Bond University

Bond Law Review

Volume 37 Issue 1

2025

Drawing Boundaries Between Data Protection and Privacy: The Centre for Reforming the Data Protection Paradigm

Haodi Deng
Tongji University

DRAWING BOUNDARIES BETWEEN DATA PROTECTION AND PRIVACY: THE CENTRE FOR REFORMING THE DATA PROTECTION PARADIGM

HAODI DENG*

Abstract

This article demonstrates the evolving relationship between data protection and privacy in Europe, the US, and China, from interconnection to separation. In Europe, data protection and privacy have shifted from being intertwined into distinct concepts, notably propelled by the Charter of Fundamental Rights of the European Union. Similarly, China has firmly separated data protection and privacy through legislation like the Civil Code and the Personal Information Protection Law. Even in the US, a subset of privacy akin to data protection has been delineated within the expansive privacy framework. By examining China's landscape in more detail, this article examines the differences between data protection and privacy in terms of subject matter, the scope of subjects, burden of proof, and compensation for mental damage. Furthermore, this article critically evaluates the individual-centric, rights-based data protection paradigm, noting its shortcomings in achieving substantive fairness and tackling the escalating asymmetries between data controllers and data subjects. Afterwards, it calls for a more assertive state role in ensuring robust data protection, emphasising the importance of recognising the protection for personal data as a fundamental right to effectively counteract the mounting influence of data power.

* PhD student, Shanghai International College of Intellectual Property, Tongji University. I would like to thank Professor Megan Richardson for her insightful suggestions and the anonymous reviewers for their valuable comments.

I Introduction

The relationship between privacy and data protection is a complex and debatable topic and has attracted extensive academic interest.[1] Are they overlapping or parallel? Does one include the other? Answers may vary across jurisdictions, and even within the same jurisdiction at different times.

This article explores the evolving relationship between data protection and privacy in Europe, the US, and China, elucidates their distinction in China, and evaluates the current data protection paradigm.

Part II demonstrates a trend from interconnection to separation between data protection and privacy in Europe, the US and China. In Europe, the transition has been actualised through the *Charter of Fundamental Rights of the European Union*.[2] Even in the US, where privacy is a sweeping concept, a subset of privacy resembling data protection has been distinguished. In China, the separation between data protection and privacy was established with the introduction of the *General Provisions of Civil Law*,[3] which is further reinforced by the *Civil Code*[4] and the *Personal Information Protection Law*.[5]

Part III explores the distinction between data protection and privacy in China from the perspectives of subject matter, the scope of subjects, burden of proof, and compensation for mental damage. To begin with, the subject matter of privacy does not necessarily need to appear as information and be recorded, whereas personal information does. However, the privacy subject matter manifested as information is much narrower than personal information. Next, data protection rules impose similar obligations on both public and private entities, while privacy regulations exclusively apply to private entities. Despite this, private entities subject to privacy regulations have a broader scope than those

---

1 See, eg, Megan Richardson, 'Is Data Protection the New Privacy?' (2013) 93 *Amicus Curiae* 2; Orla Lynskey, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2014) 63(3) *International and Comparative Law Quarterly* 569; Robert Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere' (2017) 67(5) *Duke Law Journal* 981; 韩旭至 [Han Xuzhi], 《个人信息与个人隐私的区分》 [The Difference between Personal Information and Privacy] [2017] (2) 网络法律评论 *Internet Law Review* 88; 王利明 [Wang Liming], 《和而不同：隐私权与个人信息的规则界分和适用》 [Harmony and Difference: The Demarcation and Application of Privacy and Personal Information Rules] [2021] (2) 法学评论 *Law Review* 15.

2 Charter of Fundamental Rights of the European Union [2000] OJ C 364/1 ('EU Charter').

3 《中华人民共和国民法总则》 [General Provisions of the Civil Law of the People's Republic of China] (People's Republic of China) National People's Congress, Order 66, 15 March 2017 (repealed in 2020) ('PRC General Provisions').

4 《中华人民共和国民法典》 [Civil Code of the People's Republic of China] (People's Republic of China) National People's Congress, Order 45, 28 May 2020 ('PRC Civil Code').

5 《中华人民共和国个人信息保护法》 [Personal Information Protection Law of the People's Republic of China] (People's Republic of China) National People's Congress, Order 97, 20 August 2021 ('PIPL').

governed by data protection rules. Further, although liabilities arising from privacy invasions and data protection infringements are both fault-based, plaintiffs in privacy cases are required to prove defendants' fault, whereas in data protection cases, defendants must demonstrate their non-fault status due to a rule governing the reversal of the burden of proof. Lastly, in privacy cases, plaintiffs can only receive compensation for mental damage if they suffer 'serious mental damage' as a result of privacy invasions. In contrast, plaintiffs in data protection cases are entitled to compensation equal to the mental damage suffered, regardless of the severity of the damage.

Part IV evaluates the data protection paradigm, which is individual-centred and rights-based. Under the paradigm, data subjects are granted a set of micro-rights related to data processing (eg informed consent, access, and correction), which they ought to exercise to protect their pertinent interests. It is argued that, in the era of big data, the rights-based paradigm faces challenges in achieving substantive fairness when data subjects have limited cognitive and practical resources, and it struggles to address the increasing asymmetries between data controllers and data subjects, which give rise to data power. In reaching their optimal levels of data protection and curbing data power, data subjects should not be left alone. The state should take a more proactive role in achieving effective data protection. For this purpose, it is essential to recognise a fundamental right to the protection of personal data.

II The Changing Relationship between Privacy and Data Protection: From Interconnection to Separation

A *Privacy and Data Protection in Europe: From the ECHR to the GDPR*

The tradition of protecting private life has a long history in Europe.[6] In 1953, the *European Convention for the Protection of Human Rights and Fundamental Freedoms* ('*ECHR*') came into force.[7] According to Article 8 of the *ECHR*, individuals have the right to private life (covering the right to privacy).[8] Private life is a broad concept.[9] It covers, among others, personal data that individuals can legitimately expect not to be disclosed without their consent.[10] At this stage,

---

6 See generally James Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113(6) *Yale Law Journal* 1151.

7 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) ('*ECHR*').

8 See European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights', *ECHR Knowledge Sharing Platform* (Web Page) 52 <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng>.

9 Ibid 26.

10 Ibid 31.

personal data was protected through privacy and the line between them was unclear.

In 1970, following the *Hessian Data Protection Act*,[11] which emphasised the impact of informational technology on personhood and dignity,[12] data protection in Europe gradually separated from privacy. In 1977, Germany passed the *Federal Data Protection Act*.[13] The legislation tied its purposes directly to human dignity[14] and free development of personality provided for in the *German Constitution*.[15] Its drafting process was heavily influenced by the American scholars Alan Westin and Arthur Miller, in which the concept of informational self-determination was first used.[16] In 1983, the Federal Constitutional Court of Germany in the *Census Act Case* confirmed the right to informational self-determination as a constitutional right of personality.[17] According to the Court, the right to informational self-determination confers on the individual the authority to decide for themselves fundamentally on the disclosure and use of their personal data.[18] In its decision, the Court did not rely on any legal notion of privacy.[19]

In the 1980s, data protection rose to a higher level in Europe. Two seminal international documents, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[20] in 1980 ('*OECD Guidelines 1980*') and the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[21] in 1981 ('*Convention 108*'), were created. Although *Convention 108* does not strictly distinguish between data protection and privacy, its scope is

---

11 *Hessisches Datenschutzgesetz vom* [Hessian Data Protection Act] (Germany) 30 September 1970, GVBI Ⅰ, 1970, 625.

12 Meg Leta Jones, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47(2) *Social Studies of Science* 216, 220.

13 *Bundesdatenschutzgesetz* [Federal Data Protection Act] (Germany) 27 January 1977, BGBI Ⅰ, 1977, 201 ('*German Data Protection Act*').

14 Human dignity covers a wide range of values, and privacy is only one part of these values. See European Data Protection Supervisor, 'Towards a New Digital Ethics: Data, Dignity and Technology', *EDPS* (Web Page) 12 <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf>.

