人信息: 利益再衡量的理論與制度安排"《中國法學》2015 年第 3 期, 第 44 頁).

128 Personal Information Protection Act (n 123 above) art 60. See also Yang (n 122 above) p 75.

129 Personal Information Protection Act (n 123 above) art 58.

130 Bo Zhao and Yang Feng. "Mapping the Development of China's Data Protection Law: Major Actors, Core Values, and Shifting Power Relations" (2021) 40 *Computer Law & Security Review* 1, 15.

131 *Ibid*., pp 9 and 11; Yang (n 122 above) pp 65–68 and 80.

132 Liming Wang, "Privacy Protection in China: Paths, Characteristics and Issues" (王利明, "中國的隱私保障: 路徑、特徵與問題"), *The 39th International Conference of Data Protection and Privacy Commissioners*, September 2017.

133 *Ibid*.

134 Xinbao Zhang, *The Legal Protection of Right to Privacy* (Qunzhong Press, 1997) (張新寶, 《隱私權的法律保護》(群众出版社 1997 年); Hao Wang, *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China* (Springer, 2011) p 33.

illicit secret, 陰私), a phrase with similar pronunciation and wording to "privacy" (隱私) in Chinese, was repeatedly used in Chinese legal discourse to indicate personal secrets regarding immoral or illegal sexual relations.[135]

As noted, the conception and appreciation of privacy has changed significantly since the 1980s in China, especially among legal professionals.[136] Nevertheless, many ordinary Chinese people still link privacy with *Yinsi* (shameful secret, 陰私).[137] A recent anthropological study by University College London concurs with this observation, concluding that while the debates regarding privacy and social media in Europe and North America are primarily based on "the belief that privacy is a kind of natural condition now threatened by online visibility", in general this belief is not held in China, either traditionally or currently.[138] The study revealed that although people in urban China may have become familiar with the concept of privacy, for those in rural areas privacy is still considered as "a fashionable or Western word".[139] Besides, the anthropologists focusing on industrial sites in China found that factory workers and other working-class people still showed a tendency to link the concept of privacy with illicit and immoral secrets, and a sacrificing of one's privacy is commonly regarded as a way to show strong moral fibre, honesty or emotional closeness.[140] The study also indicates that ordinary Chinese people, as opposed to well-educated Chinese elites, generally regard social media as enhancing rather than threatening their experience of privacy, which is in sharp contrast to ordinary people in the EU or United States.[141]

In a similar vein, Li et al. assert that "saving face", a cultural value underlying the traditional Chinese *Yinsi*, is the main impetus behind privacy protection in today's China and continues to affect the operation and development of Chinese privacy law.[142] Due to the negative connotations associated with privacy in Chinese society, "parties to a dispute over privacy might just let it pass or seek resolution outside of a public forum", thereby avoiding further loss of face and humiliation.[143] What is more, even if the aggrieved individuals choose to resort to legal remedies, Chinese courts are often reluctant to support a privacy claim if the plaintiff's related behaviour challenged the social values that are rooted in traditional Confusion heritage and socialist ideologies.[144]

Chinese businesses tend to support the *status quo* of Chinese data protection law, and the gap between that and Western jurisdictions, by emphasising Chinese people's restricted conception of privacy and its sharp distinction from their Western counterparts. For example, Kai-fu Lee, CEO of a Chinese technology-savvy investment firm and a former executive of Microsoft and Google, has argued that, unlike Westerners, "Chinese internet users are willing and ready to exchange personal privacy for convenience or security" and this "cultural factor"

---

135 For instance, in an article published in 1981 on the *People's Judicatory*, the official journal of the Supreme Court, it was noted that *Yinsi* (陰私) was a commonly known and frequently used concept in Chinese judicial discourse especially in marriage cases. See Hancheng He, "A Marriage Case Is Not Necessarily a Case of Yinsi" [1981] 8 *People's Judicator* 1, 1 (何漢成, "婚姻案件不等於陰私案件" 《人民司法》1981 年第 8 期, 第 1 頁).

136 Yao-Huai Lü, "Privacy and Data Privacy Issues in Contemporary China" (2005) 7 *Ethics and Information Technology* 7, 8.

137 *Ibid*.

138 Daniel Miller et al., *How the World Changed Social Media* (UCL Press, 2016) p 188.

139 *Ibid*., 189.

140 Xinyuan Wang, *Social Media in Industrial China* (UCL Press, 2016) pp 120–124.

141 *Ibid*., pp 5 and 124.

