Penn State Journal of Law & International Affairs

Volume 8 | Issue 1

May 2020

China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?

Emmanuel Pernot-Leplay

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2020 VOLUME 8 NO. 1

CHINA'S APPROACH ON DATA PRIVACY LAW: A THIRD WAY BETWEEN THE U.S. AND THE EU?

Emmanuel Pernot-Leplay[*]

ABSTRACT

Because of state surveillance, data privacy in China is often assumed to be inexistent. Yet, the country regulates differently privacy from the state and privacy from private actors. Consumer data privacy in China is at the forefront of new regulations issued during the last years to create a legal framework on data protection, up to the Cybersecurity Law. Despite the tremendous increase of data transfers from the West to China, there is a scarcity in the legal research about Chinese data protection rules, the building of China's approach on this domain and its consequences.

This Article compares China's data privacy laws (most notably the Cybersecurity Law and its guidelines) to the dominant approaches coming from the EU and the U.S. The goal is to identify China's direction, whether it transplants their rules, and the specificities that make China's approach different from Western models. The results of this comparative study show that China initially followed a path resembling the U.S. approach, before recently changing direction and converge with the more stringent EU rules on several legal elements, especially through the Cybersecurity Law and the Personal Information Security Specification. Up to the point that China now has a comprehensive data protection law on its legislative agenda and encourages privacy protection for consumers that sometimes surpasses U.S. rules.

This research identifies and decrypts specificities of data protection in China that make China's voice special with the potential to gain influence in this field, whereas Western rules are the only bearing regulatory clout so far. These Chinese characteristics, such as the paradoxical – yet parallel – increase of both state surveillance and consumer privacy and the cyber-sovereignty principle impacting personal data protection, now compose China's approach. This "data privacy with Chinese characteristics" will bear consequences on the country's forthcoming regulations on artificial intelligence and for future policy developments in the EU and the U.S.

TABLE OF CONTENTS

I. INTRODUCTION

China is undergoing a rapid development of its data privacy framework. While the legal literature on personal data protection and privacy[1] focuses on the EU and the U.S. approaches, little consideration is given to Chinese laws. The predominance of the EU and the U.S. in personal data processing and transfers, coupled with their starkly opposed approaches, explain why it concentrates the debates. But the ever-increasing data exchanges and use of Chinese technologies in the West convey the need for such research. On the other hand, there was admittedly little material on data privacy in China to be analyzed and compared until recently, and the discussions on privacy in China revolved around concerns on state surveillance (they still mostly do). Therefore, this Article proposes to identify China's direction on data protection, especially in comparison to the EU and the U.S. approaches, to underline the specificities that make it unique and the consequences they may engender in the field.

Unlike the EU and the U.S., data protection regulations in China are overdue. In 2010, Xue argued that "[b]oth the domestic social economic development and the international trade and economic exchange will eventually push China to observe the international standard of privacy and personal data protection."[2] For Greenleaf in 2012, "China's direction [on data protection] is unknown," with only "piecemeal and incoherent" initiatives which led

---

* Ph.D candidate in comparative law at Shanghai Jiao Tong University, Koguan Law School, focusing on data protection and privacy rules in the EU, the U.S. and China. Data privacy consultant at Deloitte Cyber Risk services. I am grateful to the editors of the *Penn State Journal of Law & International Affairs* for their remarkable editorial assistance, even during the pandemic.

[1] This Article uses "data protection" and "privacy" as synonyms. Research comparing both rights however find that, despite similarities, some differences exist under EU law, *see generally* Juliane Kokott & Christoph Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIV. L. 222, 222–28 (2013). The authors argue that "[a] closer appreciation of the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union shows that despite substantial overlaps there are also important differences, in particular with regard to the scope of both rights and their limitation."

[2] Hong Xue, *Privacy and personal data protection in China: An update for the year end 2009*, 26 COMPUTER L. & SEC'Y REV. 284, 289 (2010).

him to leave China out of his seminal comparative article.[3] However, he stated that if these are "replaced or supplemented by a national data privacy law, China may well influence developing countries and China's trading-partners."[4] By 2014, China had taken the first steps to bring protection to personal data but its approach was still very limited compared to other nations. This situation let scholars expecting more, with the vision that China's voice on data privacy will become more influential.[5] Only four years later, in 2018, an expert who took part in the drafting of China's latest guidelines stated that "we are stricter than the U.S., but not as much as the EU."[6] Such a statement, if verified, suggests significant changes in Chinese laws within a relatively short timeframe and that China positions itself as in between the U.S. and EU approaches. This Article, then, is the first substantial effort to compare and position Chinese laws on data privacy with the EU and U.S. models, and determine their direction and underline the specificities that constitute China's own nascent approach.[7]

The EU and U.S. models are indeed well established, yet antagonistic. Both sides of the Atlantic have a different philosophy underlying their approach, which leads to differences in the legal instruments used and the level of protection afforded to individuals. In the EU, the rights to privacy and to the protection of personal data are both fundamental rights and are protected by a comprehensive

---

[3] Graham Greenleaf, *The influence of European data privacy standards outside Europe: implications for globalization of Convention 108*, 2 INT'L DATA PRIV. L. 68, 72 (2012).

[4] *Id.* at 72.

[5] LEE ANDREW BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 209 (2014). Bygrave states that "[China] will increasingly have a voice on data privacy issues, although the importance of its message remains to be deciphered, let alone clearly heard" (alteration to the original).

[6] Yanqing Hong, *Responses and explanations to the five major concerns about the Personal Information Security Specification*, WEIXIN (Feb. 5, 2018), https://mp.weixin.qq.com/s/rSW-Ayu6zNXw87itYHcPYA.

[7] *But see* the work of experts such as Graham Webster (Editor-in-Chief of the Stanford-New America DigiChina Project at the Stanford University Cyber Policy Center and China Digital Economy Fellow at New America) and Samm Sacks (Senior Fellow at Yale Law School's Paul Tsai China Center and a Cybersecurity Policy Fellow and China Digital Economy Fellow at New America), supporting similar ideas in their reports, commentaries and contributions in media cited in this Article.

legal standard. The law has a wide scope; it applies to all organizations collecting and processing personal data. Personal data is broadly defined to cover all information relating to an individual. The law provides strong guarantees for those individuals, that the General Data Protection Regulation ("GDPR")[8] recently furthered, confirming the EU direction. In the U.S., conversely, there is no federal law covering all aspects of data privacy. Relevant provisions are instead scattered among many laws regulating different topics and sectors, with a variety of scope. They may concern government agencies, data on children, health data, focus on data breaches and being a federal law or a state law. They typically establish less requirements and offer less protection than in the EU. The EU model is proven to be increasingly influential on third-countries' laws[9] at the expense of the U.S. way which has not attained the same success.[10] If, in terms of consumer data privacy, China shows signs of convergence toward the EU model, it would leave the U.S. isolated with its minimalist approach.

China started to develop its data privacy framework much later than the EU and the U.S. Faced with the problem of lacking these regulations (such as numerous data breaches), China has the possibility to turn to existing models solving the same issue, and to import their rules into its domestic law. This phenomenon, called legal transplantation ("the moving of a rule or system of law from one country to another"),[11] is well-known in comparative law scholarship. This Article finds that China did progressively include international principles of privacy and data protection in its laws, initially at a very slow pace. The country first considered going the EU route with a comprehensive law covering the entire scope of personal data, before renouncing and resorting to a U.S.-like approach, *i.e.* several sectorial

---

[8] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[9] *See generally* Greenleaf, *supra* note 3.

[10] *See generally* Ryan Moshell, *And then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection*, 37 TEX. TECH L. REV. 357 (2004).

[11] ALAN WATSON, LEGAL TRANSPLANTS: AN APPROACH TO COMPARATIVE LAW 21 (1 ed. 1974).

laws offering limited protection. But, unlike in the U.S., data privacy rights focus solely on *consumer*s whereas *citizens* do not enjoy the same level of protection as part of their civil liberties. Bearing this difference in mind, consumer privacy in China continued to progress through various types of legal instruments, either binding or non-binding—the latter being more influential that could be assumed from a Western point of view. These progresses now culminate with data protection principles in Chinese rules going beyond what exists in U.S. laws and the OECD guidelines on data privacy ("OECD Privacy Guidelines"),[12] getting closer to the EU on such requirements as additional safeguards for sensitive data, processing of personal information only for the purpose initially specified to the individual, or data portability.

Given the legal and political differences between Western countries and China, a straightforward transplantation would face significant challenges. China instead does not depart from its own rationale, and even creates specificities of its own, in the same way that EU and U.S. different underlying philosophies engender their divergent approaches. Like the well-known "socialism with Chinese characteristics" developed by Deng Xiaoping,[13] there is a "data privacy with Chinese characteristics," made notably of the consequences of the cyber-sovereignty principle and the separation between privacy from private actors and privacy from the government. This reflects both the country's sociopolitical context and geopolitical ambitions, and defines China's own approach to the question.

The present research develops and details these arguments in the following way: Part I briefly presents EU and U.S. approaches and outlines their differences. This frames the two models China could import rules from and that serve as references throughout this study. Part II focuses on the first period of China's building of its legal

---

[12] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines), 1980, OECD, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[13] Deng Xiaoping first used the phrase in his Opening Speech at the Twelfth National Congress of the Communist Party of China, on September 1, 1982. Deng Xiaoping, Opening Speech at the Twelfth National Congress of the Communist Party of China (Sept. 1, 1982), http://en.people.cn/dengxp/vol3/text/c1010.html (last visited Sep 6, 2019).

framework and details the legal instruments used. It shows that the Chinese approach first scatters data protection provisions in various laws, which resembles the U.S. way, before widening the scope of its rules and now being on the verge of adopting a comprehensive law on data privacy, the type of legal instrument that the EU favors. Some of this progress happens through non-binding texts, but the study underlines their special status in China's legal system. Part III then performs a deeper analysis on the content of the latest laws, *i.e.* the Cybersecurity Law and its accompanying non-binding standard, being the most significant and comprehensive rules in China to date. The comparative analysis demonstrates a significant change in China's direction: while some key legal elements remain notably different from EU rules and still closer to the U.S. approach, others bear eloquent signs of EU influence. Finally, Part IV goes beyond the comparison and supports that China's data privacy legal framework is more than a legal transplantation of pre-existing Western models and instead features characteristics that are specific to China, together with the legal transplants. Undoubtedly, this "data privacy with Chinese characteristics" will globally weigh in on future policy developments and discussions.

II. EU'S STRONG PROTECTION OR U.S.'S MINIMALIST APPROACH: THE TWO MODELS FOR CHINA

The EU and the U.S. began to build their legal framework on data protection around the same time. However, they each have their own philosophy underlying their approach, which led them to feature significant differences in both legal instruments (I.A) and level of protection. (I.B)

A. Underlying Philosophy and Legal Instruments

The EU and the U.S. both have a long experience in regulating the protection of personal information. Conversely, China, like other countries, developed its data privacy laws later than these two blocks. In the field of comparative law, the literature on legal transplantation shows that a country confronting a problem will first turn to solutions

developed in foreign countries to solve a similar issue.[14] A well-known example of legal transplantation in China is the Anti-Monopoly Law, which borrows from both European and U.S. rules.[15] In personal data protection, China also has these two reference models to draw inspiration from. However, the U.S. and EU models are largely diverging from each other.

Data protection emerged at the same time in the U.S. and in EU Member States, during the 1970s. Both were based on common data protection principles.[16] In the beginning of the 1980s, the OECD issued its Privacy Guidelines and the Council of Europe passed the Convention 108,[17] both featuring a set of core data protection principles. The OECD Privacy Guidelines are a soft law instrument and its basic principles are considered to be the minimum international standards, widely found in data protection laws.[18] On the other hand, the Convention 108 contains more stringent provisions than the OECD Privacy Guidelines and is the only international legally binding

---

[14] Jonathan M. Miller, *A Typology of Legal Transplants: Using Sociology, Legal History and Argentine Examples to Explain the Transplant Process*, 51 AM. J. COMP. L. 839, 845–46 (2003). Miller identified several types of legal transplants from one country to another. Among them, the "cost-saving transplant" happens when a country uses a reference model to transplant rules from, rather than creating its own approach at the expense of a long and costly process. Other types of transplants are the externally-dictated transplant, the legitimacy-generating transplant and the entrepreneurial transplant.

[15] *See*, *e.g.*, Wentong Zheng, *Transplanting antitrust in China: economic transition, market structure, and state control*, 32 U. PA. J. INT'L L. 643 (2010).