15 Grundgesetz für die Bundesrepublik Deutschland [Basic Law for the Federal Republic of Germany] arts 1-2 ('German Constitution').

16 Jones (n 12) 221.

17 *German Census Act Case of 1983*, Bundesverfassungsgericht [German Constitutional Court], 1 BvR 209/83, 15 December 1983 reported in (1983) 65 BVerfGE 1.

18 Ibid 42.

19 Paul Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' (1989) 37(4) *American Journal of Comparative Law* 675.

20 Organization for Economic Co-operation and Development, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', *OECD iLibrary* (Web Page) <https://www.oecd-ilibrary.org/science-and-technology> ('*OECD Guidelines 1980*').

21 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, ETS No 108 (entered into force 1 October 1985) ('*Convention 108*').

limited to 'automated processing' of 'personal data'.[22] In 1995, the *EU Directive 95/46*,[23] designed to unify the level of data protection between EU members and remove barriers to the flow of personal data, went into effect. It gives substance to and amplifies the data protection principles contained in the *Convention 108*. However, the right to privacy serves as a fundamental pillar of the *EU Directive 95/46*.[24] As a result, the right to privacy still had a considerable impact on the EU's data protection regime.

In the 21st century, privacy and data protection have been clearly separated in terms of the legal basis for protection. To begin with, the *Charter of Fundamental Rights of the European Union* ('*EU Charter*') delineated the division between privacy and data protection on the fundamental rights level.[25] Article 8 of the *EU Charter* provides for the 'protection of personal data' as a fundamental right ('the right to data protection'),[26] independent of the right to 'respect for private and family life' under Article 7. According to the EU Court of Justice, the right to data protection, which 'has no equivalent in the ECHR', is 'distinct from [the right to privacy] enshrined in Article 7 of the [EU] Charter'.[27] Indeed, the distinction between the right to data protection and the right to privacy in the EU Charter is not symbolic. The two rights differ in terms of the subject matter, the rights holders, and the parties responsible.[28] Furthermore, in contrast to the right to data protection, which is fairly clear-cut, the right to privacy is more value-laden and circumstance-dependent.[29]

Next, according to the *Treaty on the Functioning of the European Union* ('*TFEU*'),[30] the right to data protection in the *EU Charter* is part of the constitutional fabric of the EU. Article 16 of the *TFEU* reiterates

---

22 Article 2 of the *Convention 108* defines 'personal data' as 'information relating to an identified or identifiable individual'.

23 *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* [1995] OJ L 281/31 ('*EU Directive 95/46*').

24 According to Article 1 of the *EU Directive 95/46*, the protection of the fundamental rights and freedoms of natural persons, especially the right to privacy, is one of its objectives. Furthermore, 'privacy' is mentioned in several places in the *EU Directive 95/46*: arts 9, 13, 26.

25 EU Charter (n 2).

26 Notably, the right to data protection was once drafted as an individual's 'right to determine for himself whether his personal data may be disclosed and how they may be used', emphasising the notion of informational self-determination: see Lynskey (n 1) 591.

27 *Tele2 Sverige AB v Post- och Telestyrelsen* (Court of Justice of the European Union, C-203/15, ECLI:EU:C:2016:970, 16 March 2017) [129].

28 Firstly, data protection covers all information relating to identifiable and identified persons, while privacy does not. Secondly, data protection is limited to natural persons, whereas privacy is granted to both natural and legal persons. Thirdly, data protection imposes similar obligations concerning data processing on public authorities and private parties, while privacy addresses public authorities only. See Kokott and Sobotta (n 1) 225.

29 Post (n 1) 1011.

30 *Treaty on the Functioning of the European Union* [2016] OJ C 202/47.

that everyone has the right to the protection of personal data.[31] It also provides that the EU Council and Parliament should lay down rules on data protection.[32]

Lastly, the *General Data Protection Regulation* ('GDPR'), which became effective in 2018, identifies the right to data protection as a legal basis,[33] and none of its provisions mention the right to privacy.

B *Privacy and Data Protection in the US: From the Right to be Let Alone to Information Privacy*

As far back as the 19th century, there have been discussions about the right to privacy in the US.[34] In 1890, Warren and Brandeis published the article 'The Right to Privacy'.[35] They argued for the legal recognition of the right to privacy, characterised as a right 'to be let alone' and 'to an inviolate personality'.[36] Their argument led to a century of reform in tort law in the US. By 1960, according to William Posser, privacy torts had covered torts of intrusion upon seclusion, public disclosure of private facts, false light publicity and misappropriation of name or likeness.[37] Meanwhile, Warren and Brandeis's argument framed privacy discussions in the twentieth-century US, where privacy expanded and acquired meanings as 'limited access to the self', 'secrecy' of certain matters, a form of 'intimacy' and 'protecting personhood', and 'control over personal information'.[38]

Theoretically, the separation of data protection from traditional privacy - sometimes termed 'the right to be let alone' or 'decisional privacy' - in the US was prompted by the theory of 'control over personal information' ('control theory'). According to Alan Westin, who is generally regarded as the founder of the theory, the key to privacy is the ability of individuals (or groups, institutions) to have some degree of control over their information.[39]

Followers of the control theory formulated a new notion of privacy, namely information privacy,[40] an analogue to the European concept of 'data protection'. Information privacy is usually conceptualised as the

---

31 Ibid art 16.

32 Ibid.

33 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such data, and Repealing Directive 95/46/EC* [2016] OJ L 119/1, art 1 ('GDPR').

34 David Seipp, 'The Right to Privacy in Nineteenth Century America' (1981) 94(8) *Harvard Law Review* 1892, 1910.

35 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193.

36 Ibid 205.

37 William Prosser, 'Privacy' (1960) 48(3) *California Law Review* 383.

38 Daniel Solove, 'Conceptualizing Privacy' (2002) 90(4) *California Law Review* 1087.

39 Alan Westin, *Privacy and Freedom* (Atheneum, 1967) 7.

40 Westin did not use 'information privacy' to describe his conception of privacy: see ibid.

right to control the flow of personal data.[41] Michael Froomkin declared that information privacy is a right to control the 'acquisition' and 'release' of personal information.[42] According to Eugene Volokh, information privacy refers to a right to control the 'communication' of personal information.[43] Margaret Ann Irving characterised information privacy as a right to control the conditions under which personal information is 'collected, used, and disseminated'.[44] A similar definition was also adopted by the Clinton Administration.[45] Moreover, the US Supreme Court defined privacy as 'control over information concerning his or her person'.[46]

The key focus of information privacy is not on protection against intrusion but on the control of personal information (or data).[47] Besides the defensive function of preventing inappropriate disclosures of personal information, information privacy has positive functions. It allows data subjects to better control their information, enabling them to become more involved in the flow of information.

At the constitutional level, the US Supreme Court distinguished data protection (information privacy) from traditional privacy in the 1977 case *Whalen v Roe* ('*Whalen*').[48] In this case, the Court held that the constitutional right to privacy covers at least two 'different' interests: (a) freedom from interference in making certain fundamental decisions, and (b) having personal information kept private.[49] The first is known as 'decisional privacy' while the second is widely recognised as the Court's definition of the constitutional right to information privacy.[50] Decisional privacy is related to certain significant decisions (like marriage,[51] abortion[52] and contraception[53]) and individuals'

---

41 Elbert Lin, 'Prioritizing Privacy: A Constitutional Response to the Internet' (2002) 17(3) *Berkeley Technology Law Journal* 1085, 1095.

42 Michael Froomkin, 'The Death of Privacy' (2000) 52(5) *Stanford Law Review* 1461, 1463.

43 Eugene Volokh, 'Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You' (2000) 52(5) *Stanford Law Review* 1049, 1050.

44 Margaret Ann Irving, 'Managing Information Privacy in the Information Age' (2001) 53(2) *Administrative Law Review* 659, 661.

45 US Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (Report, October 1995) 2.

46 *United States Department of Justice v Reporters Committee for Freedom of the Press*, 489 US 749, 763 (1989).

47 Fred Cate, *Privacy in the Information Age* (Brookings Institution Press, 1997) 22.

48 *Whalen v Roe*, 429 US 589 (1977) ('*Whalen*').