142 Li, Zhou and Bronfman (n 20 above) p 13.

143 *Ibid*., p 10.

144 *Ibid*., p 12; Yang (n 122 above) pp 70–71.

can be a competitive advantage for China in global AI development.[145] Following this logic, it would become both unreasonable and unnecessary for China to line up with Western data protection standards.

Given that the concept of privacy has only a weak appeal or even negative connotations for the Chinese public,[146] it is not surprising that the adoption of comprehensive and rigorous legislation for preserving privacy is not a priority in China. Put differently, the prevailing understanding of data protection law, which equates data protection with privacy protection, unintentionally undermines the impetus for the government to undertake a more active role in data protection legislation and enforcement.

4.2 Chinese privacy as a civil law right

In contrast to the EU, where the right to privacy is a fundamental right, privacy in the Chinese legal system is a civil law right, designed to tackle the legal relationships and conflicts between individuals or between an individual and private sector entities.[147] To equate data protection with privacy may cause complications in the legal context of China, as the nature of Chinese civil right to privacy implies that public authorities can be reasonably and unwittingly exempted from the spotlight of data protection discussions and legislation. Unless Chinese legislators make a deliberate effort to include public authorities, public authorities' data-processing activities will be left to internal supervision and regulation only. In effect, the development trajectory of the Chinese data protection regime has already shown this unfortunate tendency.[148]

Under the current Chinese data protection regime, public authorities appear mainly in the capacity of supervisory bodies rather than data controllers to be regulated.[149] Moreover, the latest

---

145 Tech.qq.com, "Interview with Kaifu Lee: Why China Will Win the Competition of Global Artificial Intelligence" *Tech.qq.com* (17April 2018) (騰訊科技, "專訪李開復:中國為何將贏得全球人工智能的競爭" 騰訊科技 , 2018 年 4 月 17 日), available at https://tech.qq.com/a/20180417/002049.htm (accessed 1 June 2021).

146 See nn 137–143 above. A recent example is that the 2020 *Freshman Safety Knowledge Handbook* of China Academy of Art states that "having privacy and being caught by others" ("懷有隱私,讓人抓住把柄") for female students may increase their own risk of being sexually assaulted. See Xuan Zhu, "Attributing Female Sexual Assault to 'Self-factors' Raises Doubts, China Academy of Art Responds: Investigating" *the paper.cn* (24 September 2020) (朱軒, "將女生受性侵歸咎於 '自身因素'引質疑, 中國美院:正調查" 澎湃新聞, 2020 年 9 月 24 日), available at https://www.thepaper.cn/newsDetail_forward_9324332 (accessed 1 June 2021).

147 There are in fact a few provisions in the Chinese Constitution that might be interpreted as preserving certain elements of privacy. For instance, arts 39 and 40 of the Constitution of the People's Republic of China (《中華人民共和國憲法》), respectively, protect the inviolability of residence, and secrecy and the freedom of correspondence. Nevertheless, none of the constitutional provisions refers to "privacy" or "data protection". While these provisions were included into Chinese Constitution in the early 1980s, the concept of privacy has yet to gain recognition in Chinese legal discourse (see n134–135). What is more, unlike most Western jurisdictions, there is no constitutional court or similar mechanism in the Chinese legal system to acknowledge privacy as a constitutional right. Thus, the idea that privacy is a value already acknowledged by the Chinese Constitution, unfortunately, is just the wishful thinking of a few privacy advocates and optimistic scholars.

148 In the newly released draft Personal Data Protection Act of China (n 123 above), a section is dedicated to the regulation of personal data processing by public authorities (arts 33–37). While it is certainly a welcome move for the Chinese legislature to include public authorities within the governing scope of the draft Personal Data Protection Act, it is too early to celebrate or to say that the Chinese law's long-standing tendency to neglect data protection in the public sector is going to change. For instance, according to the draft Personal Data Protection Act, the legal consequence for a public authority that breaches the data protection rules is that its higher-level agency or a supervisory authority shall order it to correct the issue and the directly responsible people will be subject to internal sanction (art 64). Furthermore, given the fact that the supervisory responsibility remains scattered under the draft Personal Data Protection Act, it is doubtful that the supervisory bodies will have the motivation to spend their limited resources on overseeing or investigating other public authorities in practice. See also n 125 above.