[16] Colin J Bennett, *Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States*, 1 GOVERNANCE: INT'L J. POL'Y AND ADMIN. 415, 421–24 (1988). Bennett noted the similarities of regulations from countries having different cultural and legal backgrounds, which allows to identify a common core of data protection principles. As a result, "[w]hile the codification of these principles may vary, their substance is strikingly similar."

[17] Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108.

[18] Greenleaf, *supra* note 3, at 73.

instrument in the field, meaning that countries adhering to the convention must pass laws reflecting its principles.[19]

Differences between U.S. and EU approaches started to appear when the European Commission asked EU Member States to ratify the Convention 108, leading them to bring in their laws more stringent protections than recommended by the OECD Privacy Guidelines. From then on, differences between EU and U.S. approaches were characterized by their choice of legal instruments, their scope and the level of protection afforded to individuals. These elements amount to a great divergence between the two. The underlying reason for it is the rationale that drives each of these approaches. In the EU, abuses on privacy and personal information during and after World War II justified providing strong protections, as exemplified by early German and French rules.[20] Privacy and personal information protection are now fundamental rights in the EU.[21] In the U.S., data privacy rights are balanced with other interests such as commerce and state security agencies;[22] moreover, data privacy

---

[19] Despite being from the Council of Europe, and even if members to the Convention were all European initially, the Convention is open to any country for ratification; recently more and more foreign countries are joining it or considering doing so: "Although it originated from the Council of Europe, since 2011 data protection Convention 108 is steadily being 'globalised'. In addition to its 47 European parties, five countries outside Europe are now Parties: Uruguay, Mauritius, Senegal, Tunisia and Cape Verde . . . Four more countries have had Accession requests accepted, but have not yet completed the accession process: Morocco, Argentina, Mexico, and Burkina Faso. Eleven other countries, or their [data protection authorities], are now Observers on its Consultative Committee", GRAHAM GREENLEAF, *Convention 108+ and the Data Protection Framework of the EU (Speaking Notes for Conference Presentation)* (2018), https://papers.ssrn.com/abstract=3202606.

[20] Moshell, *supra* note 10, at 359.

[21] In its Article 8, the Charter of Fundamental Rights in the European Union provides that everyone has the right to the protection of personal data, which should be processed on a legitimate legal basis such as consent, that everyone has the right of access to their personal data and the right to have it rectified, and that an independent authority shall control compliance with these rules. Charter of Fundamental Rights of the European Union, Dec.7, 200 art. 8, 2012/C 326/02.

[22] Shawn Marie Boyne, *Data Protection in the United States*, 66 AM. J. COMP. L. 299, 301 (2018); Stephen Cobb, *Data privacy and data protection: US law and legislation*, ESET WHITE PAPER 1 (2016).

finds itself facing the right to free speech as protected by the First Amendment of the U.S. constitution[23]—sometimes referred to as "the most significant factor in counterbalancing privacy protections in the U.S."[24]

The first main consequence of it bears on the legal instruments used to protect personal data. The EU built its model through one main law that governs the field, known as a "comprehensive data protection law." This model took shape in 1995 with the Directive on data protection (Directive 95/46/EC),[25] with two main goals: the protection of fundamental rights of natural persons, in particular their right to privacy with respect to the processing of personal data and to prevent barriers to the free flow of data in the Union.[26] It has since been replaced by the General Data Protection Regulation ("GDPR")[27] in 2018. This comprehensive law is complemented by rules operating as a *lex specialis*, such as the E-Privacy Directive[28] and the forthcoming E-Privacy Regulation, whereas the comprehensive law is the *lex*

---

[23] U.S. Const. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.").

[24] UNITED STATES - THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 269 (Alan Charles Raul, Frances Faircloth, and Vivek K. Mohan, eds., 4 ed. 2017). *See also* Paul M. Schwartz, *The EU-U.S. Privacy Collision: a Turn To Institutions and Procedures*, 126 HARV. L. REV. 1966, 1976–77 (2013). Schwartz reminds that in *Sorrell v. IMS Health Inc.*, the Supreme Court struck down a Vermont law against the sale of information about doctors' prescribing practices by retailers (then used to target doctors for the sale of pharmaceuticals), as the Court held that the law violated the First Amendment.

[25] Directive 95/46/EC, of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281).

[26] *Id.* at art. 1.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 2016 O.J. (L 119/1).

[28] Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (E-Privacy Directive), as amended by the EU telecoms reform package from November 2009.

generalis. Under the GDPR, Member States have very limited possibilities for adapting the rules.[29] This EU model is now followed by an increasing number of countries in the world.[30]

Among countries that built a legal framework for the protection of personal information, the U.S. remains the greater exception to that trend.[31] The U.S. situation is much more fragmented, where privacy is protected by a patchwork of common law, federal legislation, state law, and certain state constitutions.[32] Scholars have found that the U.S. Constitution and its supporting body of jurisprudence do not provide adequate privacy protection and, therefore, the absence of a constitutional right to privacy means that data privacy acts could clash with constitutional rights, therefore limiting their effectiveness.[33] The U.S. numerous legal instruments containing data privacy protections are sector-specific, as they regulate a narrow area, such as health care, communications, or finance and credit.[34]

Among laws aimed at protecting from the government, the Privacy Act of 1974 applies to data processing by the federal government (but not state governments),[35] the Electronic Communications Privacy Act of 1986, protects individuals from the interception of their electronic communications such as emails and other records by government officials, and the Family Educational

---

[29] For example, Member States can define the age of a "child" in their domestic law, but within limits, according to Article 8(1) of the GDPR: "[. . .] the processing of the personal data of a child shall be lawful where the child is at least 16 years old. [. . .] Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."

[30] GRAHAM GREENLEAF, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority* (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529 (last visited Aug. 13, 2019).

[31] *See generally* Moshell, *supra* note 10. *See also* Greenleaf, *supra* note 3, at 70–2.

[32] Avner Levin & Mary Jo Nicholson, *Privacy law in the United States, the EU and Canada: the allure of the middle ground*, 2 U. OTTAWA L. & TECH. J. 357, 360 (2005).

[33] *Id.* at 367.

[34] Schwartz, *supra* note 24, at 1974–75.

[35] Cited as Privacy Act of 1974, 5 U.S.C. § 552a.

Rights and Privacy Act, safeguards students at institutions receiving federal funding from the disclosure of their personal data without their consent, in addition to the rights of access and modification. Among the main sectorial laws regulating the private sector, the 1996 Health Insurance Portability and Accountability Act provides protection of personal information related to an individual's health, and the Children's Online Privacy Protection Act of 1998 protects the privacy of children under the age of 13 against collection and misuse of personal data by commercial websites. Other laws protect financial information, communications, video rental records, or telephone and family information.[36] A large number of state laws add another layer of regulations. As an answer to growing concerns over data privacy, these state laws and their recent updates tend to increase the protections required from businesses to consumers.[37] The most debated of them is the California Consumer Privacy Act ("CCPA"),[38] often wrongly presented as similar to the GDPR[39] or dubbed "California's GDPR."[40] Although the CCPA indeed significantly strengthens protections, it remains a law with a narrower scope and weaker protections than the EU standard.[41]

---

[36] Levin and Nicholson, *supra* note 32, at 363–67.

[37] Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model?*, 18 COLO. TECH. L. J. (forthcoming).

[38] Cal. Civ. Code ¶ 1798.100-198, taking effect on January 1, 2020.

[39] *E.g.* Andy Patrizio, *While no one was looking, California passed its own GDPR*, NETWORK WORLD (July 5, 2018, 6:23 AM PDT 2018), https://www.networkworld.com/article/3286611/while-no-one-was-looking-california-passed-its-own-gdpr.html.

[40] *E.g.* Michael Bahar et al., *California's GDPR has become law*, LEXOLOGY (June 29, 2018), https://www.lexology.com/library/detail.aspx?g=639a495e-290c-463b-9f6a-2656ed8b61f7.

[41] The CCPA only protects California residents in their relationship with business as consumers (at the time of writing those lines, policymakers still discuss whether the CCPA should cover personal data of employees as well) and those concerned businesses must cross certain threshold to be subject to the law. The protections granted are significantly lower than the GDPR, *e.g.* there is no requirement for a legal basis for data collection and processing and the right of action for individual is limited to security issues in the context of a data breach (the bill SB 561, which would have expanded the private right of action to allow consumers to sue for any violations of the CCPA has failed to pass in the Senate on May 16, 2019).

Not only do U.S. rules apply to a narrow set of entities, but they also limit their protection to *U.S. citizens* and *residents*,[42] whereas EU rules protect the much broader *identifiable natural persons*, regardless of their citizenship.[43] The definition of "personal information"—which conditions the applicability of the protections—is also often narrower in the U.S.[44] and requires the actual name of a person and information such as numbers identifying them directly[45] to be part of a data set for them to be considered personal data. Due to the U.S. piecemeal approach, the very concept of personal information differs between the various legal instruments and there is no overarching definition of it.[46]

Under the "notice and choice"[47] mechanism, that the U.S. prefers to protect consumers' personal information, the various obligations coming from these laws are typically stated in privacy policies where companies disclose their data practices, so individuals can choose to accept the collection and use of their data. The rationale being that consumers would favor the most protective companies, leading those companies to compete on privacy protection. However, this system's efficiency is widely criticized.[48]

---

42 Privacy Act of 5 U.S.C. § 552a(a)(2): "the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence." The most recent state laws feature the same disposition, *e.g.* in California, the CCPA defines a consumer as "a natural person who is a California resident," CCPA, 1798.140.(g).

43 GDPR art. 4(1).

44 Paul Schwartz & Daniel Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 879 (2014). Certain laws feature a broadened definition, such as the CCPA.

45 *E.g.* in the latest Colorado rules on personal data protection (HB 18-1128, which took effect September 1, 2018, herein after "Colorado Consumer Data Privacy Law"), "personal information" is defined as a Colorado resident's first name or first initial and last name in combination with "personal identifying information" such as the numbers assigned to a person (social security number, ID card number, driver's license number . .), Colorado Consumer Data Privacy Law § 3 (1)(g)(I)(A).

46 Schwartz and Solove, *supra* note 44, at 888.

47 Also called "notice and consent."

48 *See, inter alia,* Joel R. Reidenberg et al., *Privacy harms and the effectiveness of the notice and choice framework*, 11 ISJLP 485 (2015); Fred H. Cate, *Protecting privacy in health research: the limits of individual choice*, 98 CALIF. L. REV. 1765 (2010).

These differences in philosophies and legal instruments form a divergence in content and level of data protection. U.S. laws cover less core data protection principles and in a lighter manner than their EU counterparts.[49]

B. Core Principles in Data Protection Laws

Despite their opposition, data protection laws on both sides of the Atlantic share several core data protection principles, identified by previous research.[50] According to Professor Paul Schwartz, a leading data protection law scholar,[51] they are "the building blocks of modern information privacy law,"[52] although not all laws on data protection contain the same number of principles nor do they give them the same meaning or depth.[53] A comparison of data protection laws should therefore be based on those principles. They are often interdependent, sometimes intertwined. Some are shared by major sources across the world and known as "global standards," while others are specific to European instruments—whether they created or significantly enhanced them—and referred to as "European standards."[54]

The core data protection principles were first explicitly listed in the 1970s in the U.S., before being a central part of the OECD Privacy Guidelines and the Convention 108, and spreading to the EU Directive 95/46/EC, the guidelines from the Federal Trade Commission ("FTC"), or the APEC Privacy Framework[55] among

---

49 Schwartz, *supra* note 24, at 1976.

50 *See, e.g.*, Anneliese Roos, *Core principles of data protection law*, 39 COMP. AND INT'L L. J. OF S. AFRICA 102 (2006). Roos compares several sources in Europe and in the U.S. to identify a set of core data protection principles used in these legal instruments.

51 In relation to data protection principles, Schwartz proposes to apply all of them when information refers to an *identified* person, whereas information referring to an *identifiable* person should be protected by less principles, *see* Paul M. Schwartz & Daniel J. Solove, *The PII problem: Privacy and a new concept of personally identifiable information*, 86 N.Y.U. L. REV. 1814, 1880 (2011).

52 Paul M. Schwartz, *Privacy and democracy in cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999).

53 Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902, 908 (2008).