49 Ibid 599-600.

50 Matthew Bunker et al, 'Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology' (1993) 20(3) *Florida State University Law Review* 543.

51 *Loving v Virginia*, 388 US 1, 12 (1967).

52 *Roe v Wade*, 410 US 113, 153 (1973). The *Roe* idea of decisional privacy has been reduced as a result of the recent US Supreme Court decision in *Dobbs v Jackson Women's Health Organization*, 597 US 215 (2022).

53 *Eisenstadt v Baird*, 405 US 438 (1972).

independence in making such decisions.[54] By comparison, information privacy focuses on the collection, use and dissemination of personal data generated in everyday life.[55] It is distinguishable from decisional privacy.

Furthermore, the notion of information privacy is reflected in certain US federal legislation. For example, the *Privacy Act of 1974* secures to individuals the right to exercise some degree of control over their personal information collected by the government.[56] Meanwhile, other pieces of legislation, such as the *Fair Credit Reporting Act* (regulating consumer reports), [57] the *Health Insurance Portability and Accountability Act of 1996* (regulating access to individuals' private medical records),[58] and the *Children's Online Privacy Act of 1998* (regulating access to personal information about children),[59] deal with specific types of interests in information privacy,[60] despite the absence of any explicit reference to 'information privacy'.

C *Privacy and Data Protection in China: From the General Principles of the Civil Law to the Personal Information Protection Law*

Similar to privacy, data protection in China was mainly governed by civil law until the *Personal Information Protection Law* ('*PIPL*') was enacted in 2021.[61] However, for a considerable period of time, Chinese civil law did not contain specific provisions regarding privacy and data protection.[62] They were protected under the umbrella of the right to reputation.[63]

The General Principles of the Civil Law, which became applicable in 1987, only protect a few personality rights (covering the right to reputation) without any reference to 'privacy' or 'personal data (information)'.[64] In an effort to offer some level of privacy protection,

---

54 Paul Schwartz, 'Property, Privacy, and Personal Data' (2004) 117(7) *Harvard Law Review* 2056, 2058.

55 Ibid.

56 *Privacy Act of 1974*, 5 USC § 552a (1974).

57 15 USC §§ 1681 (2000).

58 Pub L No 104-191, 110 Stat 1936.

59 15 USC §§ 6501–6506 (1998).

60 The US has not established a comprehensive privacy (data protection) regime and maintained an industry-specific approach, where some industries are covered and others are not.

61 周汉华 [Zhou Hanhua], 《平行还是交叉：个人信息保护与隐私权的关系》 [Parallel or Overlap: Relationships between Personal Information Protection and Privacy Protection] [2021] (3) 中外法学 *Peking University Law Journal* 1167, 1170.

62 石佳友 [Shi Jiayou], 《隐私权与个人信息关系的再思考》 [Rethinking of the Interactions Between Right of Privacy and Personal Data] [2021] (5) 上海政法学院学报 *Journal of Shanghai University of Political Science and Law* 81.

63 Ibid.

64 《中华人民共和国民法通则》 [General Principles of the Civil Law of the People's Republic of China] (People's Republic of China) National People's Congress, Order 37,12 April 1986 (repealed in 2020).

the Supreme People's Court ('SPC') categorised the publicising of others' privacy matters in written or spoken form,[65] as well as the release of others' privacy materials without consent,[66] as violations of the right to reputation in 1988 and 1993, respectively. Furthermore, in 1998, the SPC specified that the right to reputation was violated when a medical and hygiene institution disclosed, without permission, information that 'an individual suffers from gonorrhoea, syphilis, leprosy, AIDS, etc', causing harm to the individual's reputation.[67] As a result, certain health information was protected by the right to reputation. At this stage, both privacy and data protection were components of the right to reputation, with a blurred distinction between them.

At the dawn of the 21st century, Chinese courts began to treat privacy as a legitimate interest independent of the right to reputation. According to a judicial interpretation issued by the SPC in 2001, individuals are entitled to claim compensation for mental damage not only when their right to reputation is violated, but also when their 'privacy and other interests' are 'infringed upon in a manner contrary to the public interest and social morality'.[68] Further, in 2008, the SPC recognised 'invasion of privacy' as a cause of action.[69] Already, with the introduction of the *Tort Liability Law* ('*TLL*') in 2009, privacy has been delineated as a personality right separate from the right to reputation.[70] By comparison, 'personal information (data)' is not included in the roster of protected rights and interests under the *TLL*.[71]

As privacy transitioned from being adjunct to the right to reputation to a separate interest and subsequently to an independent right, courts increasingly referred to the notion of privacy to protect personal

---

65 《最高人民法院关于贯彻执行<中华人民共和国民法通则>若干问题的意见（试行）》[Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (for Trial Implementation)] (People's Republic of China) Supreme People's Court, 26 January 1988 (repealed in 2021).

66 《最高人民法院关于审理名誉权案件若干问题的解答》[Answers of the Supreme People's Court on Some Issues concerning the Trial of Cases Involving the Right of Reputation] (People's Republic of China) Supreme People's Court, 7 August 1993 (repealed in 2021).

67 《最高人民法院关于审理名誉权案件若干问题的解释》[Interpretation of the Supreme People's Court on Several Issues about the Trial of Cases Concerning the Right to Reputation] (People's Republic of China) Supreme People's Court, 31 August 1998 (repealed in 2021).

68 《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》[Interpretation of the Supreme People's Court on Issues concerning the Ascertainment of Compensation for Mental Damage in Civil Torts] (People's Republic of China) Supreme People's Court, 8 March 2001, art 1.

69 《民事案件案由规定》[Provisions on the Causes of Action for Civil Cases] (People's Republic of China) Supreme People's Court, 4 February 2008.

70 《中华人民共和国侵权责任法》 [Tort Liability Law of the People's Republic of China] (People's Republic of China) National People's Congress, Order 21, 26 December 2009, art 2 (repealed in 2020).

71 Ibid.

information. For example, in *Wangfei v Zhang Leyi*, the Second Intermediate People's Court of Beijing Municipality held that the defendant's disclosure of the plaintiff's work place, address, photos, and her extramarital affair, which were information that the plaintiff did not wish to be known to the public, constituted an invasion of privacy.[72] Likewise, in *Sun Weiguo v Shanghai Branch of China Unicom Network Communications Ltd*, the Pudong New Area People's Court held that the right to privacy entitles an individual to decide whether and to what extent his or her confidential information should be disclosed, and that others' unauthorised disclosure of the information constitutes an invasion of privacy.[73]

In 2017, the *General Provisions of the Civil Law* ('*General Provisions*') became effective.[74] It distinguishes data protection from privacy and lays the groundwork for establishing an independent data protection framework within civil law. Under Chapter V 'Civil Rights' of the *General Provisions*, Article 110 grants individuals the right to privacy. [75] Meanwhile, Article 111 provides that 'the personal information of natural persons shall be protected by law'.[76] It also outlines rules governing the handling of personal information, including lawful obtaining of personal information, prevention of unlawful collection, use, processing and transmission of personal information, prohibition of illicit trading, provision and disclosure, as well as ensuring information security.[77] While the *General Provisions* do not explicitly detail the distinction between privacy and data protection, it is clear from the relevant clauses that the two concepts are not interchangeable.

In a number of cases decided after the *General Provisions* came into force, courts distinguished between privacy and data protection.[78] For example, in *Ling Moumou v Beijing Weibo Shijie Technology Co Ltd*, after finding that the plaintiff's name, phone number, and geographical location constitute personal information, the Beijing Internet Court held

---

72 《王菲诉张乐奕隐私权纠纷案》 [Wangfei v Zhang Leyi — Privacy Dispute Case], 北京市第二中级人民法院 [Second Intermediate People's Court of Beijing Municipality, People's Republic of China], 二中民终字第 5603 号 [Civil Appeal No 5603], 23 December 2009.