149 It is argued that "what is lacking and in need of urgent legislative action in China is personal information protection in the government sector". Xiuzhe Wang, *Research on Public Law Protection of Individual Right to Privacy in Information Society* (China Democracy and Legal Publishing House 2017) (王秀哲,《信息社會個人隱私權的公法保護研究》(中國民主法制出版社 2017) pp 142–181.

legislative developments, Cybersecurity Law 2017,[150] E-commerce Law 2019[151] and Civil Code 2020,[152] among others, demonstrate the Chinese data protection regime's persistent tendency to focus on regulation of private sector entities. In other words, Chinese public authorities, despite processing and retaining enormous amounts of personal data, are, and probably will continue to be, exempted from data protection regulation in the foreseeable future. This is problematic. As many scholars have indicated, in the age of the information society, governments and private entities have become "surveillant assemblages" in which information constantly and mutually flows across both the public and the private sectors.[153]

Thanks to the conventional understanding of equating data protection with privacy, data protection law as a legal institution to preserve individuals' right to privacy is overwhelmingly regarded as an issue for civil law scholarship in Chinese legal discourse. As is well known, civil law scholars mostly, and understandably, tend to focus on legal relationships between individuals and/or private sector bodies, rather than public authorities.[154] This has resulted in a lack of research and legal discussion about the regulation of public authorities' data processing, which in turn imposes implicit but significant influences on Chinese law's regulatory focus.[155] Moreover, whereas Chinese Civil law has introduced a new right of personal data protection, as an addition to privacy right,[156] this recent move does not overturn the Chinese data protection regime's development trajectory. It has been widely accepted in Chinese legal discourse that personal data protection is a civil law right and therefore should only be tackled by private law, and that consensus, in turn, is based on the prevailing understanding that data protection equals privacy protection and privacy is a private law right in origin.[157]

4.3 Inelastic right to privacy

The right to privacy is only one of the many specific personal rights prescribed in Chinese civil law, which implies that it is not supposed to be seen or utilised as an elastic and far-reaching legal right.[158] While there is a clear trend in Western jurisdictions to stretch the ambit of the right to privacy to tackle increasingly complicated and prevalent data protection issues,[159] an analogous attempt to expand the right to privacy in China not only risks distorting the established personal rights system in Chinese civil law, but it is also out of place with respect to how ordinary Chinese people conceive privacy.

Chinese civil law makes a division between general personal rights (一般人格權) and specific personal rights (具體人格權). The former is an inherently elastic right, purposely

---

150 The Cybersecurity Law of the People's Republic of China (《中華人民共和國網絡安全法》).

151 The E-commerce Law of the People's Republic of China (《中華人民共和國電子商務法》).

152 The Civil Code of the People's Republic of China (《中華人民共和國民法典》) takes effect and replaces the General Provisions of Civil Law from 1 January 2021.

153 Julie E Cohen, "What Privacy Is for" (2012) 126 *Harvard Law Review* 1904, 1916; Kevin Haggerty and Richard Ericson, "The Surveillant Assemblage" (2000) 51 *British Journal of Sociology* 605–620; Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Company, 2016) pp 92–103.

154 Xiaodong Ding, "The Dilemma of Private Law Protection of Personal Information and Solutions [2018] 6 *Chinese Journal of Law* 194, 206 (丁曉東, "個人信息私法保護的困境與出路"《法學研究》2018 年第 6 期, 第 206 頁).

155 *Ibid*.

156 The Civil Code (n 152 above) art 111.Also see the General Provisions of Civil Law of the People's Republic of China (《中華人民共和國民法總則》) art 111 and Chapter 6.

157 Ding (n 154 above) p 195.

158 Liming Wang, "The Redefining of the Concept of Privacy" [2012] 1 *The Jurists* 108, 112 (王利明, "隱私權概念的再界定", 《法學家》2012 年第 1 期, 第 112 頁).

159 In particular, the ECtHR and the CJEU. See Bygrave (n 19 above); De Hert and Gutwirth (n 19 above).

deployed to accommodate any interests that merit civil law protection but do not fit into any enumerated specific personal rights, whereas each specific personal right has its own specified regulatory object.[160] For example, the right to image, as one of the specific personal rights in Chinese civil law, entitles individuals to prevent commercial utilisation of their personal image without consent; the right to name protects individuals' and entities' autonomy to select, use and change their names, as well as prohibits others from appropriating their names; the right to reputation tackles dissemination of false or misleading information about an individual or an entity. To stretch the governing scope of the Chinese right to privacy to encompass all personal data, such as name, image and misleading personal information, would distort the relationship between specific and general personal rights.[161]