54 Greenleaf, *supra* note 3, at 73.

55 The Asia-Pacific Economic Cooperation ("APEC") is a forum promoting free-trade in the region, composed of 21 countries. To improve data protection

others.[56] Among the most common principles found in legal systems, there are the requirements that data must be processed fairly and lawfully (fairness and lawfulness principle), data should only be processed pursuant to the purpose specified to the individual (purpose specification), only the personal information necessary for that purpose should be collected and processed and then be deleted (data minimization), such data should be relevant, accurate and up-to-date (data quality), individuals should be made aware of the processing and of their rights (transparency), these rights should allow individuals to exercise control over the processing, *i.e.* through modifying, rectifying or deleting the data or objecting to their processing (data subject participation), additional safeguards should be provided to special categories of data (sensitivity), all data should be appropriately protected against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data (security and confidentiality), and data controllers should be accountable for compliance with measures giving effect to these principles (accountability).[57] In addition to those principles, other requirements exist, such as having an independent supervisory authority dedicated to data protection, restrictions on cross-border transfers to countries with a lower level of protection, safeguards on automated decision-making, etc.[58]

Some principles and requirements exist in both the EU and the U.S. but are more stringent in Europe, *e.g.* data minimization, transparency and data quality requirements are stricter in Europe. Some are simply missing in the U.S. approach, such as additional protection for sensitive data, restrictions on cross-border transfers, the need for a legal basis for data collection and processing, oversight by

---

standards throughout member countries, the APEC adopted in 2004 a framework containing minimal data protection standards (APEC Privacy Framework). This framework is non-binding, countries can freely decide whether to implement the provisions it contains.

[56] For a detailed analysis of the history of the fair information practice principles, *see* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343, 345–55 (Jane K. Winn, ed., 2006). In this article, Cate argues against an overreliance on the "notice and choice" mechanism.

[57] Roos, *supra* note 50.

[58] Those additional elements will typically belong to the "European standards" category, as European rules contain more protections than others.

an independent supervisory authority, and limits on profiling and automated decision-making.[59] Previous comparative research identified the spreading of EU standards in third countries' laws; China was however excluded from its scope, because of the lack of rules to be studied.[60]

Therefore, this Article proposes a framework for comparing data protection laws that assesses different legal areas: the underlying philosophy of the approach, the legal instruments employed for the regulation, and the presence and substance of core data protection principles. This study aims at outlining the direction of Chinese laws in regard to these two main approaches on data protection that are the EU and the U.S. models, *i.e.* China's convergence with either of them, through the comparison of the above-mentioned elements. Because legal *convergence* implies dynamism and movement, it is different from the concept of *similarity* of laws. The practical particularity of a convergence research is thus the construction of the comparison within a timeframe, as exemplified by political science scholars.[61] Therefore, although a greater emphasis is put on the latest Chinese laws to precisely understand the current position, the main previous laws are also assessed to draw meaningful conclusions on the country's direction.

The relevant timeframe for China is much shorter than for most Western countries. It starts in the 1990s for the first mentions of "privacy," and not before the 2010s for significant rules on "personal information protection" and the inclusion of core data protection principles.

III. CHINA'S BELATED BUILDING OF ITS LEGAL FRAMEWORK

Chinese laws on data privacy arrived decades after most Western countries and China first hesitated between the EU and U.S.

---

59 Schwartz, *supra* note 24, at 1976.

60 Greenleaf, *supra* note 3, at 72.

61 Colin J. Bennett, *What is policy convergence and what causes it?*, 21 B. J. POL. SCI. 215, 230 (1991). Bennett's theory on policy convergence is that it "should also be conceptualized in dynamic terms. The relevant theoretical dimension is time rather than space. Otherwise the concept becomes a synonym for similarity".

approaches on legal instruments (II.A). Although the country eventually started to develop its legal framework through sector-specific laws much like in the U.S. (II.B), China is now on the path of enacting a comprehensive data protection law as favored by the EU (II.C).

A. The Late Emergence of Data Privacy Rights

Before any data protection rule could exist in China, the country had to bring out the right to privacy, as the first step towards to the protection of personal information. In China like in other countries, the idea of privacy was initially very little developed. Across the world, different cultures led to the same lack of privacy protection. The prevalent characteristics of societies of that time—strict moral and behavioral social norms, important rural communities with deep social ties—constituted an adverse environment for privacy protection.[62] During the nineteenth century, the development of the urban life providing a relative anonymity among the multitude, coupled with new liberal ideas and individual rights gained through revolutions, led to the conception of the right to privacy. One of the first mentions of this right appeared in the U.S. in 1890.[63] Scholarly discussions continued during the beginning of the twentieth century, but the right to privacy did not really flourish until after the Second World War, when the individual became more important in democratic legal systems—which explains why China was not part of this movement. The corollary right to data protection appeared in the 1970s, following the spread of informatization, when the U.S. and several European states moved beyond privacy protection and issued their first laws focused on personal data protection, starting to build the two models discussed above.[64]

---

[62] *E.g.* in France, prior to the French Revolution, impotent men had to fulfil their conjugal duty in public in order to avoid the annulment of marriage, *see* PIERRE DARMON, LE TRIBUNAL DE L'IMPUISSANCE: VIRILITÉ ET DÉFAILLANCES CONJUGALES DANS L'ANCIENNE FRANCE (1979).

[63] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). It defines the right to privacy as the "right to be let alone," in a reaction to the development of journalism and gossip columns.

[64] *See supra* Part I.

It has been argued that traditional Chinese culture caused the lack of privacy protection.[65] However, in culturally similar regions, Taiwan has data protection laws going beyond OECD standards[66] and Hong Kong was the first jurisdiction in Asia to have enacted a comprehensive data privacy law.[67] In mainland China, it's rather the political situation, at a time when privacy was making a breakthrough at international and national levels, that decisively precluded the emergence of privacy protection and set China apart from the developments happening elsewhere.

While Western countries were expanding privacy rights to personal data protection, the concept of a right to privacy only started to appear in China, in a series of high-level laws not mentioning personal information protection. The Constitution from 1982[68] states the inviolable character of one's personal dignity.[69] Whereas protection of personal information does not appear, the right to freedom and privacy of correspondence is explicitly stated in Article 40,[70] and privacy at home is implied in article 39.[71] However, the Constitution

---

65 For a details discussion on those Chinese particularities, *see* Tiffany Li, Jill Bronfman & Zhou Zhou, *Saving Face: Unfolding the Screen of Chinese Privacy Law*, J. L., INFO., & SCI., 4 (forthcoming), https://papers.ssrn.com/abstract=2826087.

66 Hui-ling Chen & Michael Fahey, *Data protection in Taiwan: overview*, PRACTICAL LAW (Oct. 1, 2018), https://uk.practicallaw.thomsonreuters.com/5-578-3485?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 .

67 YUETMING THAM, HONG KONG - THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW (5 ed. 2018).

68 People's Republic of China Const. (Dec. 1982) [*hereinafter* PRC Const.].

69 PRC Const. art. 38: "The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false charge or frame-up directed against citizens by any means is prohibited."

70 PRC Const. art. 40: "Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law."

71 PRC Const. art. 39: "The home of citizens of the People's Republic of China is inviolable. Unlawful search of, or intrusion into, a citizen's home is prohibited."

cannot serve as the legal ground for a judicial decision or interpretation in China,[72] which undermines the significance of these provisions.

Civil and criminal laws now provide privacy and personal information protection. In 1986, the General Principles of the Civil Law ("GPCL")[73] protect the "right to reputation" and serve as a basis for privacy protection.[74] On March 15, 2017, the GPCL received an update,[75] providing rules for protection of personal data and underlining the responsibility of individuals and organizations for data protection and collection.[76] The Criminal Law and its Amendment VII from 2009[77] sanction wrongdoings on privacy and personal information on several occasions. Article 252 states that attempting to infringe upon the right to freedom of correspondence is punishable by a prison sentence.[78] As are activities of selling and illegally providing personal data by persons working at state organs or key institutions of finance, telecommunications, which they may have obtained during

---

[72] Qianfan Zhang, *A constitution without constitutionalism? The paths of constitutional development in China*, 8 INT'L J. CONST. L. 950, 950–1 (2010).

[73] General Principles of the Civil Law of the People's Republic of China, promulgated on April 12, 1986 and came into force on January 1, 1987.

[74] For further discussion of the protection of privacy by the GPCL, *see* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS : TRADE AND HUMAN RIGHTS PERSPECTIVES 200–01 (2014), http://dx.doi.org/10.1093/acprof:oso/9780199679669.001.0001.

[75] The update took effect on October 1, 2017.

[76] GPCL art. 111: "The personal information of natural persons is protected by law. Where any organization or individual needs to obtain someone else's personal information, they shall obtain it in accordance with law and ensure information security; they must not unlawfully collect, use, process, or transfer the personal information of others, and must not unlawfully buy, sell, provide or disclose others' personal information."

[77] Criminal Law of the People's Republic of China (adopted on July 1, 1979 (Criminal Law) and Amendment Seven to the Criminal Law, adopted on February 28, 2009).

[78] Criminal Law art. 252: "Whoever conceals, destroys or unlawfully opens another person's letter, thereby infringing upon the citizen's right to freedom of correspondence, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of no more than one year or criminal detention."

their service.[79] The Tort Liability Law[80] from 2010 explicitly protects the right of privacy for the first time,[81] along with the right of reputation and the right of honor.[82] The law also protects patients' privacy data and medical history data as their disclosure requires consent.[83] However, very few actions have been tried or accepted by the courts following the enactment of the Tort Liability Law.[84]

In the regulation of businesses' use of personal data, the first Chinese dispositions on the field were overall more concerned with public security than personal privacy.[85] The emergence of innovations such as cloud computing and big data analytics convinced China to more vigorously regulate privacy, a trend later further encouraged by Edward Snowden's revelations and by the related fear over foreign

---

[79] Criminal Law art. 253 (A): "Where any staff member of a state organ or an entity in a field such as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others, shall, if the circumstances are serious, be sentenced to fixed-term imprisonment of no more than three years or criminal detention, and/or be fined. [. . .]"

[80] The Tort Liability Law of the People's Republic of China (adopted at the 12th Meeting of the Standing Committee of the Eleventh National People's Congress of the People's Republic of China on December 26, 2009, effective July 1, 2010) (Tort Liability Law).

[81] Hanhua Zhou, *Consumer Data Protection in China*, *in* CONSUMER DATA PROTECTION IN BRAZIL, CHINA AND GERMANY-A COMPARATIVE STUDY 42 (Rainer Metz et al. eds., 2016).

[82] Tort Liability Law art. 2: "'Civil rights' as mentioned in this Law refer to personal and property rights and interests, including, inter alia, the right to live, right to health, right of name, right of reputation, right of honor, right to portrait, right to privacy, right of self-determination in marriage, guardianship, ownership, usufructuary right, real right for security, copyright, patent right, exclusive right to use trademark, right of discovery, stock rights, and right of inheritance."

[83] Tort Liability Law art. 62: "Medical organizations and their medical personnel shall ensure the privacy and confidentiality of patients. Medical organizations and their medical personnel shall bear tort liability if they disclose a patient's private matters or medical records without the patient's consent and cause damage to the patient."

[84] Li, Bronfman, and Zhou, *supra* note 65, at 24.

[85] Yanfang Wu et al., *A comparative study of online privacy regulations in the U.S. and China*, 35 TELECOMMUNICATIONS POL'Y 603, 613 (2011).

intelligence practices.[86] Since, within this context of security enhancement, the inclusion of core data protection principles has started to grow.

In December 2012, the Standing Committee of the National People's Congress ("NPC")[87] promulgated the Decision on Strengthening Information Protection on Networks, effective immediately ("the 2012 NPC Decision"), then the highest level law in China about personal information protection.[88] The 2012 NPC Decision explicitly states that its goal is protect network information security, protect the lawful interests of citizens and to *safeguard national security and social order*[89]—a motivation that is unique to China and not found in EU or U.S. laws. It broadly applies to "network service providers and other enterprise and undertaking work units that collect or use citizens' individual electronic information during their business activities."[90] The electronic information is defined as information that can identify citizens and involve their privacy.[91] The Decision encompasses several core data protection principles. In particular, Article 2 which specifies that network service providers shall "abide by the principles of legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain agreement from the person whose data is collected, they may not violate the provisions of laws and regulations, and the agreement between both sides, in collecting or using information."[92]

Following the Decision, China has made significant efforts and progress in terms of developing the protection of personal data

---

86 Graham Webster, Lecture at New York University, Shanghai Campus (Dec. 6, 2017).

87 The Standing Committee is the permanent body of the National People's Congress and holds the legislative power with it.