73 《孙伟国诉中国联合网络通信有限公司上海市分公司侵犯隐私权纠纷案》 [Sun Weiguo v Shanghai Branch of China Unicom Network Communications Ltd — Privacy Dispute Case], 上海市浦东新区人民法院 [Shanghai Municipal Pudong New Area People's Court, People's Republic of China], 浦民一民初字第 9737 号 [Civil Case No 9737], 3 September 2009.

74 *PRC General Provisions* (n 3) art 206.

75 Ibid art 110.

76 Ibid art 111.

77 Ibid.

78 张建文, 时诚 [Zhang Jianwen and Shi Cheng],《<个人信息保护法>视野下隐私权与个人信息权益的相互关系》[The Relationship between Privacy and Personal Information under the Perspective of Personal Information Protection Law] [2022] (2) 苏州大学学报 *Journal of Soochow University* 46, 51.

that the defendant's processing of the information without the plaintiff's consent violated the plaintiff's legitimate interest in the information.[79] However, the Court rejected the argument that the processing violated privacy because the information in question was not the subject matter of privacy.[80] Likewise, in *Huang Yan v Shenzhen Tencent Computer System Co Ltd* decided by the same court, the defendant, operating a book reading App, disclosed the plaintiff's reading records to his friends on the App without consent.[81] The Court held that the disclosure violated the plaintiff's interest in his personal information, but it did not constitute an invasion of privacy since the reading records were not deemed confidential.[82]

In 2021, the *Civil Code* came into effect, strengthening the separation between privacy and data protection.[83] The *General Provisions* were slightly revised to become Book I 'General Provisions' of the *Civil Code*.[84] As a result, Articles 110 and 111 of the *General Provisions* are now Articles 110 and 111 of the *Civil Code*.[85] Meanwhile, Chapter 6 of Book IV 'Personality Rights' is titled 'Privacy and Personal Information Protection' and consists of detailed rules on privacy and data protection.[86] To begin with, the concluding paragraph of Article 1032 and the second paragraph of Article 1034, respectively, define the subject matters of privacy (ie the tranquillity of private life as well as private and confidential space, activities, and information) and personal information (ie information relating to an identifiable or identified individual), indicating distinctions in the scope of privacy and data protection, despite some overlap.[87] Next, Articles 1033 and 1035 describe actions that may constitute invasions of privacy and the principles for handling personal information, respectively.[88] Lastly, the third paragraph of Article 1034 specifically addresses confidential and private information, which falls under both personal information and the sphere of privacy.[89] It stipulates that provisions on privacy apply to

---

79 《凌某某诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案》 [Ling Moumou v Beijing Weibo Shijie Technology Co Ltd — Privacy and Personal Information Dispute Case], 北京互联网法院 [Beijing Internet Court, People's Republic of China], 京 0491 民初 6694 号 [Civil Case No 6694], 30 July 2020.

80 Ibid.

81 《黄燕诉深圳腾讯计算机系统有限公司案》 [Huang Yan v Shenzhen Tencent Computer System Co Ltd], 北京互联网法院 [Beijing Internet Court, People's Republic of China], 京 0491 民初 16142 号 [Civil Case No 16142], 30 July 2020.

82 Ibid.

83 *PRC Civil Code* (n 4) art 1260.

84 Ibid book I.

85 Ibid art 110-11.

86 Ibid art 1032-9.

87 Ibid arts 1032, 1034.

88 Ibid arts 1033, 1035.

89 Ibid art 1034.

private and confidential personal information; if no such provisions exist, the provisions on protecting personal information will apply.[90]

Just ten months after the implementation of the *Civil Code*, the *PIPL* became effective.[91] The *PIPL* expressly articulates its objective to protect 'the rights and interests relating to personal information'[92] and sets forth comprehensive regulations concerning data protection. As of this point, the Chinese legal framework clearly distinguishes between privacy and data protection.

III The Distinction between Privacy and Data Protection: A Chinese Perspective

In the previous discussion, it became clear that privacy and data protection have evolved into different concepts across Europe, the US, and China. However, the distinction between privacy and data protection varies within these jurisdictions, as the concepts themselves are perceived differently. In Part III, this article will delve into the disparity between privacy and data protection in China through the lenses of subject matter, legal subjects, burden of proof, and compensation.

A *Subject Matter*

The first distinction between data protection and privacy lies in their respective subject matter.

To begin, data protection covers all personal information, defined as 'information, recorded electronically or otherwise, related to an identified or identifiable natural person, excluding anonymised information'.[93] By comparison, the subject matter of privacy includes (1) a natural person's 'tranquillity of private life' (ie a state of life that is not 'intruded upon by means of phone calls, text messages, instant messaging tools, e-mails, flyers, etc')[94] and (2) private and confidential spaces (eg private parts of the body, personal residence, diaries, pockets),[95] activities (eg sexual life) and information (eg information about one's medical conditions, sexual orientation)[96] that a natural person does not wish to be known by others.[97]

---

90 Ibid.

91 *PIPL* (n 5) art 74.

92 Ibid art 1.

93 Ibid art 4.

94 *PRC Civil Code* (n 4) art 1033.

95 杨立新 [Yang Lixin],《关于隐私权及其法律保护的几个问题》[Several issues concerning the right to privacy and its legal protection] [2000] (1) 人民检察 *People's Procuratorial Semimonthly* 26.

96 黄薇 [Huang Wei],《中华人民共和国民法典释义及适用指南》[Interpretation and Application Guide of the Civil Code of the People's Republic of China], (中国民主法制出版社[China Democracy and Legal System Publishing], 2020) 1539.

97 *PRC Civil Code* (n 4) art 1032.

It can be seen that the subject matter of privacy does not necessarily manifest itself as information but can take other forms. In contrast, Article 4 of the *PIPL* requires personal information to be recorded by electronic or other means.[98] This requirement is also present in the definition of 'personal information' in Article 1034 of the *Civil Code*[99] and Article 76 of the *Cybersecurity Law*.[100] Therefore, personal information does not encompass aspects of privacy that are not recorded.

On the other hand, the scope of privacy subject matter existing in the form of information is narrower than that of personal information. For privacy to attach to personal information, the information must be 'confidential' and 'private', and simultaneously what its subject does 'not wish to be known by others'.[101]

Firstly, 'confidential' in the privacy sense does not suggest that the information is not known to anyone besides its subject, but rather that it is not readily accessible through public channels.[102] In *Huang Xinwen v Weisirui International Sports Development Co Ltd*, where the defendant used photos shared by the plaintiff on his WeChat Moments for advertising purposes without consent, the Pingxiang Intermediate People's Court held that the photos in question were confidential because they were only viewable by the plaintiff's WeChat friends, and not by those who were not friends.[103]

Secondly, 'private' requires that personal information has only an indirect connection to the public interest.[104] This means that leaving the information unprocessed would not harm the public interest.[105] Conversely, if not processing personal information would be detrimental to the public interest, the information is not 'private', and therefore processing it to the necessary extent to protect public interest would not be an invasion of privacy.[106] For example, under Article 999

---

98 Cf *Privacy Act 1988* (Cth) s 6.

99 Article 1034 of the *PRC Civil Code* defines personal information as 'information, recorded electronically or by other means, that can identify a specific individual either on its own or in combination with other information': art 1034.

100 《中华人民共和国网络安全法》 [Cybersecurity Law of the People's Republic of China] (People's Republic of China) National People's Congress, Order 53, 7 November 2017.

101 *PRC Civil Code* (n 4) art 1032.

102 张璐 [Zhang Lu],《何为私密信息？》[What is Private and Confidential Information?] [2021] (1) 甘肃政法大学学报 *Journal of Gansu University of Political Science and Law* 86.

103 《黄鑫文诉萍乡市维斯瑞国际体育发展有限公司隐私权纠纷案》 [Huang Xinwen v Weisirui International Sports Development Co Ltd — Privacy Dispute Case], 江西省萍乡市中级人民法院 [Jiangxi Province Pingxiang Municipal Intermediate Court, People's Republic of China], 赣 03 民终 240 号 [Civil Appeal No 240], 26 July 2017.

104 彭錞 [Peng Chun],《再论中国法上的隐私权及其与个人信息权益之关系》[The Right to Privacy and its Relationship with Personal Information in Chinese Law] [2023] (1) 中国法律评论 *China Law Review* 161, 167.