The restricted scope of the right to privacy is not only attributable to its status as a specific personal law right in Chinese civil law, but it also reflects the Chinese people's general perception of privacy. As noted by a data protection law professor, the Chinese people do not consider information such as political conviction, religious belief and ethnic group to be related to the idea of privacy.[162] Given the huge mismatch between Western and Chinese conceptions of privacy, this professor suggests defining the boundaries of the Chinese right to privacy by referring to the traditional Chinese concept of *Yinsi* (shameful secret, 陰私), rather than following Western jurisdictions.[163] Such a proposal may sound extreme, but it is a reminder that a comprehensive Western-style right to privacy may not resonate with the Chinese people or gain traction in China. In effect, some leading Chinese scholars who were in favour of a comprehensive right to privacy have also recognised this conceptual mismatch in recent years and have shifted to support a more restricted way of conceptualising privacy rights in China.[164]

Several judicial decisions have affirmed that the right to privacy in China is indeed a restricted one in terms of governing scope. For instance, in *Zhu Yinguang v China United Network Communications*,[165] the court rejected the plaintiff's claim based on the violation of the right to privacy and held that the plaintiff's mobile phone payment records were not deemed a matter of privacy and the disclosure by the defendant telecommunication company thereby did not amount to a breach. Similarly, in *Wang Sujing v Beijing City Branch of China United Network Communications Co, Ltd*,[166] the court refused to regard individuals' contact details *per se* as falling within the scope of the right to privacy, despite acknowledging that certain ways of using individuals' contact details might constitute infringement of one's right to privacy (such as frequent unsolicited calls).[167]

---

160 Lixin Yang and Yin Yan, "On the General Personality Rights and Related Civil Law Protection" [1995] 2 *Hebei Law Science* 6, 6 (楊立新,尹艷, "論一般人格權及其民法保護" 《河北法学》1995 年第 2 期, 第 6 頁).

161 Wang (n 158 above) p 113.

162 See Deliang Liu, "Basic Conceptions in Constructing the Legal Institution of Personal Information" *China Civil and Commercial Law* (7 December 2017) (劉德良, "個人信息法律制度構建的基本觀念" 中國民商法律網 , 2017 年 12 月 1 日), available at http://www.civillaw.com.cn/zt/t/?id=33474 (accessed 1 June 2021).

163 *Ibid*.

164 For instance, see Liming Wang, "New Development in Privacy Right" [2009] 1 *Renmin University Law Review* 3, 18–25. (王利明, "隱私權的新發展", 《人大法律評論》2009 年第 1 期, 第 18–25 頁); Wang (n 158 above) pp 118–119.

165 *Yingguang Zhu v Lianyungang City Branch of China United Network Communications Co., Ltd* (《朱迎光與中國聯合網絡通信有限公司連雲港市分公司、傅紅隱私權糾紛案》) (2014) (連民終字第 0006 號).

166 *Sujing Wang v Beijing City Branch of China United Network Communications Co., Ltd* (《王景素與中國電信北京分公司隱私權糾紛案》 (2017) 京 02 民終 194 號).

167 *Ibid*.

To mitigate the regulatory gap left by the restricted right to privacy,[168] the Chinese General Provisions of Civil Law 2017[169] and the Civil Code 2020[170] create a new right/interest on personal data protection, as an addition to the right to privacy. Nevertheless, as argued earlier, this does not change the issue of the current Chinese data protection regime focusing overwhelmingly on private-sector bodies and leaving personal data processing by public authorities largely unregulated. Most significantly, if data protection is distinct from protection of the right to privacy, what then is personal data protection for?[171] This fundamental weakness of the current Chinese data protection is understated. There is little discussion about why China needs data protection law, which values are to be preserved or what objectives need to be achieved by regulating the processing of personal data in Chinese legal discourse.[172]

The lack of a clear and robust impetus for data protection law in China is detrimental to implementation and development of such a law. A typical example is a recent judicial decision regarding the illegal processing of personal data by Douyin, the Chinese version of TikTok.[173] Although the court in this case acknowledged that the information (ie, name and mobile phone number) collected by Douyin is indeed personal information, and Douyin did not obtain consent from the data subjects as required by law, the court held that Douyin's personal data processing was a reasonable use of personal data. The main justification given by the court was that "data is an important factor of production in the era of digital economy" and "overly absolute protection for personal data" is undesirable for sake of the healthy development of the information industry.[174] In other words, although the regulatory gap caused by the restricted right to privacy has been increasingly recognised in Chinese legal discourse, no alternative framework or value is currently available to justify or to guide personal data protection in Chinese law. As a result, enacted data protection rules might be easily overridden or frequently overlooked in practice. This is particularly true in the cases when other tangible interests, like economic development, governance efficiency and prevention of crimes are involved.