88 Adopted on 28 December, 2012 at the 30th Committee Meeting of the 11th NPC Standing Committee. Retrieved from https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection (last visited Aug. 24, 2019).

89 Preamble of the 2012 NPC Decision.

90 2012 NPC Decision art. 2.

91 2012 NPC Decision art. 1.

92 2012 NPC Decision art. 2.

through including several principles and requirements as part of later rules. But rather than enacting an omnibus data privacy law in the European way, China continued on a path resembling the U.S. approach, with data protection provisions comprised in laws for sectors such as banking and finance, consumer protection, postal services, healthcare, credit reporting, telecommunications and internet, etc.

B. Initial Preference for the Minimalist Approach

China's first preference for having several sectorial laws for the regulation of data privacy bears resemblance with the U.S. approach (II.B.1) although Chinese specificities can be observed through the special role of non-binding guidelines (II.B.2).

1. Various Legal Instruments

China nearly chose to follow the EU path on legal instruments when a personal data protection law was considered from 2005 to 2008. This draft was based on data protection principles mostly similar to the OECD Privacy Guidelines and would have brought the country closer to global standards.[93] The broad scope of the law would have been a first sign of convergence with the comprehensive law model promoted by Europe. While its content was closer to the OECD Privacy Guidelines and U.S. privacy laws, the instrument resembled the comprehensive law used in the EU, its content was not as protective.[94] Interestingly, and unlike present rules in China, it explicitly included government authorities in its scope of application, although with less obligations than for the private sector.[95] This law would have been a significant step from China in the direction of the Western practice of personal data privacy, but the project stalled, and the text remained a draft. It still is an influential reference years after its completion, used today when considering the possibility of a law

[93] Xue, *supra* note 2, at 287. *See also* Graham Greenleaf, *China's Proposed Personal Information Protection Act,* 91–2 PRIV. L. & BUS. INT'L NEWSL. 1 (2008).

[94] Greenleaf, *supra* note 93, at 12.

[95] *Id.* at 5–7.

dedicated to data privacy in China.[96] It does shed light on a direction that was possible although not taken then, when today the possibility of a comprehensive data protection law in China is coming back in the legal debate.[97]

Instead of going this route, China started to build a sector-specific data privacy protection framework following the line of the 2012 NPC Decision. As in the U.S. approach, data privacy requirements are included in several sectorial laws mainly concerning consumers privacy. In 2013, the NPC's Standing Committee updated the Consumer Protection Law,[98] making data protection a distinct right for consumers in its Article 14,[99] and notably including the core data protection principles from the 2012 NPC Decision, especially on security and confidentiality, purpose specification and consent.[100]

---

[96] *See infra* section II.C. Greenleaf noted in 2008 that whether or not this draft were to become law (which it did not), it "will remain significant as indicating some of the earliest and most detailed expert thinking on the subject of privacy in China," *Id.* at 2.

[97] *See infra* section II.C.

[98] Decision on Amending the PRC Law on the Protection of Consumer Rights and Interests, adopted by the Standing Committee of the Twelfth National People's Congress on October 25, 2013, and took effect on March 15, 2014. Consumer Protection Law (Including 2013 Amendments), retrieved from https://www.chinalawtranslate.com/consumer-protection-law-including-2013-amendments/?lang=en (last visited Aug 24, 2019).

[99] Consumer Protection Law art. 14: "When purchasing or using goods or receiving services, consumers enjoy the right to personal dignity, the right to have their ethnic customs respected, and enjoy the right to have their personal information protected."

[100] Consumer Protection Law art. 29: "Proprietors collecting and using consumers' personal information shall abide by principles of legality, propriety and necessity, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consumers' consent. Proprietors collecting or using consumers' personal information shall disclose their rules for their collection or use of this information, and must not collect or use information in violation of laws, regulations or agreements between the parties.

Proprietors and their employees must keep consumers' personal information they collect strictly confidential and must not disclose, sell, or illegally provide it to others. Proprietors shall employ technical measures and other necessary measures to ensure information security, and to prevent consumers' personal information from being disclosed or lost. In situations where information has been or might be disclosed or lost, proprietors shall immediately adopt remedial measures.

However, they remain vague and general, and the rights of access, modification and deletion are missing. In 2013 the Ministry of Industry and Information Technology ("MIIT") adopted the Telecommunications and Internet Personal User Data Protection Regulation ("2013 MIIT Regulation").[101] The Regulation adds new requirements on top of earlier rules from 2011,[102] which apply to the collection and use of personal user data in the process of providing telecommunications services and Internet information services within China and includes requirements of minimum data collection, notice and data breach notifications, meeting several of the OECD Privacy Guidelines principles. The 2013 MIIT Regulation applies to both ISPs and telecommunications business operators and is intended as an implementing measure for the 2012 NPC Decision. The broad definition of personal data,[103] comprising *identifiable* information, has its roots in EU law. A number of sector specific laws followed the 2012 NPC Decision.[104]

Proprietors must not send commercial information to consumers without their consent or upon their request of consumers, or where they have clearly refused it."

[101] The 2013 MIIT Regulation was passed on June 28, 2013 at the 2nd ministerial meeting of the Ministry of Industry and Information Technology of the People's Republic of China and took effect on September 1, 2013. Retrieved from https://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/ (last visited Aug 24, 2019).

[102] The text "Several Regulations on Standardizing Market Order for Internet Information Services" has been issued on December 7, 2011 and came into effect on March 15, 2012.

[103] 2013 MIIT Regulation art. 4: "Personal user data as named in these regulations, refers to users' names, dates of birth, identity card number, address, telephone number, account number, password and other information with which the identity of the user can be distinguished independently or in combination with other information, as well as the time, and place of the user using the service and other information, collected by telecommunications business operators and Internet information service providers in the process of providing services."

[104] *Inter alia*, the Administrative Regulations on the Credit Reporting Industry of 2013; amendments to the Prevention and Treatment of Infectious Diseases Law in 2013; Administrative Provisions on the Medical Records of Medical Institutions of 2014; or the Security Measures on the Protection of Users' Personal Information for Mailing and Courier Services of 2014. *See* Vincent Zhang & John Bolin, *China Data Protection & Privacy*, GETTING THE DEAL THROUGH (Aug. 2019) ,

The most important milestone in China's data protection legal landscape is the Cybersecurity Law ("CSL"), enacted on November 7, 2016 by the Standing Committee of the National People's Congress and which came into force on June 1, 2017. Requirements about data privacy are comprised among dispositions related to the other aspects of cybersecurity. The CSL has a broader scope than previous laws and brings the country even closer to global standards. As detailed below, personal data are defined similarly as in the GDPR, and the data protection principles have been improved compared to previous binding laws. The CSL covers several of them, although they are not as distinctly listed as they are in the guidelines accompanying the CSL.[105] They are mostly in the first paragraph of article 41, requiring that "network operators collecting and using personal information shall abide by the principles of legality, propriety and necessity; make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is collected."[106] The second paragraph of this article relates to what network operators shouldn't do, such as collecting personal information unrelated to the services they provide, violating the laws or agreements with the data subject, in their data collection and/or data processing activities: "Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations and agreements with users to process personal information they have stored."[107] The CSL and its accompanying guidance text are discussed in more details in Part III.

As these principles show, the requirements of the CSL remain so general that either a very strict or a very lenient interpretation would not breach the letter of the law—this delta being a source of legal

---

https://gettingthedealthrough.com/area/52/jurisdiction/27/data-protection-privacy-china/.

105 *See infra* section II.B.2.

106 CSL art. 41.

107 *Id.*

uncertainty for businesses. To alleviate this situation, China makes use of guidance texts.

2. The Role of Non-Binding Rules

Generality and vagueness are typical traits of Chinese law. The legal literature commonly acknowledges that China's legal system is characterized by laws broadly drafted and significantly flexible[108]—the CSL counts among this type of vague laws. The law contains many dispositions and definitions where the lack of precision gives rise to questions placing entities in a state of legal uncertainty.[109] This provides the government with room for maneuver and flexibility in interpreting and enforcing the law, and can be construed as necessary to prevent the law from being rapidly outdated by evolution of usage and technological developments. The government may however use this vagueness to drive the implementation of the CSL in the way it sees fit according to the interests of the moment, even on a case-by-case basis that could lead to different implementation depending on the target.[110]

To palliate the shortcomings of having vague binding laws, China uses non-binding texts to provide details and to guide the laws' implementation. They set best practice standards that companies are encouraged to implement themselves voluntarily—*in theory*. To comprehend the breadth of this Chinese characteristic, the particular legal value of these texts should be outlined. This legal value is ruled by the Standardization Law from 2017,[111] which sets two kinds of

---

[108] *See generally* Deborah Cao, *Chinese Law and Imprecise Language*, *in* CHINESE LAW: A LANGUAGE PERSPECTIVE (2017).

[109] Adeline Poisson, *Extraterritorialité et protection des données personnelles : aperçu comparatif en droit européen et droit chinois*, INSTITUT DE DROIT COMPARE DE PARIS (2018), http://idc.u-paris2.fr/extraterritorialit%C3%A9-et-protection-des-donn%C3%A9es-personnelles-aper%C3%A7u-comparatif-en-droit-europ%C3%A9en-et. She notes that the CSL remains evasive in several ways, despite being the result of three previous draft versions.

[110] Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 98 (2018).

[111] Standing Committee of the National People's Congress, Standardization Law of the People's Republic of China, issued on November 4, 2017 and came into effect on January 1, 2018 (Standardization Law). It revises the 1989 Standardization Law.

standards: on the one hand, compulsory standards (annotated *GB*)[112] that shall be implemented to produce, import and/or sell products in China; and on the other hand, recommended standards (annotated *GB/T*) that can be adopted voluntarily.[113] Both types of standards are drafted by a standardization technical committee or a group of experts, and draft versions are released to seek opinions. Compulsory requirements are those providing requirements for "safeguarding human health and the safety of the person, state security, ecological environment security, and meeting fundamental needs of social and economic administration."[114] Specifications on personal data protection fall out of this category and their implementation is therefore only recommended in principle. However, they are to be taken as "quasi-implementing rules,"[115] a "reference point" for regulators[116] which reflect their thinking on data privacy.[117] These non-binding rules show China's direction on data protection and how authorities are likely to interpret the laws, which makes them more important than voluntarily frameworks in a Western context.[118]

---

112 GB stands for "GuoBiao" (国标), meaning "national standard".

113 Standardization Law art. 21.

114 Standardization Law art. 9.

115 Barbara Li, Anna Gamvros & Tom Wong, *China data privacy: New guidance to strengthen protection of personal data*, DATA PROTECTION REPORT (Mar. 7, 2017), https://www.dataprotectionreport.com/2017/03/china-data-privacy-new-guidance-to-strengthen-protection-of-personal-data/.

116 Luo Yan, *China's New Draft National Standards on Personal Information Protection*, COVINGTON (Jan. 6, 2017), https://www.insideprivacy.com/international/china/chinas-new-draft-national-standards-on-personal-information-protection/.

117 Luo Yan, China Releases Draft Amendments to the Personal Information Protection Standard, COVINGTON (Feb. 11, 2019), https://www.cov.com/-/media/files/corporate/publications/2019/02/china_releases_draft_amendments_to_the_personal_information_protection_standard.pdf.

118 Samm Sacks, *New China Data Privacy Standard Looks More Far-Reaching than GDPR*, CTR. FOR STRATEGIC & INT'L STUD. (Jan. 29, 2018), https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.

In the field of personal data protection, the most important of these rules are the 2018 Specification,[119] and before it the 2013 MIIT Guideline.[120] The 2013 MIIT Guideline has a broader scope than binding laws at the time, covering more businesses than the binding MIIT Regulations from 2011 and 2013. More issues are addressed, such as data exports and data subjects' access and correction rights. Eight basic principles are set out, similar to those found in the OECD Privacy Guidelines, such as purpose specification, a soft data minimization requirement (not on par with its EU equivalent), transparency, data quality, lawfulness (although the only legal basis allowed is consent, and therefore implicit consent), accountability and security.[121] The text also shows certain signs of convergence with the EU model, as, for the first time in China, the sensitivity principle appears: the difference is made between sensitive information and other personal information, requiring additional safeguards to protect the former. The improvement on the compliance with international practice led to identify the document as being a possible basis for a future comprehensive data protection law.[122] Although this did not yet

---

[119] The "Information Security Technology – Personal Information Security Specification - (GB/T 35273-2017)" has been issued by the National Information Technology Standardization Technical Committee (the TC260) on December 29, 2017 and took effect on May 1, 2018. The TC260 is jointly supervised by the Standardization Administration of China and the Cyberspace Administration of China for the purpose of setting standards. *Translation: China's Personal Information Security Specification*, NEW AMERICA (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/.