105 Ibid.

106 Ibid.

of the *Civil Code*, personal information can reasonably be utilised for activities serving the public interest, such as news reporting and supervision by public opinion.[107]

Finally, the phrase 'not wish to be known by others' highlights the intentions of information subjects. If an individual lacks the intention to maintain the confidentiality of certain information, privacy will not exist in the information, even if it is confidential and private.[108]

Overall, compared to other personal information, personal information protected by privacy not only possesses the ability to directly or indirectly identify a natural person, but also satisfies three additional criteria: confidentiality, privateness and the subject's intention to preserve its confidentiality.[109] Consequently, private and confidential information constitutes just a subset of personal information.

B *Scope of Subjects*

The second distinction between privacy and data protection concerns their subject scope. Although both privacy and data protection are granted exclusively to natural persons,[110] they differ in terms of the range of obligated parties.

One aspect of the subject scope relates to the obligations of public entities. Privacy rules are primarily found in the *Civil Code*,[111] which governs personal and property relations among parties of equal legal standing.[112] As the *Civil Code* does not address relationships between unequal entities, privacy does not create obligations for public authorities. In contrast, data protection, as given expression by the *PIPL*, imposes similar obligations with regard to the processing of personal information on public and private entities.[113] Therefore, public entities must adhere to data protection rules when processing personal information, irrespective of their purposes.

On the other hand, privacy places obligations on a broader spectrum of private entities than data protection. Every private entity, including natural persons, legal persons and unincorporated organisations, is

---

107 *PRC Civil Code* (n 4) art 999.

108 许可, 孙铭溪 [Xu Ke and Sun Mingxi],《个人私密信息的再厘清》[Re-clarification of Private and Confidential Personal Information] [2021] (1) 中国应用法学 *China Journal of Applied Jurisprudence* 3, 13.

109 *PRC Civil Code* (n 4) art 1032.

110 Ibid arts 1032, 1034.

111 程啸 [Cheng Xiao],《论个人信息权益与隐私权的关系》[On the Relationship between the Right to Personal Information and the Right to Privacy] [2022] (4) 当代法学 *Contemporary Law Review* 59, 68.

112 *PRC Civil Code* (n 4) art 2.

113 *PIPL* (n 5) arts 3, 33.

obliged to refrain from invading others' privacy through actions such as 'spying, intrusion, divulgence, disclosure, etc'.[114]

In contrast, while data protection imposes obligations with respect to the processing of personal information ('data protection obligations') on private entities, not all of them are bound by such obligations. This conclusion may not be immediately apparent from the *Civil Code*, as it does not explicitly exempt any private entities. However, the data protection rules within the *Civil Code* should be read alongside the *PIPL*, as they form part of a unified data protection regime.[115] According to Article 72 of the *PIPL*, data protection rules do not apply to the processing of personal information by a natural person for personal or household affairs.[116] As a result, individuals who process personal information in the course of non-commercial or non-professional activities do not qualify as 'information processors'[117] in the data protection sense and are exempt from data protection obligations.[118]

Notably, although PIPL does not exclude the possibility of natural persons as information processors, in most data protection cases, the defendants are not natural persons.[119] Instead, they are technology companies, banks, and telecommunications companies that run websites or apps.[120] These private entities, acting as information processors, are usually more powerful and possess a greater amount of information than information subjects ('power and information asymmetries').[121] Therefore, the relationship governed by the data protection regime between information subjects and information processors is often imbalanced, despite their equal legal standing under the law.

This phenomenon may be more pronounced in other jurisdictions. For example, the Australian *Privacy Act 1988* provides exemptions not only for personal, family and household affairs, but also, inter alia, for

---

114 *PRC Civil Code* (n 4) art 1032.

115 丁晓东 [Ding Xiaodong],《隐私权保护与个人信息保护关系的法理》[The Jurisprudence of the Relationship between the Protection of Privacy and Personal Information] [2023] (6) 法商研究 *Studies in Law and Business* 61, 70.

116 *PIPL* (n 5) art 72.

117 The concept of 'personal information processors' in the *PIPL* is more aligned with 'data controllers' than 'data processors' under the *GDPR*. As outlined in Article 73 of the *PIPL*, 'personal information processors' refer to organisations or individuals that independently determine the objectives and methods of processing personal information.

118 杨芳 [Yang Fang],《我国<个人信息保护法>中私人事务例外规则之解释》[Interpretation of the Private Affairs Exception Rule in the Personal Information Protection Law] [2022] (3) 南大法学 *Nanjing University Law Journal* 147, 158.

119 林凯, 张建肖 [Lin Kai and Zhang Jianxiao],《个人信息纠纷民事判决之历时性比较分析》[A Diachronic Comparative Analysis of Civil Judgments on Personal Information Disputes] [2023] (1) 数据法学 *Data Law Review* 119, 139.

120 Ibid.

121 Ibid.

most small businesses with an annual turnover below $3 million.[122] Similarly, the *California Consumer Privacy Act of 2018* excludes data processing by natural persons and establishes stringent criteria for regulated businesses.[123] Consequently, there are information and power asymmetries between the businesses it regulates and consumers.

C *Burden of Proof for Fault*

For liability arising from both privacy and data protection infringements, fault is a crucial element.[124] However, in terms of who is responsible for proving fault, privacy and data protection differ.[125] Specifically, to establish an invasion of privacy, the plaintiff must prove, inter alia, the fault of defendant.[126]

In contrast, in data protection cases, the burden of proving the absence of fault rests on the defendant, who acts as the information processor. This reversal of the burden of proof is a result of Article 69(1) of the *PIPL*, which presumes the information processor to be at fault for any processing activities that harm information subjects.[127] Consequently, an information processor cannot be exempted from liability unless able to demonstrate the absence of fault. Moreover, since fault is generally understood objectively, the information processor typically must show compliance with data protection rules to meet the burden of proof.[128]

When formulating Article 69(1) of the *PIPL*, the legislator took into account the information asymmetry between information processors and subjects, where processors possess the bulk of information on

---

122 *Privacy Act 1988* (n 98) ss 6, 6C, 6D, 16

123 A 'business' regulated by the *California Consumer Privacy Act of 2018* must meet at least one of the following criteria: (A) has annual gross revenues exceeding twenty-five million dollars; (B) alone or in combination, annually purchases, sells, or shares the personal information of 100,000 or more consumers or households; (C) generates 50 percent or more of its annual revenues from selling or sharing consumers' personal information: Cal Civil Code §§ 1798.100-1798.199 (West 2021).

124 程啸 [Cheng Xiao] (n 111) 70.

125 Ibid.

126 Fault-based liability also encompasses other elements, namely the act, the damage and the causal connection between the act and the damage: *PRC Civil Code* (n 4) art 1165.

127 *PIPL* (n 5) art 69(1).

128 See, eg,《余甜甜诉邵佰春个人信息保护纠纷案》 [Yu Tiantian v Shao Baichun — Personal Information Dispute Case], 重庆市合川区人民法院 [Chongqing Municipal Hechuan District People's Court, People's Republic of China], 渝 0117 民初 3906 号 [Civil Case No 3906], 29 January 2023;《单学文诉江西二向箔实业发展有限公司个人信息保护纠纷案》 [Shan Xuewen v Jiangxi Erxiangbo Industrial Development Co Ltd — Personal Information Dispute Case], 江西省南昌市青山湖区人民法院 [Jiangxi Province Nanchang Municipal Qingshanhu District People's Court, People's Republic of China], 赣 0111 民初 4656 号 [Civil Case No 4656], 1 November 2022;《祝琦诉大连庄河市九洲职业培训学校》 [Zhu Qi v Jiuzhou Vocational Training School], 辽宁省庄河市人民法院 [Liaoning Province Zhuanghe Municipal People's Court, People's Republic of China], 辽 0283 民初 6961 号 [Civil Case No 6961], 3 January 2023.

processing operations.[129] Such information asymmetry would constitute a significant obstacle for information subjects to hold those who process their information accountable without the rule governing the reversal of the burden of proof in place.[130] In this sense, the rule helps to redress the information asymmetry.