5. The Ideological Collision behind Data Protection

168 See the analysis of the problems of the Chinese approach, which relies on the civil right to privacy to protect personal data: Yuanyang Xie, "Examining the Value of Personal Information from the Perspective of Information Theory—and a Critique of the Data Protection Model via Privacy Protection" [2015] 3 *Tsinghua China Law Review* 94, 94 (謝遠揚, "信息論視角下個人信息的價值—兼對隱私權保護模式的檢討"《清華法學》2015 年第 3 期, 第 94 頁).

169 See n 156 above.

170 See n 152 above.

171 Despite the separation in legislation, Chinese legal discourse about the status of data protection remains unclear: for example, (1) is it a civil right or interest, (2) what is the relationship between the new right/interest and the right to privacy, (3) what are the obligations created by the civil right/interest on data protection, and (4) what is the underlying values/objectives of data protection? Xinbao Zhang, "On the Personal Information Protection Provision in the General Provisions of Civil Law of China" [2019] 1 *Peking University Law Journal* 54, 55 (張新寶, "《民法總則》個人信息保護條文研究"《中外法學》2019 年第 1 期, 第 55 頁). Not surprisingly, privacy and data protection are often referred altogether or interchangeably without distinction in judicial decisions after the enactment of the General Provisions of Civil Law. For example, see *Sijie An v Pingxing Liu and Ju Wang* (《安思傑與劉平興王俊隱私權糾紛案》 (2018) (川 07 民終 2098 號). *Qingdao Tianyi Elite Training School v Qinhui Wang, Intermediate Court of Qin Dao City* (《 青島天一精英人才培訓學校與王慶輝隱私權糾紛案》) (2019) 魯 02 民終 7482 號).

172 See n 127 above.

173 *Ling v Douyin (Beijing Weibo Shijie Tech Ltd.)* (《凌某某訴北京微播視界科技有限公司(抖音)侵權案 》) (2019) (京 0491 民初 6694 號).

174 *Ibid*., 40.

Whereas the concept of privacy and data protection law is constantly grouped, and strongly intertwined, with the values of democracy and liberty in Western legal discourse, China tends to resist these Western ideologies.[175] This largely overlooked ideological incompatibility may have serious implications.[176] On the one hand, it risks irritating countries that don't have Western-style liberal democratic systems, such as China, being a disservice to their people and complicating the prospect for international harmonisation and coordination on data protection regulation.[177] On the other hand, this incompatibility could also be utilised by non-democratic governments as an excuse to dismiss public requests for data protection legislation or to adopt a lax attitude in enforcement. If the ultimate end of the privacy/data protection legislation is to maintain liberal democracy, it may not be needed for jurisdictions where the political system is essentially different.

Scholars frequently advocate the close connection between privacy/data protection and the Western institutions/ideologies of liberal democracy. In the West, privacy is traditionally defined as "a right or interest that citizens possess by virtue of their citizenship within liberal democratic states".[178] Privacy protection is even considered as a factor to distinguish "a democratic society" from "an authoritarian society".[179] Accordingly, data protection law is also seen as having its roots "in more broadly construed liberal democratic thought", rather than being non-ideological.[180] Likewise, it is argued that "concern for privacy tends to be high in societies espousing liberal ideas", which in turn explains why data protection laws are more developed in Western liberal democracies and underdeveloped in most African and Asian countries.[181] It is also commonplace for Western scholarships to regard the importance of privacy in safeguarding the political system of liberal democracy as the principal justification for data protection legislation.[182]

By contrast, the Chinese government has rejected the Western liberal democratic political models, since the establishment of the People's Republic in 1949.[183] China's rise in global

---

175 For further discussion about China's resistance to Western ideologies, see Matthieu Burnay, Joëlle Hivonnet and Kolja Raube, "Bridging the EU-China's Gap on the Rule of Law?" (2016) 14 *Asia Europe Journal* 95–106.

176 As Bygrave argued, "One of the most intriguing aspects of the policy debates in international forums over the last 40 years is that they have largely occurred within the Western, liberal, democratic 'camp'. There has been little serious engagement with the rest of the world specifically on Privacy issues". Bygrave (n 86 above) p 49.