[120] The "Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems - (GB/Z 28828-2012)" has been issued by the TC260 on November 5, 2012 and effective on February 1, 2013. Under the previous Standardization Law, *GB/Z* indicated a voluntary standard as well. *Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems*, CHINA COPYRIGHT AND MEDIA (Aug. 9, 2013), https://chinacopyrightandmedia.wordpress.com/2013/01/21/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/ (last visited Aug 8, 2019).

[121] 2013 MIIT Guideline art. 4.2.

[122] CHINESE LEGAL REFORM AND THE GLOBAL LEGAL ORDER: ADOPTION AND ADAPTATION 168 (Yun Zhao & Michael Ng eds., 2017),

happen, the 2018 Specification draws upon the 2013 MIIT Guideline and improves it.

As above-mentioned, whereas the CSL centralizes dispositions on personal information protections, it contains only a few articles with vague wording that need clarification. Among the several guidelines accompanying the law, the 2018 Specification is the one focusing on personal data privacy.[123] Because of the scarcity of dispositions in the law, creating a comprehensive guidance was a challenge for the drafters; to palliate this lack, they acknowledged that they looked to foreign rules and transplanted rules that benefited from the more mature experience of foreign countries.[124] It provides core data protection principles, which are defined and outlined in a much clearer manner than in the CSL, in particular the principles of purpose specification, transparency, lawfulness (although with consent as the only legal basis, as in the 2013 MIIT Guideline), participation, security, sensitivity and a requirement of data minimization that now matches the EU strictness (only the data *necessary for* the purpose should be processed and not those *related to* it, as was the case in the 2013 MIIT Guideline).[125] Some of these principles show strong signs of

---

https://www.cambridge.org/core/books/chinese-legal-reform-and-the-global-legal-order/9B2888850C95C7F79726BEEA2CDCF06E.

[123] Another guideline for the protection of personal information, currently at the drafting stage, is the "Personal Information Outbound Transfer Security Assessment Measures". Cindy L, Qiheng Chen, Mingli Shi, and Kevin Neville, *Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China*, NEW AMERICA (June 13, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/ (last visited Aug 8, 2019).

[124] Wei Zhao, *About the Companies' Personal Information Protection Compliance Rules Based on the Personal Information Security Specification* (Feb. 1, 2018), https://mp.weixin.qq.com/s?__biz=MzIxODM0NDU4MQ==&mid=2247484784&idx=1&sn=6c56a88d51f5197ee712e8e22af72027&chksm=97eab89aa09d318c7258c3d7873ffde97fd1c1569d9769758c47f78430c5d7c46f9667dbd8e1&scene=21#wechat_redirect. The author, a senior expert in data privacy compliance at Tencent and one of the drafters of the 2018 Specification, states that "there are only a few articles on personal information in the Cyber Security Law, which makes difficult to cover all important areas of personal information protection; this posed challenges for the preparation of the [2018 Specification]."

[125] 2018 Specification art. 4.

convergence with the EU standards.[126] Despite its non-binding nature, the 2018 Specification represents the level of protection that data controllers in China should be aiming for. As the Standardization Law requires, the final version of the Specification follows a draft that was issued in order to collect public opinions, and which did bear some differences.[127] Propositions for amendments to the current version are now being discussed on topics such as consent requirements or data breach notification.

These guidelines are useful in providing details missing in laws. For example, both the 2012 NPC Decision and the CSL mandate a privacy notice requirement, without stating what terms ought to be included. Useful precisions and details are however present in both the 2013 MIIT Guideline and the 2018 Specification. Other examples of the kind exist in the level of details for security and data subject's participation. Most importantly, and as will be detailed in the next Part, those specifications recommend significantly strong protection for personal information.

A parallel can be drawn here with the use of guidelines in the EU system, most notably those from the European Data Protection Board ("EDPB"),[128] composed of representatives from all supervisory authorities in the EU. These guidelines seek to explain and illustrate a particular point of the data protection rules in a very detailed manner. Their format is however different. Whereas a guideline in the EU is an actual explanatory text, sometimes close to an instruction manual, Chinese guidance texts are organized by articles in the manner of binding laws, reinforcing their quasi-implementing character.

C. Towards a Comprehensive Data Privacy Law

Despite the initial choice to disseminate data protection provisions in many laws, the studying of the evolution of the rules'

---

126 *See infra* section III.B.

127 For example, the draft version of the 2018 Specification was only applicable to entities above certain thresholds, *see infra* note 132.

128 The GDPR created the EDPB to replace the WP29, a group with similar functions born with the Directive 95/46/EC and that issued most of the current guidelines, now endorsed by the EDPB.

scope and of China's legislative agenda demonstrates that the country is getting closer to having a national data protection law, and therefore converging with the EU model on legal instruments, rather than continuing in the U.S. way.

The CSL has a broad scope that is a significant sign of China's intentions to group rules on personal data protection previously disseminated among dozens of laws, sometimes contradicting each other.[129] The CSL applies to virtually any company: the dispositions related to data protection are applicable to "network owners, managers and network service providers"[130] who collect and use information.[131] The focus on network is expected, as those dispositions exist in the context of a *cybersecurity* law and not purely a *personal data protection* law like in the EU or even a *consumer privacy* law as often found in the U.S. The term "network" encompasses the "systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing."[132] This is in fact the basic definition of a computer network, which in theory can make nearly every company a network owner. Even if the definition is narrowly interpreted, the CSL targets more organizations, and is less sectorial in nature, than previous laws containing privacy requirements. It is not, however, sufficient to classify it as a comprehensive law as promoted by the EU, which should apply to all organizations collecting and processing personal data.

The 2018 Specification goes further and makes clear that it applies to "all types of organizations' activities handling personal information."[133] This broad scope is similar to the GDPR. It is an improvement upon the Draft 2018 Specification, which did not apply to organizations employing fewer than ten people or earning less than RMB 1,000,000, that do not process more than 10,000 people's

---

129 Zhao, *supra* note 125. It should be recalled, however, that the CSL does not supersede previous laws.

130 CSL art. 76.3.

131 CSL arts. 40–1.

132 CSL art. 76.1.

133 2018 Specification art. 1.

personal information in any continuous twelve-month period.[134] The 2018 Specification also provides a broad definition for data controllers ("an organization or individual that has the authority to determine the purposes and/or methods of the processing of personal information")[135] and for data subjects ("a natural person identified by personal information").[136] In the first draft of the Cybersecurity Law, the person identified or identifiable could only be a Chinese citizen; this was in line with the U.S. approach, where laws protect U.S. residents or a given state's residents for state laws.[137] The final version then broadened the definition to "natural person,"[138] in line with the EU.

As for the definition of "personal information," the OECD and the EU agree in including all information related to a natural person identified or identifiable. As explained above, most U.S. legal instruments feature a narrow definition of personal information, comprising information that *directly* identifies a person.[139] The CSL departs from the U.S. approach and prefers a broad definition of personal information, defining them as "all kinds of information recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth."[140]

The 2018 Specification contains the same definition and includes an indicative list of examples.[141] These definitions give the 2018 Specification a global scope, similar to comprehensive data protection laws in general and to the GDPR in particular. Regarding binding law, the scope of the CSL is narrower because it refers to network operators, although it has the potential to be broadly

134 Draft 2018 Specification art. 1.
135 2018 Specification art. 3.4.
136 2018 Specification art. 3.3.
137 *See supra* § I.A.
138 CSL art. 76(5).
139 *See supra* § I.A.
140 CSL art. 76(5).
141 2018 Specification art. 3.1.

interpreted especially under the lights of the specification's guidance. This shows that China is moving away from the sector-specific approach to data protection that is favored by the U.S., and instead goes towards the EU model.

As for the territorial jurisdiction, the GDPR has an extraterritorial scope, because it may apply to organizations established outside the Union when they offer goods or services to data subjects in the Union or monitor their behavior when it takes place in the EU.[142] Extraterritorial competence also exist in the U.S., for example, in California.[143] In China however, the CSL is only applicable to operations happening within the country.[144]

As a consequence of this trend, chances are high that China will soon enact a dedicated personal data protection law. The NPC Standing Committee's Five-year Legislative Plan for the period 2018-2023 features a "Personal Information Protection Law" that is now in the "mature" drafting stage.[145] The drafting of this law was commented on in 2019 by Zhang Yesui, spokesman for the second session of the 13th National People's Congress, when he outlined that provisions on personal information were too scattered and so there is a need "to have a law specifically on the protection of personal information to form a unified force of regulation."[146] Although a previous draft for a privacy

---

142 GDPR art. 3(2).

143 Although it is not expressly stated and in the absence of cases to date, the CCPA probably has an extraterritorial scope. The CCPA indeed applies to an entity that "does business in the State of California" (CCPA, para. 1798.140(c)(1)), and the comparison with other California rules with a "doing business" requirement shows that extraterritorial applicability of the CCPA is likely, *see* Alice Marini et al., *CCPA, face to face with the GDPR: An in depth comparative analysis* DataGuidance & Future of Privacy Forum 8–9 (2018), https://fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/.

144 CSL art. 2: "This law applies to the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the mainland territory of the People's Republic of China."

145 A translation of the 13th NPC Standing Committee Legislative Plan is available at https://zh.wikisource.org/wiki/User:NPCObserver/13thNPCSCLegislativePlan (last visited Aug 24, 2019)

146 Xinying Zhao, *Legislation coming to better protect personal details, spokesman says*, CHINA DAILY (March 4, 2019),

act has been kept away since the 2000s,[147] supporters of such law are optimistic that it will be enacted before 2023.[148] According to the drafters of the 2018 Specification, the latest rules on personal data protection, there is a "high possibility that the future personal information law will be compatible with [the 2018 Specification]."[149] As the next Part demonstrates, this 2018 Specification is highly converging with EU rules. The law should therefore be more precise and further strengthen the requirements found in the CSL, bringing China one step closer to the EU model and to the large number of countries that adopted such law. It is likely that this convergence will continue and increase, which would leave the U.S. the last of the group not to have a dedicated and comprehensive law on data privacy. Apart from this convergence on legal instruments, a similar trend is observable for the content and meaning of the rules.

IV. CHINA'S NEW DIRECTION: MORE PROTECTIVE THAN THE U.S., NOT AS STRICT AS THE EU?

Dr. Hong, who led the drafters of the 2018 Specification, argues that these rules are "stricter than the U.S., but not as much as the EU."[150] Given China's late awakening to the issue and the debates surrounding surveillance, such declaration may seem bold and conveys the need for a deeper analysis. The study of data protection principles and requirements contained in the newest Chinese rules show that they maintain similarities with the U.S. approach on several elements (III.A), but the CSL, and mostly the 2018 Specification, also features important signs of convergence with EU law (III.B). This indeed demonstrates a significant change in China's direction, in favor of stronger data protection requirements than the U.S. but without going as far as the EU, but with Chinese characteristics that Part IV details.

---

https://www.chinadaily.com.cn/a/201903/04/WS5c7cbaa4a3106c65c34ec9ae.html.

147 *See supra* § II.A

148 Yuehong Wang, *Why do we still talk about optimism after waiting 12 years for a personal data protection law?*, SCI. & TECH. DAILY (Mar. 4, 2017), http://i.cztv.com/view/12442896.html.

149 Zhao, *supra* note 124.

150 Hong, *supra* note 6.

A. Where China Remains Closer to the U.S. Than to the EU

The legal elements illustrating the most that China conserves some resemblance with U.S. laws are the requirements on a legal basis for data collection and processing (III.A.1), as well as rules on data breaches and supervisory authorities (III.A.2).

1. Requirements for Data Collection and Processing

The principle of lawfulness of data processing is one of the most significant differences between EU and Chinese data protection principles, and a point where China is relatively in line with the U.S. The lawfulness requirement means that collection and processing should rely on a defined legal basis to be performed.[151] The legal bases often found in data protection laws are: consent from the data subject; performance of a contract to which the data subject is a party; the processing is necessary for his vital interests; necessary for the compliance with a legal obligation that the data controller should abide by; for a task carried out in the public interest; or the processing is necessary for the legitimate interests of the data controller unless the rights and freedoms of the data subject override them.[152] The GDPR provides all of the legal bases in its Article 6, with a strict conception of consent: it must be freely given, informed and unambiguous, which excludes *implicit* consent. On the opposite side of the spectrum, the U.S. approach strongly relies on individuals' consent to data processing[153] or even allows by default the collection and processing of personal data (without the need to rely on consent at all or any other

[151] Roos, *supra* note 50, at 108.