D *Threshold for Mental Damage Compensation*

Although individuals affected by both privacy and data protection infringements may be eligible for compensation for mental damage, they face different criteria. According to Article 1182 of the *Civil Code*, compensation for mental damage as a result of a privacy invasion is only applicable if the damage is deemed 'serious'.[131] In contrast, Under Article 69(2) of the *PIPL*, individuals are entitled to compensation equivalent to the damage (covering material and mental damage) caused by data protection infringement, irrespective of the severity of the damage.[132] It can be seen that the threshold for compensation for mental damage in data protection infringements is lower than that in privacy invasions. The rationale behind the *PIPL*'s lower threshold is that in cases where a data protection infringement does not involve reputation, likeness, etc, resultant mental damage, such as anxiety and loss of peace of mind, often far fails to meet the threshold of severity.[133] If individuals had to prove 'serious' mental damage to claim compensation, the burden of proof would be too challenging to meet.[134]

Similar to the *PIPL*, data protection laws in certain jurisdictions do not require mental damage to be serious to entitle victims of data protection infringements to compensation.[135] For example, Article 28 of the Taiwan *Personal Data Protection Act*, dealing with compensation, does not employ the term 'serious' to qualify 'non-pecuniary damage'.[136] It also guarantees that victims will receive a minimum compensation of $500 for mental damage.[137]

---

129 杨合庆 [Yang Heqing],《中华人民共和国个人信息保护法释义》[Interpretation of the Personal Information Protection Law of the People's Republic of China], (法律出版社[Law Press], 2022) 169.

130 Ibid.

131 *PRC Civil Code* (n 4) art 1182.

132 *PIPL* (n 5) art 69(2).

133 蔡一博, 郭福卿 [Cai Yibo and Guo Fuqing], 《隐私与个人信息区分下的衔接保护》[Articulated Protection under the Distinction between Privacy and Personal Information] [2022] (12) 学术交流 *Academic Exchange* 105, 110.

134 Ibid.

135 See, eg, *German Data Protection Act* (n 13) 83.

136 《個人資料保護法》[Personal Data Protection Act] (Republic of China) Legislative Yuan, 31 May 2023, art 28.

137 Ibid.

IV The Rights-based Data Protection Paradigm: Inadequacy and Enhancement

Although data protection and privacy are now distinguishable, they were intermingled for a considerable period. As a result, the paradigm of data protection closely resembles that of privacy, being individual-centric and rights-based. The Fair Information Practices Principles ('FIPPs'), which form the backbone of data protection frameworks, protect the diverse interests of data subjects by granting them various micro-rights concerning data processing (eg the right to access and correct personal data). Grounded in this rights-based paradigm, individuals' capacity to control data and participate in its processing is significantly enhanced. Nevertheless, as data processing technologies evolve, the rights-based paradigm encounters substantial challenges.

A *Overview of the Rights-based Data Protection Paradigm*

In discussing the rights-based data protection paradigm, it is essential to associate the discussion with the FIPPs, which provide a 'common language' for the discourse of data protection issues.[138]

Since their inception, the idea of entitlement has been embedded in the FIPPs. The initial version of the FIPPs was introduced in the 1973 report titled *Records, Computers, and the Rights of Citizens* ('RCRC report'), released by the Advisory Committee on Automated Personal Data Systems,[139] as a response to public concerns over the increasing use of computers to maintain personal records in both the public and private sectors.[140]

The RCRC report established five basic principles for data processing, with three specifically focusing on the rights of individuals.[141] These principles, inter alia, ensure that individuals can know what personal data is being collected in a record and how the information is being used, prevent the use of their data for purposes other than those for which the individuals have given consent, and correct or amend records of personal identifiable data.[142] Accordingly, the original version of the FIPPs grant individuals three micro-rights concerning data processing: the right to know, the right to consent, and the right to correct or amend.

---

138 Paula Bruening, 'Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy', *Policy@Intel* (Blog Post, 19 October 2014) <https://community.intel.com/t5/Blogs/Intel/Policy-Intel/Rethink-Privacy-2-0-and-Fair-Information-Practice-Principles-A/post/1332705>.

139 Advisory Committee on Automated Personal Data Systems, 'Records, Computers, and the Rights of Citizens', *Office of the Assistant Secretary for Planning and Evaluation* (Web Page, 30 January 1973) <https://aspe.hhs.gov/reports/records-computers-rights-citizens>.

140 Robert Gellman, 'Fair Information Practices: A Basic History', *SSRN* (Unpublished Manuscript, 6 April 2022) 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020>.

141 Ibid.

142 Ibid.

Since their inception, the FIPPs have profoundly influenced subsequent information privacy legislation in the US, where they originated.[143] Further, following their incorporation into the *OECD Guidelines 1980* and the *Convention 108*, the FIPPs have been widely embraced by nearly all jurisdictions dedicated to data protection.[144] With their extensive adoption by international organisations and different jurisdictions, multiple versions of the FIPPs have been developed.[145] While these versions may vary, the core idea of entitlement in the FIPPs — protecting the pertinent interests of individuals by conferring them a spectrum of micro-rights concerning the processing of their personal data — remains unchanged.[146] For example, according to the 'Individual Participation Principle' identified by the *OECD Guidelines 1980*, the most commonly cited version of the FIPPs,[147] data subjects should have a set of micro-rights regarding their personal data.[148] These micro-rights include the right to confirm whether a data controller has their personal data, the right to access their personal data retained by the controller, and the right to erase, rectify, and amend their personal data.[149] For another example, the *GDPR*, representing the most recent manifestation of the FIPPs in EU law,[150] not only entitles data subjects to access, correct, and delete their personal data, but also grants them the rights to informed consent, restriction of processing, data portability, and not to be subjected to automated decision-making.[151] As the *GDPR* requires adequate data protection laws for international data transfers, it is reasonable to expect that the rest of the data-creating world will continue implementing certain versions or aspects of the FIPPs, thereby strengthening the rights-based data protection paradigm.[152]

---

143 The FIPPs, as identified by the RCRC report, laid the foundation for the *Privacy Act of 1974*, 5 USC § 552a (1974). Meanwhile, various federal laws adopted some version of the FIPPs: see, eg, *Family Educational Rights and Privacy Act of 1974*, 20 USC § 1232g (1974); *Cable Communications Policy Act of 1984*, 47 USC §§ 521-73 (1984); *Driver's Privacy Protection Act of 1994*, 18 USC §§ 2721-5 (1994); *Video Privacy Protection Act*, 18 USC § 2710 (1998). Similarly, at the state level, certain regulations governing data processing by state governments have integrated the FIPPs, such as the *Minnesota Government Data Practices Act*, Minn. Stat. § 13 (1974).

144 Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices' (2017) 76(4) *Maryland Law Review* 952, 959.

145 See generally Fred H Cate, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer Protection in the Age of the Information Economy* (Routledge, 2016) 343, 345-55.

146 Ibid.

147 Gellman (n 140) 12.

148 *OECD Guidelines 1980* (n 20) pt 2.

149 Ibid.

150 Hartzog (n 144) 960

151 *GDPR* (n 33) arts 6, 12-22.

152 Hartzog (n 144) 960.

B *Inadequacy of the Rights-based Data Protection Paradigm*

As the FIPPs have become synonymous with data protection,[153] the idea of protecting relevant interests of data subjects by conferring micro-rights regarding the processing of their data has become deeply embedded in data protection regimes worldwide, shaping the paradigm of data protection.[154] The rights-based data protection paradigm has been around for a long time and functions well in some respects.[155] However, with the advent of the big data era, it has exposed some inadequacies. Firstly, the rights-based paradigm is difficult to achieve substantive fairness. Secondly, it falls short in effectively addressing the growing asymmetry between data controllers and data subjects.