177 As Kahn-Freund argued, among all the environmental forces against transplantation of a foreign law, the political element is the most rigorous resistance in the modern era. See Otto Kahn-Freund, "On Uses and Misuses of Comparative Law" (1974) 37 *Modern Law Review* 1, 11–13. Likewise, Teubner has argued that the "tight coupling" between a legal institution and social fragments peculiar to the foreign jurisdiction will impose "additional difficulties" on the attempted legal transfer, because such a transfer "will not only be confronted with idiosyncrasies of the new legal culture" but also "have to face resistance external to the law". Gunther Teubner, "Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergencies" (1998) 61 *Modern Law Review* 11, 21. Admittedly, the division between liberal democracy and an authoritarian regime is broad brush and overlooks the complexity and distinctions among a wide range of jurisdictions within each camp. However, such a division helps to highlight the ideological collisions that affect data protection regulation in some, although not all, jurisdictions outside Western-style liberal democracies.

178 Bennett and Raab (n 98 above) p xxiv.

179 It is argued that "considerations of privacy protection involve more than any one particular right: they determine the choice between a democratic and an authoritarian society". Spiros Simitis, "Reviewing Privacy in an Information Society" (1987) 135 *University of Pennsylvania Law Review* 707, 734. See also Alan Westin, *Privacy and Freedom* (Ig Publishing, 1968) p 26.

180 Bennett (n 13 above) p 152; Volker Boehme-Neßler, "Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection" (2016) 6 *International Data Privacy Law* 222, 229.

181 Bygrave (n 44 above) pp 175–176.

182 For instance, see C Keith Boone, "Privacy and Community" (1983) 9 *Social Theory and Practice* 1, 25; Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer, 2009) p 45.

183 Perry Keller, "The Protection of Human Dignity under Chinese Law" in Marcus Düwell et al (eds), *The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives* (CUP, 2014) p 414.

economic and political power has strengthened the Chinese government's confidence in its domestic model.[184] While other non-Western countries might be ready to align with the EU regulatory standards, the so-called Brussels effect[185] is significantly constrained when it comes to China.[186] This is particularly evident in the case of data protection legislation, which, as advocated in Western legal discourse, is rooted in and strongly intertwined with the institution and ideology of liberal democracy. It should be borne in mind that "upholding the leadership by the Chinese Communist Party" is one of the "Four Basic Principles" brought forward by the former Chinese leader Deng Xiaoping.[187] It has been always emphasised that the development of the Chinese legal system must rest on the Chinese Communist Party's leadership, which is opposed to the principles of Western liberal democracy. While acknowledging the benefits of learning from foreign jurisdictions, it is stressed that China must not blindly copy foreign legislative ideologies or models.[188]

This ideological incompatibility between China and the West deters the Chinese government from aligning with Western countries on the issue of data protection legislation. This may also cause significant issues for the EU. While EU data protection law expressly bans transfer of data to "third countries" that fail to ensure "an adequate level of protection" of individuals' personal data,[189] enforcing this prohibition against China would cause severe commercial disruption and potentially also political conflicts between the two sides.[190] As indicated in a report for the European Parliament, "if a legalistic approach was adopted, then no common ground could be found between two fundamentally different systems both in their wording and in their *raison d'être*",[191] and so data transfers from the EU to China would need to be prohibited in accordance with EU law. Nevertheless, the report also conceded that "this would be an impractical, if not unnecessary position", given the fact that "China constitutes today a central economic power, a major EU trade partner and substantial global political player".[192]

---

184 *Ibid*.

185 Anu Bradford, "The Brussels Effect" (2012) 107 *Northwestern University Law Review* 1, 68.

186 *Ibid*., 49. It is reckoned that "over time, the EU's regulatory clout may begin to erode as the emerging markets increase in size and affluence of their consumer base".

187 For more discussion, see Min Yan, "Government and Regulation in Promoting Corporate Social Responsibility—the Case of China" (2020) 33 *Columbia Journal of Asian Law* 264, 281.