[152] Roos finds these legal bases, either all of them or just some, in the Directive 95/46/EC, UK's DP Act of 1998 and Netherland's WBP (which are laws implementing the Directive), the OECD Guidelines and the Fair Credit Reporting Act of 1970 in the USA. *See id.* at 109.

[153] Schwartz, *supra* note 24, at 1976.

legal basis), unless forbidden by another law.[154] Even the CCPA only lightly requires consent and does not list other legal bases.[155]

In China, much like in the U.S., the CSL establishes consent as the only legal basis for data collection and processing and has a loose conception of it, allowing for *implicit* consent. While the CSL and the 2018 Specification do not use the term *implied*,[156] drafters of the specification later clarified that explicit consent is required only if the term *explicit consent* is expressly mentioned (*e.g.* for collecting sensitive information[157]), not where just *consent* is used.[158]

A particularity of the CSL is that it does require consent at all times and does not allow collection or processing by default. But it does so without giving data controllers the possibility of using another legal basis when asking for consent is not practical. In the EU, this is done on the basis of the "legitimate interest" of the controller.[159] To palliate this deficiency in China, entities will have to extensively use implicit consent for those purposes, which undermines its value. Drafters of the 2018 Specification attempted to remedy this problem,

---

154 As Schwartz observes, "the United States does not rely on a notion that personal information cannot be processed in the absence of a legal authorization. Rather, it permits information collection and processing unless a law specifically forbids the activity." *Id.* at 1976.

155 Marini et al., *supra* note 143, at 23.

156 The 2013 MIIT Guideline distinguishes between implied and express consent, but does not provide the necessary conditions and details to assess whether a consent is implicit or explicit. Because other legislations fail to clarify this issue, Zhou considers that "in practice there is thus still considerable ambiguity as to the requirements and conditions of consent" *see* Zhou, *supra* note 81, at 55.

157 2018 Specification art. 5.5.

158 As Sacks notes: "According to Dr. Hong, the definition of consent is 'looser than the EU and more in line with the United States' because it allows for 'implied or silent' consent in certain instances. He acknowledges that the written standard does not specifically use the term 'implied' consent, which may have led to some misunderstanding. But the language of the [2018 Specification] supports his point. The [2018 Specification] defines explicit consent as meaning a written statement or affirmative action. But the term is only used in certain instances", Samm Sacks, *China's Emerging Data Privacy System and GDPR*, CENT. FOR STRATEGIC AND INT'L STUD. (Mar. 9, 2018), https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

159 GDPR art. 6(1)(f).

but because they are not legislators they couldn't go against the letter of the law; hence the inclusion of more legal bases was impossible, as they later explained.[160] Nevertheless, the drafters included a series of exemptions to obtaining consent that partially cover GDPR's legal bases, but without explicitly mentioning "legitimate interests." Data controllers do not need to obtain consent to collect and process data where there is a direct relation to national security or defense,[161] public health,[162] criminal investigations or enforcement of judgments,[163] where it's done to protect the life or major lawful rights of the data subject,[164] or where the data has been lawfully and publicly disclosed previously.[165] In addition, the final version of the 2018 Specification contains exemptions that were not present in earlier versions, such as where the processing is required for performing a contract,[166] or "where used to preserve the secure and stable operations of products or services they provide, such as discovering or handling problems with the product or service."[167] The exemptions in Chinese law only partially resemble the legitimate interest basis in the GDPR[168] because Article 6.1(f) of the GDPR is broader and can, for example, under certain conditions, justify data processing for direct marketing purposes.[169]

Another core element where China does not put as much emphasis as the EU does is data quality. The data quality principle mandates that personal data should be *relevant* to the purposes for which they are to be used and, to the extent necessary for those purposes, should be *accurate* and kept *up-to-date*.[170] All major sources of

---

160 Hong, *supra* note 6.

161 2018 Specification art. 5.4.a.

162 2018 Specification art. 5.4.b.

163 2018 Specification art. 5.4.c.

164 2018 Specification art. 5.4.d.

165 2018 Specification arts. 5.4.e, 5.4.f.

166 2018 Specification art. 5.4.g. This exemption is analogous to the "performance of a contract" basis in GDPR, art. 6(1)(b).

167 2018 Specification art. 5.4.h.

168 Sacks, *supra* note 158.

169 GDPR, Recital 47.

170 Roos, *supra* note 50, at 114–16. See also GDPR art. 5.1(d), stating that personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having

data protection rules provide similar definition of personal data quality.[171] In the U.S., the requirement of data quality is part of certain federal laws such as the Privacy Act, but not in state laws seen as more protective, for example, the CCPA or Colorado's new consumer privacy rules.[172] In China, the data quality principle is not clearly stated in the CSL. Article 42 prohibits tampering with or destroying the data collected but does not require to ensure that the data is accurate, relevant or up-to-date. Although the rights of correction and deletion can be "post-facto substitutes for data quality requirements"[173]—because this provides a way for the data subject to ensure data relevancy and accuracy—it requires the subject's precise knowledge and intervention, which in practice lowers the effective level of protection through the requirement of data quality. In fact, the data quality principle in the CSL remains embryonic at best. The requirement exists in the 2013 MIIT Guideline and was clearly expressed in the last Draft 2018 Specification,[174] as a requirement for the data controller to ensure personal data's accuracy, veracity, validity, and usability.[175] Surprisingly, there is no mention of the principle in the final version of the 2018 Specification. Hence, China is still closer to the U.S. approach, where data quality is not systematically a requirement.

2. Enforcement and Consequences in Case of Data Breaches

In the U.S., requirements for data breach notification exist but are not as strict as in the EU. Moreover, there is no supervisory authority dedicated to the protection of personal information, whereas such authority is a fundamental part of the EU system. China is similar to the U.S. on both of these points, although the data security requirement is defined similarly in all three approaches.

---

regard to the purposes for which they are processed, are erased or rectified without delay".

171 Privacy Act of 1974, 5 U.S.C § 552a(e)(5); GDPR art. 5.1(d); OECD Privacy Guidelines, para. 8; Convention 108 art. 5.c and d.

172 Colorado Consumer Data Privacy Law, *supra* note 45.

173 Graham Greenleaf & Scott Livingston, *China's New Cybersecurity Law – Also a Data Privacy Law?* 144 UNSWLRS 1, 5 (2016).

174 2018 Specification art. 4.e.

175 Draft 2018 Specification art. 4.e.

Data security is a core data protection principle that is enshrined in data protection laws, because security and confidentiality are necessary for personal data privacy to be effective. This principle is present in almost all the early data protection instruments.[176] According to the OECD, "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data;"[177] U.S. and EU laws are similar, featuring an appropriateness criterion as well. Because its main focus is on cybersecurity, the CSL has many requirements regarding this broader topic, such as infrastructure security and monitoring. On personal data especially, the law requires security but does not expressly mention the relative criterion. Article 40 states that "network operators shall strictly maintain the confidentiality of user information they collect, establish and complete user information protection systems" and Article 42 adds they "shall adopt technological measures and other necessary measures to ensure the security of personal information they gather, and prevent personal information from leaking, being destroyed or lost." The criterion is explicit in the 2018 Specification, as data controllers should "possess the appropriate security capacity taking into account the security risks faced, and employ sufficient management and technical measures to protect the confidentiality, integrity, and availability of personal information."[178] Therefore, EU, U.S. and China definitions on this requirement are similar. However, it's when a security breach occurs that the consequences differ between the three approaches.

A security problem can be the cause of a data breach. Once it occurs, the notification requirement obliges the entity in charge of the data to notify the supervisory authority and/or the affected individuals.[179] Following the revision in 2013, the OECD Privacy

---

176 Roos, *supra* note 50, at 125. Privacy Act of 1974, 5 U.S.C § 552a(e)(10); GDPR art. 32; OECD Privacy Guidelines, para. 11; Convention 108 art. 7; CCPA, 1798.150.(a)(1).

177 OECD Privacy Guidelines ¶ 11.

178 2018 Specification art. 4.f.

179 The definition of a data breach can differ depending on the rules considered. It may be limited to a leak or include problems related to the availability or integrity of data.

Guidelines encourage countries to adopt data breach notification laws. The Guidelines do not have any requirements on the timing of the notification, because the OECD estimates that more experience is required before doing so.[180] The obligation to notify about the personal data breaches has existed in the U.S. since 2002.[181] The timeframe for notification is large for example thirty days[182] or even up to a reasonable time.[183] A data breach notification requirement was absent from the EU Directive in 1995 (although included in some Member States national laws). Drawing on rules from Member States and the European Union Telecommunications Framework, the EU now goes further than both the OECD and the U.S. and compels data controllers to notify supervisory authorities of a security breach within seventy-two hours after the data controller became aware of it.[184] They should notify data subjects as well if there is a high risk to their rights and freedoms.[185]

In China, previous rules mandated that data controllers notify authorities but not individuals.[186] The CSL now requires data controllers to inform authorities as well as individuals in case of a data breach: "When the leak, destruction or loss of personal information occur, or might occur, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make report to the competent departments in accordance with regulations."[187] The 2018 Specification gives more details and requires companies to draft a personal information security incident response plan and organize drills annually.[188] In case of a breach, affected entities should record a

---

180 OECD Privacy Guidelines, Explanatory Memorandum, 27.

181 California S.B. 1386, effective on July 1, 2003 (California Data Security Breach Notification Law).

182 For example, in Colorado, where notification to the affected Colorado residents must be made within thirty days after the determination that a breach occurred, *see* Colorado Consumer Data Privacy Law § (2).

183 California Data Security Breach Notification Law, 1798.29.(a) and 1798.82.(a): "The disclosure shall be made in the most expedient time possible and without unreasonable delay."

184 GDPR art. 33(1).

185 GDPR art. 34.

186 Greenleaf and Livingston, *supra* note 173, at 5.

187 Cybersecurity Law art. 42.

188 2018 Specification arts. 9.1(a), (b).

set of information about the incident, assess its impact, and report it in a timely manner.[189] It further requires affected entities to promptly inform data subjects and provides a non-exhaustive list of information to be included in the notice.[190]

But the 2018 Specification does not precisely quantify the timeframe for notification. By requiring prompt notification, the Chinese legislator may want to gain more experience before setting a clear timeframe, as does the OECD. Therefore, the new provisions of Chinese laws for data breach notification are an improvement towards global standards, without being as strict as EU rules. It does resemble more the U.S. approach, where notification within a reasonable time is a common requirement.

The authority to which the notification should be made is not apprehended in the same way in the EU and the U.S. The first version of the OECD Privacy Guidelines didn't explicitly mention data protection authorities, and the requirement of having an independent and dedicated authority is a European standard.[191] The version following the 2013 revision now asks OECD Member countries to establish privacy enforcement authorities, free from instructions, bias or conflicts of interest,[192] with the "governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis."[193] Europe considers it a crucial part in recognising that a third country guarantees a level of data protection essentially equivalent to its own.[194]

---

189 2018 Specification art. 9.1(c)3.

190 2018 Specification art. 9.2.

191 Greenleaf, *supra* note 3, at 73.

192 OECD, Explanatory Memorandum, 28.

193 OECD Privacy Guidelines ¶ 19(c).

194 This is done through the adequacy decision granted by the European Commission, which allows data transfers from the EU to the third country without additional safeguards. To do so, the European Commission must take account of "the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States," GDPR art. 45(2)b.