1 *Difficulty in Achieving Substantive Fairness*

Firstly, granting individuals the right to choose during data collection does not necessarily adequately protect their interests. The right to choose means that individuals can decide whether to consent to the collection of personal data in response to a notice from a data collector (eg a website). Data subjects rely on the 'notice-consent' framework to exercise their right to choose during data collection.[156]

Numerous studies have shown that the 'notice-consent' framework faces formalism problems. Firstly, individuals rarely read privacy notices from data collectors.[157] Secondly, individuals may not have enough time to read privacy notices with boring content.[158] Lastly, they may have difficulty understanding professional privacy notices[159] or discerning the risks described in the notices.[160] As such, although the 'notice-consent' framework gives individuals choices, the choices they make may not be well-considered or meaningful, because privacy notices may not fulfil the purpose of informing.

---

153 Ibid 954.

154 丁晓东 [Ding Xiaodong],《论个人信息法律保护的思想渊源与基本原理：基于公平信息实践的分析》[On the Ideological Origin and Basic Principles of Legal Protection of Personal Information: An Analysis Based on the Fair Information Practices Principles] [2019] (3) 现代法学 *Modern Law Science* 96.

155 Ibid 104.

156 Joel Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (1999) 52(5) *Stanford Law Review* 1315, 1359.

157 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009) 105.

158 Lorrie Faith Cranor, 'Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2012) 10(2) *Journal on Telecommunications and High Technology Law* 273, 273-4.

159 Kent Walker, 'The Costs of Privacy' (2001) 25(1) *Harvard Journal of Law and Public Policy* 87.

160 Alessandro Acquisti and Jens Grossklags, 'What Can Behavioral Economic Teach Us about Privacy?' in Alessandro Acquisti et al (eds), *Digital Privacy: Theory, Technologies, and Practices* (CRC Press, 2007) 363.

Moreover, the formalism problems of the 'notice-consent' framework cannot be effectively addressed, even if the law stipulates that privacy notices should be clear and intelligible.[161] A lot of legislation requires privacy notices to be clear and intelligible and avoid being overly professionalised. For example, under Article 12 of the *GDPR*, privacy notices should use 'clear and plain language' and be provided in a 'concise' and 'intelligible' manner.[162] However, such a requirement ignores the fact that data practice itself is highly complicated. The requirement that privacy notices be clear and understandable does not change the nature of data processing. Accordingly, if data collectors are required to express their practices in simple privacy notices, individuals will probably be more confused.[163]

Secondly, granting individuals rights in relation to data processing after collection does not necessarily adequately protect their interests.

Theoretically, individuals may maintain control over their personal data after collection by exercising rights such as the 'right to be forgotten' and the 'right to restriction of processing'.[164]

In practice, however, individuals often have difficulty exercising their post-collection rights of control. Firstly, data processing has become extremely complicated thanks to big data and algorithms.[165] Individuals may have trouble understanding how data is stored, used, and transferred, and therefore cannot control its processing after collection. Secondly, data processing can be surreptitious. Take the Facebook-Cambridge Analytica data scandal as an example, in which Cambridge Analytica collects data from the public under the guise of psychological study and then uses these personal data for purposes such as political analysis.[166] The public was unaware of Cambridge Analytica's conduct until the news media exposed it massively. Therefore, it has become increasingly difficult for individuals to exercise their rights effectively to protect legitimate interests in the face of such complicated and stealthy data processing.

Finally, granting more rights concerning data processing to individuals increases the costs of data controllers. The increase may lead data controllers to allocate a significant portion of their resources to privacy notices and other formalistic compliance, because obtaining consent from individuals before collecting personal data and resolving

---

161 Ryan Calo, 'Against Notice Skepticism in Privacy (And Elsewhere)' (2011) 87(3) *Notre Dame Law Review* 1027, 1027-33.

162 *GDPR* (n 33) art 12.

163 Walker (n 159).

164 *GDPR* (n 33) arts 17-18.

165 Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) *International Data Privacy Law* 74, 76.

166 Carole Cadwalladr and Emma Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (online, 18 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

complaints post-collection could potentially shield data controllers from liability.[167] As a result, data controllers' attention may be diverted from the risks associated with data breaches and misuse of data during the entire process of collection, storage, use, and disclosure.

2 *Inadequate Response to Increasing Asymmetry*

Undeniably, the FIPPs' makers were aware of the problem of asymmetry between data controllers and data subjects.[168] The FIPPs were created to ensure individuals had some leverage in their interactions with more powerful government agencies and large corporations.[169] However, half a century after the FIPPs were created, technological advances have dramatically increased the asymmetry between the controllers and the subjects of data.[170]

Firstly, advanced technologies, specifically big data and algorithms, have profoundly changed data processing. This has allowed data controllers to exert greater control over data resources and exacerbated the asymmetry between controllers and subjects.

Previously, data controllers could only handle 'small data' with a narrow scope and small volume due to limitations in traditional data processing technologies. Nowadays, thanks to advanced technologies such as big data techniques and algorithms, data controllers can process 'big data'. Data processing has improved unprecedentedly in terms of scale, variety, speed and accuracy.[171] This elevates the data controller's control over data resources.

Furthermore, the greater control data controllers have over data, the stronger the impact they have on society and individuals.[172] Data controllers who control data resources can determine data subjects' preferences through psychological knowledge and guide their behaviour through online media to achieve desired outcomes.[173] Arguably, data controllers with control over data resources can gain a strong position in cyberspace and reality.

On the other hand, individuals generally cannot control data resources through data processing since it requires extensive capital investment and technical expertise. Individuals as data subjects are at a

---

167 Omri Ben-Shahar and Lior Jacob Strahilevitz, 'Contracting Over Privacy: Introduction' (2016) 45(2) *Journal of Legal Studies* 1, 8.

168 Advisory Committee on Automated Personal Data Systems (n 139).

169 Ibid.

170 Nadezda Purtova, 'Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation' (2008) 2(3) *European Journal of Legal Studies* 193, 205.

171 The characteristics of big data include volume, velocity, variety, value, and validity: see, eg, Ishwarappa and J Anuradha, 'A Brief Introduction on Big Data 5Vs Characteristics and Hadoop Technology' (2015) 48 *Procedia Computer Science* 319, 321.

172 文禹衡 [Wen Yuheng],《数据权力的生成机理、潜在风险与规制路径》[The Generation Mechanism, Potential Risk and Regulatory Paths of Data Power] (2023) 43(5) 西安交通大学学报 *Journal of Xian Jiaotong University* 172, 172.

173 Ibid 173-5.

disadvantage in terms of data resources and lack enough data to make decisions. Thus, they become subject to the dominance of data controllers, resulting in an asymmetrical relationship.

Secondly, asymmetric controller-subject relationships allow data power to emerge, whereas advanced technologies expand and deepen the asymmetry by shaping power distribution.

For one thing, power can be defined as the capacity to establish a dominance relationship.[174] As a result of differences in control over data resources, a dominance relationship has gradually developed between data controllers and data subjects. Therefore, it can be argued that an entirely novel form of power (or quasi-power), namely data power, has arisen. Joseph Nye, a political scientist, asserted that power is shifting away from the 'capital-rich' to the 'information-rich'.[175] Today, this assertion can be modified to read that power is shifting from the 'information-rich' to those with vast amounts of data.

For another, advanced technology has reshaped social power distribution. Power and resources are inseparable.[176] In other words, power holders must possess resources. Previously, governments usually monopolised resources such as the military, police, and prisons. Consequently, individuals and corporations were unlikely to gain traditional power based on these resources. By comparison, data power is based on data resources, unlike traditional power derived resources such as military. In the era of big data, advanced technology has enabled some giant corporations, such as banks, airlines, and large internet companies, to control data resources and thus participate in the distribution of data power. This means that a wider range of data controllers can have power (or quasi-power). Furthermore, traditional power holders can also possess data power simultaneously. Combining traditional power with data power can maximise the advantages of each and produce results that extend beyond what can be achieved using either power alone. On the other hand, as mentioned earlier, individuals may not control data resources. Therefore, they may not share data power. Consequently, the asymmetry between data controllers and data subjects in terms of data power widens and deepens.