188 The Central Committee of the Communist Party of China, "Decision of the Central Committee of the Communist Party of China on Several Major Issues in Promoting the Rule of Law" (23 October 2014) (中共中央委員會, "中共中央關於全面推進依法治國若干重大問題的決定", 2014 年 10 月 23 日中共中央第四次全體會議通過), available at http://cpc.people.com.cn/n/2014/1029/c64387-25927606.html (accessed 1 June 2021). China's vigilance and continuing resistance to Western ideological "threats" in Chinese law was evidenced in a speech given by Zhou Qiang, the president of China's Supreme Court, to the presidents of the high courts in 2017: "We must never fall into the trap of the wrong ideologies and judicial independence of the West, and must decisively follow the path of socialist rule of law with Chinese characteristics". Sheng Yu, "Showing a Sword to Wrong Ideological Trends and Preserving Judicial Justice" *People.cn* (17 January 2017) (俞声, "亮劍錯誤思潮維護司法公正", 人民網, 2017 年 1 月 17 日), available at http://opinion.people.com.cn/n1/2017/0117/c1003-29029551.html (accessed 1 June 2021).

189 The EU Data Protection Directive 1995 art 25; the EU General Data Protection Regulation art 44.

190 International data transfers to China may happen under a wide variety of circumstances. See Zhao and Chen (n 12 above) pp 98 and 104. See also Bo Zhao and GP Mifsud Bonnici, "Protecting EU Citizens' Personal Data in China: A Reality or a Fantasy?" (2016) 24 *International Journal of Law and Information Technology* 128, 150.

191 Paul De Hert and Vagelis Papakonstantinou, *The Data Protection Regime in China: In-depth Analysis for the LIBEC Committee* (October 2015), available at http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf (accessed 1 June 2021).

192 *Ibid*., pp 6–8. In the recent *Schrems II judgement*, the European Union has shown a clear and firm stance on the issue of data protection in its confrontation with the United States. However, China is unlikely to concede to the European Union either, especially on an issue that appears to be incompatible with or even threaten its political institution. The Chinese government seems to have anticipated and began preparing for future possible EU action against China. Two recent pieces of evidence support this standpoint: the newly enacted Chinese Personal Information Protection Act (n 123 above) includes a provision, art

This is the *status quo* of the EU's regulation of cross-border data transfer to China, which was reflected in a formal inquiry posed to the European Commission by a group of members of the European Parliament in June 2016.[193] There is no mechanism currently functioning between the EU and China to guarantee that transfers of EU citizens' data to China are compatible with EU requirements on data protection.[194] As a result, protection of EU citizen's personal data is "largely at the mercy of controllers and processors in China" at the moment, and this is particularly true for Chinese entities without a physical presence in the EU.[195]

To be clear, this article does not intend to challenge the argument that privacy and data protection are crucial for the functioning of a liberal democracy, an argument already forcefully elaborated by many distinguished scholars.[196] Nor are we suggesting that European countries should make concessions to the emerging power of China. On the contrary, the point here is to call for a more universally applicable and relatively ideologically neutral theoretical framework to promote broader transnational discussion and harmonisation on data protection. This will ensure that the data protection efforts of Western jurisdictions will not be eroded and, at the same time, will benefit billions of citizens outside of liberal, democratic societies worldwide. Such a framework should be able to encourage countries that endorse political systems other than liberal democracy, such as China, to participate in data protection regulation and, in the meantime, provide the elasticity to accommodate the Western tradition in linking data protection with democracy and liberty.[197]

6. Conclusion

Despite the widely shared ambition for an international legal framework for data protection, the intricate and uncertain relationship between privacy and data protection creates difficulties for global harmonisation of data protection law. This conceptual barrier is at the heart of the

43, empowering Chinese authorities to adopt reciprocal countermeasures against any countries or regions that impose prohibitive or restrictive measures that are discriminatory in their nature against China with respect to personal data protection. In the meantime, China has been promoting its data governance approach (including data protection norms) through the internationally influential Belt and Road Initiatives. Accordingly, scholars argue that there is an emerging "Beijing Effect" in contrast with the "Brussels Effect", as China's influence on data governance norms grows globally, especially in developing countries. See Matthew Steven Erie and Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance" (2021) 54 *New York University Journal of International Law and Politics* (forthcoming).

193 Verónica Miño, "Data Transfers EU–China: The Next Battle?" *datenschutz-notizen.de* (1 July 2016), available at https://www.datenschutz-notizen.de/data-transfers-eu-china-the-next-battle-0815138/ (accessed 1 June 2021). Marc Rotenberg, "Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection" (2020) 26 *European Law Journal* 1, 9. It is noted that while the CJEU invalidated the "Privacy Shield" arrangement between the United States and European Union with the *Schrems II* decision in July 2020, the United States complains that the European Union "doesn't seem to care about misuse of EU citizens' data by Russia or China".