The independency of these supervisory authorities is a requirement for the authority itself but also for its members.[195] As opposed to the EU, the U.S. does not provide for a regulatory oversight by an independent data protection authority,[196] but rather a combination of "the US Federal Trade Commission, state attorneys general, the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services, the Department of Education, the judicial system, and [. . .] the US plaintiffs' bar."[197] The Federal Trade Commission ("FTC") has grown to become the most important privacy enforcement agency in the US.[198]

China's CSL does not establish a data protection authority in the European sense. The Cyberspace Administration of China ("CAC") has a general responsibility for planning and coordination cybersecurity efforts, a central role given by Article 8 of the CSL, but there are several regulators responsible for data protection enforcement efforts. The same article states that the Ministry of Public Security and the MIIT are responsible for network security protection, supervision and management efforts within the scope of their responsibilities, along with "other relevant organs" and "within the scope of their responsibilities." Therefore, different authorities are in charge of data protection for their own sectors, in accordance with the sectorial approach that is still effective in China today. Those are, *inter alia*, the MIIT for telecommunications and information technology, the China Insurance Regulatory Commission for the insurance industry, or the China Banking Regulatory Commission for the banking industry. Much like in the U.S., there are several authorities in

---

195 GDPR art. 52.

196 Schwartz, *supra* note 24, at 1976.

197 UNITED STATES - THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW, *supra* note 24, at 269.

198 Boyne, *supra* note 22, at 301; UNITED STATES - THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW, *supra* note 24, at 284. Raul, Faircloth, and Mohan quote FTC Commissioner Julie Brill saying: "the FTC has become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its disposal to prosecute an impressive series of enforcement cases."

charge of enforcing privacy provisions on their own sector, and the allocation of competence is not always clear.[199] The CSL did not change the situation that still resembles the U.S. approach more than the EU's.

Several examples of enforcement have been reported since the CSL came in effect,[200] but the law does not allow authorities to issue highly deterrent fines like the GDPR does in the EU, based on the company's turnover. U.S. laws usually feature a different system, with a fine on a per violation basis, *i.e.* if the violation of the law concerns 100 people, the fine will be multiplied by 100.[201] Following the GDPR in the EU, and data privacy scandals in the US, sanctions for personal data breaches recently attained amounts that cannot be ignored by companies.[202] Under the CSL, companies in China face significantly lower risks, as fines can only be up to RMB 1,000,000 (USD 150,000) or ten times the amount of unlawful gains from the misuse of data. However, authorities may order the business to temporarily suspend its operations, shut down the website or even cancel business licenses and relevant operations permits,[203] which may have a deterrent effect.

B. Signs of China's Convergence with the EU Model

Despite some key differences, certain new Chinese rules on data privacy bring more protection to individuals than the OECD Privacy Guidelines, most U.S. laws, even those state state laws regarded

---

199 Bo Zhao & G.P. (Jeanne) Mifsud Bonnici, *Protecting EU citizens' personal data in China: a reality or a fantasy?*, 24 INT'L J. L. AND INFO. TECH. 128, 135 (2016).

200 Eliza Gritsi, *Dust has yet to settle two years after China's landmark cybersecurity law*, TECHNODE (June 10, 2019), https://technode.com/2019/06/10/dust-has-yet-to-settle-two-years-after-chinas-landmark-cybersecurity-law/; MARISSA (XIAO) DONG, CHINA - THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 133 (4 ed. 2018).

201 *E.g.* in California, under Section 1798.155(b) of the CCPA, the fine can be up to USD 7,500 per violation, which for 100 people impacted would bring the fine to USD 750,000.

202 In July 2019, the Information Commissioner's Office ("ICO"), the data protection authority in the UK, fined British Airways a record GBP 183,000,000 (USD 230,000,000), while in the U.S. the FTC settled with Facebook on a record USD 5,000,000,000 fine.

203 CSL art. 64.

as the most protective such as the CCPA. The following demonstrates that these stronger protections are often transplants of EU rules, showing the convergence of Chinese law with the EU model. As underlined below, most of those rapprochements come from the non-binding 2018 Specification, whereas the CSL is often too vague to soundly demonstrate convergence.

1. Transparency and Further Processing

Transparency makes it possible for individuals to understand that their personal data is collected and processed, to know who the data controller is, their means to establish the existence and nature of personal data, the main purpose of their use, and their rights.[204] The principle exists in the U.S., but EU rules are the example of thorough implementation of transparency,[205] where transparency has been strongly reinforced with the GDPR compared with the previous Directive.[206] In China, the 2012 NPC Decision requires "explicitly stating the purpose, manners and scope of information collection and usage" and is followed in it by the subsequent legislation.[207] The Cybersecurity Law briefly makes the requirement to "make public rules for collection and use."[208] Then, the 2018 Specification is more specific and mandates data controllers to "disclose the scope, purpose, and rules for processing personal information in a clear and comprehensible manner and accept external oversight."[209] The 2018 Specification again brings more clarity and precision than article 41 of the CSL.

After the entity informs the individual of the intended use of the information demanded at the time of collection, this purpose constitutes the frame within which the data can be used— further processing, such as selling the data to a third party, cannot go against

---

[204] Roos, *supra* note 50, at 116–17.

[205] *Id.* at 117–18.

[206] Transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent GDPR art. 6(1)(a).

[207] Zhou, *supra* note 81, at 56.

[208] CSL art. 41.

[209] 2018 Specification art. 4.e.

this specified purpose. This requirement is known as the purpose specification principle.[210] In China, the principle is established in article 41 of the CSL, stating that a network operator cannot violate "agreements between the parties to gather or use personal information."[211] Article 42 prohibits the conveyance to others of personal data by network operators without consent from the user, meaning that consent is necessary to process data for another purpose that the one initially specified.[212] The purpose specification principle is also expressly covered in the 2018 Specification, as the data controller should "have a legal, legitimate, necessary, and clear reason for processing personal information"[213] and "express the purpose, methods, scope, and rules for processing personal information to the data subject and solicit their authorization and consent."[214] If a data controller wants to use the personal information for a purpose different from the one specified at the time of data collection, it should seek explicit consent from the individual.[215] Here, China is in the wake of the European rules and diverges from the U.S., which does not afford the same level of protection and, for example, allows internet providers to sell users' data without their consent to this purpose.[216]

---

[210] OECD Privacy Guidelines ¶ 9; Convention 108 art. 5.b; GDPR art. 5(1)b; Privacy Act of 1974, 5 U.S.C § 552a(e)(3); CCPA, 1798.100. (b). *See* Roos, *supra* note 50, at 111.

[211] CSL art. 41.

[212] CSL art. 42.

[213] 2018 Specification art. 4(b).

[214] 2018 Specification art. 4(c).

[215] 2018 Specification art. 7.3(c).

[216] In October 2016, the Federal Communications Commission ("FCC") approved new rules for enhancing customers' privacy on the internet, forbidding internet providers from selling personal information such as browsing history, app usage or mobile location without the customers' explicit consent to this purpose. However, as other Obama administration's data protection initiatives, it has been repealed by the Republicans, in 2017. *See* Brian Fung, *The House just voted to wipe away the FCC's landmark Internet privacy protections*, THE WASH. POST (Mar. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/?noredirect=on&utm_term=.9c05bf05bd62. Another example can be found in the Privacy Act of 1974, which contains several exceptions to the rule prohibiting disclosure of personal data, such as "routine use" (5 U.S.C. § 552a(b)(3)).

2. Limitations on Data Processing Activities

The EU authorizes entities to only collect and process the amount of data *necessary* for the purpose specified to individuals, which constitutes the data minimization principle.[217] Data no longer necessary should be deleted.[218] The OECD Privacy Guidelines provide for softer rules, which only require that data should be *relevant to* the purposes for which they are to be used.[219] As often with the U.S. data privacy approach, the existence and meaning of the data minimization requirement varies. It exists in the Privacy Act[220] but none of its provisions explicitly limit data retention periods. The data minimization principle is absent from the FTC's list of fair information practice principles but exists in the list provided by the Department of Homeland Security.[221] It is not an express requirement in the CCPA. The U.S. approach therefore does not match the emphasis put on this principle by the EU,[222] especially since the adoption of GDPR.

The Chinese stance is dual. On the one hand, the CSL requires a soft minimization, as network operators are forbidden to collect personal information *unrelated to* the services they provide, which is more lenient than strict *necessity*.[223] However, the first paragraph of article 41 does require the network operator to abide by the principle of necessity. This could be used to interpret the term "unrelated to" in a strict way.[224] On the other hand, the 2018 Specification clearly sets a strict data minimization principle, with data processing permitted for

---

217 GDPR, Recital 39 art. 5.1(c).

218 GDPR art. 5.1(e).

219 OECD Privacy Guidelines ¶ 8.

220 Privacy Act of 1974, 5 U.S.C § 552a(e)(1), which requires that a government agency's records shall contain "only such information about an individual as is relevant and necessary to accomplish a purpose."

221 DHS, *Fair Information Practice Principles (FIPPs)*, DEP'T OF HOMELAND SEC'Y (2015), https://www.dhs.gov/publication/fair-information-practice-principles-fipps-0.

222 Schwartz, *supra* note 24, at 1976.

223 CSL art. 41, ¶ 2.

224 For an opinion of scholars skeptical that this interpretation could be given (*nota bene* this opinion was formulated before the issuance of the 2018 Specification), *see* Greenleaf and Livingston, *supra* note 174, at 4.

only what is *necessary to* the purposes,[225] which exists in the 2013 MIIT Guideline as well.[226] It further specifies that data should be deleted once the purpose specified is achieved.[227] Here, the CSL remains closer to the U.S. but the 2018 Specification is in line with the EU.

An even clearer distinction between the EU and the U.S. data privacy protections is the sensitivity principle, pursuant to which the processing of certain categories of data should be subject to additional safeguards.[228] The requirement exists in EU rules for data such as ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, criminal convictions, and the processing of genetic data, biometric data.[229] The U.S. does not have an overarching principle providing additional safeguards to sensitive data,[230] and in fact the opposition between the EU and the U.S. during the drafting of the OECD Privacy Guidelines resulted in the absence of this principle in the final text.[231]

China leans towards the EU approach, but in its specific way—one should recall that information on a person's political or trade union affiliations are contentious in China. On the one hand, the CSL ignores sensitive data and doesn't provide a definition or specific dispositions for them. Only certain sectorial laws contain restrictions regarding sensitive data.[232] On the other hand, non-binding rules do

---

225 2018 Specification art. 4(d): "Minimization Principle: Unless otherwise agreed by the data subject, only process the minimum types and quantity of personal information necessary for the purposes for which the authorized consent is obtained from the data subject. After the purposes have been achieved, the personal information should be deleted promptly according to the agreement."

226 2013 MIIT Guideline art. 9.

227 2018 Specification arts. 4(d), 6.1.

228 Roos, *supra* note 50, at 121.

229 GDPR arts. 9 and 10.

230 Schwartz, *supra* note 24, at 1976. However, the U.S. does have varying definitions in some laws and depending on the sector. It generally includes personal health data, credit reports, personal information collected online from children under 13, precise location data, and information that can be used for identity theft or fraud; *see* THAM, *supra* note 67, at 274.

231 Roos, *supra* note 50, at 121–22.

232 "Pursuant to Article 14 of the Administrative Regulations on the Credit-Reporting Industry, credit-reporting agencies are prohibited from gathering

make the distinction and require additional protection for sensitive data. However, the definition of sensitive data differs with EU rules where sensitive data are clearly listed. Both the 2013 MIIT Guideline[233] and the 2018 Specification[234] feature instead a risk-based definition for the identification of these data, that is much broader than in Europe. They are defined as those that, if disclosed or altered, could endanger the safety of persons or property, harm personal reputation and physical or psychological health, lead to discriminatory treatment, etc. The 2018 Specification then requires additional safeguards for handling sensitive data in subsequent articles.[235] This definition is followed by a non-exhaustive list of examples, such as identification numbers, bank card numbers,[236] health records, and bio-metrics data (the last two being personal sensitive information). Higher protection for sensitive data is common to China and Europe, but the risk-based approach is a Chinese characteristic.

3. Enhanced Rights for Individuals

Several direct rights that individuals enjoy under data protection laws belong to the participation principle, requiring that data subjects should be able to control and participate in the processing of their personal information by data controllers. The participation principle contains, in particular, the right for individuals to have access to their personal data, to request their correction, to control and to object to the processing, or to request the deletion of the data (also

---

information on an individual's religious beliefs, genes, fingerprints, blood type, disease and medical history (. . .)," Zhou, *supra* note 81, at 50–1.

233 2013 MIIT Guideline art. 3.8.

234 2018 Specification art. 3.2.

235 2018 Specification arts. 5.5, 6.3, 7.1.e, 7.3.b, 8.3.c, 8.4.c, 10.4.a, Appendix B and Table B.1 for the additional safeguards.