Privileging data controllers comes at the expense of data subjects with the result of erosion of personal rights.[177] On the other hand, the divide of power between data controllers and data subjects may not be bridged by granting individuals more micro-rights concerning the processing of their data. One possible explanation is that individual

---

174 Robert Dahl, 'The Concept of Power' (1957) 2(3) *Behavioral Science* 201, 203.
175 Joseph Nye, 'Soft Power' (1990) 80 *Foreign Policy* 153, 164.
176 Joseph Nye, *The Powers to Lead* (Oxford University Press, 2008) 37.
177 Neil Richards and Jonathan King, 'Three Paradoxes of Big Data' (2013) 66 *Stanford Law Review Online* 41, 43.

rights are easily overridden.[178] For example, individuals' right to choose at the time of data collection may be reduced to a simple mouse click without reading privacy notices. Therefore, it is time to conceive an alternative way of confronting data power.

C *Towards a Strengthened Data Protection Paradigm*

As discussed above, the rights-based paradigm, which confers micro-rights concerning data processing upon individuals, falls short in offering sufficient protection due to the rise of data power and the difficulty for individuals to be vigilant, aware, and autonomous when getting involved in complex and stealthy data processing. For individuals to achieve their optimal data protection levels and curb data power, stronger support is necessary. In light of this, this article argues that the state should assume a more affirmative role in realising effective data protection.

To achieve this, it would be necessary to recognise a fundamental right to the protection of personal data at the constitutional level. Corresponding to this constitutional right, the state must eliminate barriers and provide conditions for the realisation of data protection.[179] In this regard, the state would be duty-bound to protect individuals involved in data processing from private entities, particularly those holding data power.[180] Furthermore, the state should provide organisational and procedural guarantees for data protection and cultivate an institutional environment conducive to the realisation of data protection.[181] As a result, the state must be proactive in protecting individuals against the data power of private entities.

Meanwhile, the constitutional right to the protection of personal data would also protect individuals against the state, reflecting the defensive function of constitutional rights.[182] In instances where the state interferes with the constitutional right, individuals could claim against the state to cease the interference, and the claim could be judicially upheld.[183] In this sense, the constitutional right would curtail the data power of public authorities.

The recognition of a constitutional right to the protection of personal data can be achieved in two ways. The first way is to incorporate an

---

178 Purtova (n 170) 205.

179 Donald P Kommers and Russell A Miller, *The Constitutional Jurisprudence of the Federal Republic of Germany* (Duke University Press, 3rd ed, 2012) 60.

180 王锡锌 [Wang Xixin], 《个人信息国家保护义务及展开》[States' Obligations for the Protection of Personal Information] [2021] (1) 中国法学 *China Legal Science* 145, 152.

181 张翔 [Zhang Xiang], 《基本权利的双重属性》[Dual Character of Fundamental Rights] [2005] (3) 法学研究 *Chinese Journal of Law* 21, 26.

182 张翔 [Zhang Xiang], 《论基本权利的防御权功能》[On the Defensive Function of Fundamental Rights] [2005] (2) 法学家 *The Jurist* 65.

183 Ibid.

explicit reference to data protection within the constitution.[184] For example, Article 16 of the *Constitution of Mexico* provides that 'everyone has the right to enjoy protection on his data, and to access, correct and cancel such data'.[185] Likewise, Article 47 of the *Algerian Constitution* declares that '[t]he protection of individuals when handling personal data shall be a fundamental right'.[186] Moreover, as outlined in Article 9A of the *Constitution of Greece*, '[a]ll persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data'.[187]

The second way is to interpret the constitution, treating data protection as underpinning aspects of enumerated rights. For example, the Federal Constitutional Court of Germany in the *Census Act Case*[188] inferred a constitutional right to informational self-determination based on Article 1 (concerning human dignity) and Article 2 (concerning the free development of human personality) of the *German Constitution*.[189] Similarly, it is widely acknowledged that the US Supreme Court in *Whalen*[190] recognised a constitutional right to information privacy.[191] In China, the Constitution and Law Committee of the National People's Congress, tasked with constitutional interpretation and review,[192] affirmed the constitutional underpinning for data protection as the state's respect for and protection of human rights under Article 33, the inviolability of human dignity under Article 38, and the legal protection of citizens' freedom and confidentiality of communication under Article 40 of the *Constitution of the People's Republic of China*.[193]

Notably, the recognition of a constitutional right to the protection of personal data does not conflict with the granting of micro-rights concerning data processing to individuals.[194] While this article

---

184 See, eg, *Constitution of the Kingdom of Thailand* (Thailand) s 32.

185 *Constitución Política de los Estados Unidos Mexicanos* [Political Constitution of the United Mexican States] (Mexico) art 16.

186 *Constitution de la République Algérienne Démocratique et Populaire* [Constitution of the People's Democratic Republic of Algeria] (Algeria) art 47.

187 Το Σύνταγμα της Ελλάδας [Constitution of Greece] (Greece) art 9A.

188 *German Census Act Case of 1983* (n 17).

189 *German Constitution* (n 15) arts 1-2.

190 *Whalen* (n 48) 600.

191 Lin (n 45) 1095-6.

192 《中华人民共和国全国人民代表大会组织法》 [Organic Law of the National People's Congress of the People's Republic of China) National People's Congress, Order 73, 11 March 2021, art 39.

193 全国人民代表大会宪法和法律委员会 [Constitution and Law Committee of the National People's Congress], 《关于<中华人民共和国个人信息保护法（草案）>审议结果的报告》[*Report on the Deliberation Results of the Draft Personal Information Protection Law of the People's Republic of China*] (20 August 2021) <http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313090.html>; 《中华人民共和国宪法》[Constitution of the People's Republic of China] arts 33, 38, 40.

194 吕炳斌 [Lv Bingbin], 《数字时代个人信息保护权利基础的二元融贯论》[The Dualistic Integration Theory of the Right Basis for Personal Information Protection in the Digital Age] [2024] (3) 社会科学辑刊 *Social Science Journal* 110, 112.

contends that micro-rights alone may not be sufficient, it also acknowledges the inappropriateness of completely denying these rights to individuals. Firstly, data subjects are likely to protect their interests by exercising their micro-rights. Secondly, although individuals primarily exercise their rights out of self-interest, such actions can, when viewed from a broader perspective, contribute to the common good. While the exercise of rights by a single data subject has a limited impact on data power, the collective assertion of rights by millions of data subjects can effectively curtail data power.[195] To be specific, extensive objections to and restrictions on data processing, and the erasure of data, can disrupt the integrity and centralisation of data.[196] This consequently weakens data controllers' control over data resources, thereby constraining the formation and operation of data power.[197]

V Conclusion

This article illustrates a discernible shift from interconnection to separation between privacy and data protection in Europe, the US, and China. In Europe, the *EU Charter* has crystallised this evolution. In the US, a variant of privacy akin to data protection — information privacy — has emerged within the broad privacy sphere, indicating a nuanced distinction. In China's legal framework, particularly in the *General Provisions of the Civil Law* and subsequent legislation, a clear distinction exists between privacy and data protection.

Taking a closer look at the Chinese landscape, this article reveals the significant differences between privacy and data protection. Firstly, privacy does not always involve information, whereas data protection specifically deals with personal information. Secondly, while both the public and private sectors are subject to data protection rules, privacy regulations apply exclusively to private entities. Nevertheless, privacy regulations cover a wider range of private entities than data protection rules. Thirdly, the burden of proof differs between cases involving privacy and data protection. In privacy cases, plaintiffs must prove the defendant's fault, whereas in data protection cases, defendants are required to prove they are not at fault. Finally, for plaintiffs to receive compensation for mental damage resulting from privacy invasions, the damage must be serious. In contrast, plaintiffs are entitled to compensation equivalent to mental damage caused by data protection infringements, whether the damage is serious or not.

The current data protection paradigm, which is individual-centric and rights-based, faces challenges in the big data era, particularly in

---

195 文禹衡 [Wen Yuheng] (n 172) 178.
196 Ibid.
197 Ibid.

addressing power asymmetry between data controllers and subjects. To achieve substantive fairness and effective data protection, the state must take a more proactive role. Recognising a fundamental right to the protection of personal data is crucial in adapting to the challenges and ensuring robust safeguards for individuals in an increasingly data-driven world.