194 *Ibid*.

195 Zhao and Chen (n 12 above) p 112. It is very difficult for EU citizens and EU authorities to find any misuse of EU citizen's personal data taking place in China. Moreover, even if such violations were found, punishments and legal remedies would probably not happen, because Chinese courts generally do not recognise EU courts' decisions. Also see Zhao and Bonnici (n 190 above).

196 Paul Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 *Vanderbilt Law Review* 1607; Cohen (n 153 above).

197 One possible way is to conceive liberal democracy as one of the many essential values that can benefit from data protection in a given society, but not the principal legitimacy nor the necessary social condition for data protection legislation in all countries. It is not the purpose of this article to offer a solution. Within the limited space of this article and given the complexity of the matter, we can only provide the direction for future research. A theoretical framework based on the theories of information society and legal intuitionalism will be developed elsewhere.

comparative study of data protection law. As exhibited, conceptions of privacy diverge significantly across different societies. This raises the question of whether the data protection model and legislative experience in advanced jurisdictions, particularly the EU, are helpful or relevant at all for jurisdictions shaped by different social, political and cultural contexts. While there are recommendations to downplay such discrepancies among the different conceptions of privacy, in order to increase the chance of transnational consensus, this will however compromise the efforts to stretch the concept of privacy to tackle increasingly complicated data protection issues, as we have seen in the Western jurisdictions.

The conceptual difficulty in comparative legal research is further exacerbated by persistent transatlantic disagreements and the changing relationship between privacy and data protection within the EU. In addition, grouping the concept of privacy and data protection with the ideology and institution of liberal democracy has the unintended impact of dissuading governments without the typical democratic political system from accepting such laws. This may further complicate the prospect for international harmonisation and coordination on data protection.

In conclusion, this article highlights the serious complications and difficulties caused by divergent conceptions of privacy and the obscure relationship between privacy and data protection. Instead of equating data protection with privacy, a notoriously contentious and culturally inflected concept, we suggest that data protection and privacy are better understood as interrelated but distinct concepts, for the sake of comparative legal research.[198] Such a distinction would provide the possibility for comparative researchers to explore alternative paths to understanding data protection, other than protection of privacy, and thereby to construct the more universally applicable and relatively ideologically neutral theoretical framework needed for promoting broader transnational discussion and harmonisation on data protection law. It would also give data protection legal discourse worldwide[199] the necessary flexibility to discuss and to address a variety of values that are imperilled by ubiquitous data processing in the information age, no matter whether such values are conceived as relating to privacy in a society.[200]

---

198 As Lyon argued, "[P]rivacy is both contested and confined in its scope. Culturally and historically relative, privacy has limited relevance in some contexts". David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in David Lyon (ed), *Surveillance as Social Sorting* (Routledge, 2005) p 19. It is noted that while scholars tend to discuss the interests to be protected in personal information under the rubric of privacy, "the fact that privacy is an evolving concept, burdened with several definitions, complicates this approach". Patricia Mell, "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness" (1996) 11 *Berkely Technology Law Journal* 1, 8–9.

199 For example, "Vietnamese netizens may view privacy not as a right… It is not their privacy per se that Vietnamese respondents seem to feel is threatened on the internet; it is their wallets and their social capital". Greenleaf (n 49 above) p 364. Likewise, some Thai scholars have indicated that that privacy is often confused with secrecy or certain aspects of urban lifestyles like credit cards, which "only help to make people less aware of the fact that their personal data may be abused". It is believed that to increase Thai people's awareness and interests, it is crucial to link the issue of data protection with "something more fundamental such as health, safety and personal belongs". Ramasoota and Panichpapiboon (n 31 above) pp 114 and 118.

200 Many distinguished scholars have indicated that data protection problems that have emerged in the information age cannot be represented and addressed by privacy. For instance, Zuboff states: "We've entered virgin territory here. The assault on behavioural data is so sweeping that it can no longer be circumscribed by the concept of privacy and its contests". *Cf*. Jonathan Cinnamon, "Social Injustice in Surveillance Capitalism." (2017) 15 *Surveillance & Society* 609, 611. Likewise, Andrejevic argues that the issue at stake is "more than a highly variable, legally contested, and double-edged right to privacy"; there are also problems of "power relations" and "asymmetrical access to information resources, databases, and processing power". Mark Andrejevic, "Surveillance in the Digital Enclosure" (2007) 10 *Communication Review* 295, 314.