236 In the EU, non-binding rules issued by the EDPB (the "Guidelines on Data Protection Impact Assessment ("DPIA") and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, wp248rev.01") qualify financial information as "data with a highly personal nature" for which extra-care should be given because they "can be considered as increasing the possible risk to the rights and freedoms of individuals," but not as sensitive information, at 9.

known as the "right to be forgotten").[237] The OECD regards it as the most important privacy protection safeguard.[238] The most recent among them are the right to be forgotten and the right to data portability. The right to request the deletion of personal data exists in China, although it is a weaker version of its EU equivalent. In the EU, the right to erasure that was a component of the right of access in the Directive 95/46/EC[239] was strengthened in 2014 when the Court of Justice ("ECJ") recognized the existence of the individual right to be forgotten in the *Google Spain v. Costeja* decision.[240] The GDPR then made it a specific right.[241]

The creation of a right to be forgotten in the EU was received with scepticism in the U.S.[242] Critics like Eugene Volokh, a prominent scholar on American constitutional law, oppose the right to be forgotten on the basis of freedom of speech[243] that the First

---

237 Roos, *supra* note 50, at 119. Those rights can be found in OECD Privacy Guidelines –7; GDPR arts. 15-21.

238 OECD Privacy Guidelines, Explanatory Memorandum, 58: "The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language."

239 Directive 95/46/EC, art. 12.

240 Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014 EUR-Lex 62012CJ0131.

241 For a detailed look at the evolution of the right to erasure to the right to be forgotten, *see* Stefania Alessi, *Eternal Sunshine: The Right to Be Forgotten in the European Union After the 2016 General Data Protection Regulation*, 32 EMORY INT'L L. REV. 145 (2017). *See also, generally,* Gabriela Zanfir, *Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right*, *in* REFORMING EUROPEAN DATA PROTECTION LAW 227–49 (Serge Gutwirth, Ronald Leenes, & Paul de Hert eds., 2015).

242 Steven C. Bennett, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 164–68. Most negative reactions revolved around supposed inconsistencies with the freedom of expression and interference with business demands for data.

243 In an op-ed about the New York Bill A05323 (titled "An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act"), Eugene Volokh criticizes the bill for being too broad and unconstitutional: "the deeper problem with the bill is simply that it aims to censor what people say, under a broad, vague test based on what the government thinks the public should or shouldn't be discussing. It is clearly unconstitutional under current

Amendment of the U.S. Constitution protects. The debate is currently ongoing, with scholars finding elements of the right to be forgotten existing in the jurisprudence.[244] Among the latest state laws, the CCPA now includes a right to deletion, with a First Amendment exception[245] (a similar exception exists in the GDPR).[246]

The conceptual differences between China and the UN over the right to freedom of expression are well known.[247] In addition to that, free speech activists sometimes criticize the right as a way to facilitate censorship.[248] This could lead one to think that a right to be forgotten would be less problematic in China than in the U.S. However, in May 2016 (before the CSL took effect), the Haidian

---

First Amendment law, and I hope First Amendment law will stay that way (no matter what rules other countries might have adopted)," Eugene Volokh, *N.Y. bill would require people to remove 'inaccurate,' 'irrelevant,' 'inadequate' or 'excessive' statements about others*, WASH. POST (Mar. 15, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/15/n-y-bill-would-require-people-to-remove-inaccurate-irrelevant-inadequate-or-excessive-statements-about-others/ (last visited Aug 13, 2019).

244 *See generally* Amy Gajda, *Privacy, Press, and the Right to Be Forgotten in the United States*, 93 WASH. L. REV. 201 (2018).

245 CCPA § 1798.105.(d)(4).

246 GDPR art. 17(3)(a), providing that the right to erasure is not applicable when the processing is necessary "for exercising the right of freedom of expression and information."

247 *See generally* Caroline Syversen Lilleby, *The right to freedom of expression in China and the West: China's right to a cultural specific freedom of expression orientation?*, NORWEGIAN U. LIFE SCI. (2017). As the author summarizes, "The [United Nation's] criticism of China's freedom of expression orientation is embedded in a universalist understanding and conflicts with the cultural relativistic position China takes over the same rights. China and cultural relativists argue that the cultural, historical and political particularities of a state impact human rights orientation and by such, never can be universal."

248 As Thomas Hughes, executive director of Article 19, an NGO supporting the free speech as a human right said: "if European regulators can tell Google to remove all references to a website, then it will be only a matter of time before countries like China, Russia and Saudi Arabia start to do the same. The [ECJ] should protect freedom of expression, not set a global precedent for censorship." Owen Bowcott, *"Right to be forgotten" could threaten global free speech, say NGOs*, THE GUARDIAN (Sept. 9, 2018), https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos.

District People's Court in Beijing ruled in favor of Baidu, China's main search engine, against a plaintiff invoking the right to be forgotten, from his right of name and right of reputation.[249] The judges ruled there was no right to be forgotten in Chinese law, that the information was relevant and useful to the public because the information is recent and the plaintiff's still works in the same field, the information is important for customers to make a judgment, and he was not part of a group that required special protection such as minors.[250]

The right to erasure that exists in China since the 2012 NPC Decision[251] is not actually as far reaching as the right to be forgotten in the EU. The right has been confirmed in the CSL but is limited to the cases where the network operator has violated laws or agreements between the parties.[252] The 2018 Specification is in line with this.[253] It goes further by requiring controllers to also notify third parties to whom data have been shared to delete them, as does the GDPR, but the requirement is still only applicable where a law or an agreement has been breached. None of the other grounds found in EU law to strengthen the right to erasure exist.[254] Therefore, on the one hand the

---

[249] Ren Jiayu and Beijing Baidu Netcom Technology Co., Ltd.Beijing Haidian District First Interm People's Ct. Dec. 25, 2015). *See* Ren Jiayu and Beijing Baidu Netcom Technology Co., Ltd., , GLOBAL FREEDOM OF EXPRESSION - COLUMB. U. , https://globalfreedomofexpression.columbia.edu/cases/ren-jiayu-v-baidu/.

[250] *Id.*

[251] 2012 NPC Decision art. 8: "If a citizen discovers a network information that reveals his or her personal identity, spreads personal privacy, [. . .] he or she has the right to request the network service provider to delete the relevant information or take other necessary measures to stop it."

[252] CSL art. 43: "Where individuals discover that network operators have violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information, they have the right to request the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to request the network operators make corrections. Network operators shall employ measures for deletions and corrections."

[253] 2018 Specification art. 7.6.

[254] According to Article 17(1) of the GDPR, "the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

right to deletion is more established in China than in most laws in the U.S. On the other hand, it remains narrower than EU or California rules. In the context of the drafting of the upcoming China's comprehensive data protection law, several Chinese experts call for an extension of that right in the EU way.[255]

Also, part of the new rights related to the participation principle, the right to data portability allows individuals to ask an organization to port their data directly to another organization or to receive them in an interoperable format. In the U.S., data portability is required in California,[256] for certain health data in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[257] and the Obama administration launched the "My Data initiatives" to foster data portability in 2010,[258] but there is no overarching requirement. Data portability as a data right that spans across sectors is a novelty from the GDPR.[259]

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based [. . .] and where there is no other legal ground for the processing;
(c) the data subject objects to the processing [. . .] and there are no overriding legitimate grounds for the processing [. . .];
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) [related to the processing of the personal data of a child]."

255 *E.g.* Qi Aimin, professor at Chongqing University's School of Law: "China can learn a lot from GDPR, including conditions of user consent, the formulation of an enterprise's privacy policy, the establishment of the right to be forgotten, and punitive measures against violations," Sheng Wei, *One year after GDPR, China strengthens personal data regulations, welcoming dedicated law*, TECHNODE (June 19, 2019), https://technode.com/2019/06/19/china-data-protections-law/.

256 CCPA, § 1798.100.(d).

257 1996 Health Insurance Portability and Accountability Act ("HIPAA").

258 Alexander MacGillivray & Jay Shambaugh, *Exploring Data Portability*, WHITEHOUSE (2016), https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability.

259 GDPR art. 20.

China follows the EU direction in the 2018 Specification, that grants the data portability right to individuals. It requires data controllers to give their personal information to data subjects or directly transfer them to a third party. However, this right is more limited than in the EU because it concerns only individuals' basic information and information about their identities, and health, psychological, education and work information.[260] This is another example where China offers more data rights than the U.S. without going as far as the EU.

Finally, another area where China follows the EU in enhancing individuals' rights is the restrictions on automated decision-making, including profiling. In the EU, a "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[261] This provision is subject to several exceptions[262] and, where a decision is taken, there needs to exist suitable safeguards to protect the individual's rights, freedoms, and legitimate interests.[263] This requirement is a feature that is specific to the EU approach on data protection.[264] In the U.S., there is no similar general prohibition on decisions based solely on automated decision-making,[265] although U.S. residents do enjoy certain rights to information or to contest in certain situations under specific laws, such as the Fair Credit Reporting Act or the Equal Credit Opportunity Act. The CSL does not mention automated processing or profiling, nor did previous Chinese laws. The 2018 Specification is the first legal instrument to define profiling[266] and to require that in case of an

---

260 2018 Specifications art. 7(9).

261 GDPR art. 22(1).

262 GDPR art. 22(2).

263 GDPR art. 22(3); WP29, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01)," adopted on Oct. 3, 2017 (revised on Feb. 6, 2018), 27.

264 Greenleaf, *supra* note 3, at 74.

265 Gabriela Bodea et al., *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield (Fact-finding and assessment of safeguards provided by U.S. law)*, EUROPEAN COMMISSION 40 (2018).

266 2018 Specification art. 3.7.

automated decision-making, the data controller should provide means for data subjects to lodge a complaint.[267]

Among other similarities with EU rules found in the 2018 Specification, details concerning organizational management or delegated processing reflect the influence of EU rules. For example, the data controller should conduct a security impact assessment to ensure that the data processor provides sufficient security safeguards and carry out an audit, as it should under the GDPR. Similarly, the data processor is bound to process data according to the controller's instructions and cannot retain them after the relationship terminates. Requirements on organizational management found in the specification[268] remind of the Data Protection Officer's ("DPO") mission assigned by the GDPR: data controllers should appoint a person responsible for personal data protection, whom should be in-house if the controller crosses the defined thresholds.[269] This person is in charge of implementing compliance within the organization and of tasks such as trainings, audits and personal data protection impact assessments. Those assessments recall the data protection impact assessments required by the GDPR.[270]

The above shows that the latest Chinese rules indeed go beyond most U.S. laws and feature elements originating in EU law. However, this convergence is not linear, as there is still no sign of convergence on several principles. In addition, and crucially, data privacy remains lower in China than both the EU and the U.S. on several points. While on other aspects, China shows its own direction,

---

[267] 2018 Specification art. 7.10: "When a decision is made on the basis of information system automated decision-making and has significant impact on the data subject's rights and interests (for example, when user profiling determines personal credit and loan amounts, or in user profiling for interview screening), the data controller should provide means for data subjects to lodge a complaint."

[268] 2018 Specification art. 10.

[269] According to Article 10.1 (c) of the Specification, the person in charge of the protection of personal data should be established in-house if the main business: involves the processing of personal information and the number of employees exceeds 200; processes personal information of more than 500,000 people or expects to process personal data of more than 500,000 people within twelve months.

[270] Comparing Article 10.2 of the Specification and Article 35 of the GDPR.

out of the paths that they traced out; those are China's specificities on data privacy.

V. DATA PRIVACY WITH CHINESE CHARACTERISTICS

The previous developments assessed the convergence of China with a foreign model. But Chinese laws showcase significant characteristics which are not found in either the EU or the U.S. approaches, expressing China's own rationale on personal data protection. They are strongly correlated with the particularity of China's wider context and relate to outbound data transfers (IV.A) and the dichotomy between civil liberties and consumer privacy (IV.B). The specificities of China's approach, combined with the influence the country may yield, are likely to bear significant consequences on policy developments in the EU, the U.S., and generally on fields heavily relying on personal data and such as artificial intelligence, which is at the core of China's cyber-strategy (IV.C).

A. Data Localization and Cross-Border Data Transfers: Impacts of the Cyber-Sovereignty Principle

Data localization provisions (requiring that at least a copy of personal data should remain within the country's border) and restrictions applied to cross-border transfers of personal data are among the legal elements that are most contentious and feature the least convergence between the three approaches. It is also where Chinese laws show most of their specificities but are the fuzziest so far.

In the absence of an international treaty to which the EU, the U.S. and China would be parties, they each regulate data exchanges pursuant to their own requirements and philosophies. The U.S approach is the simplest, as there are no special requirements for transferring personal data from the U.S. to a third country. The U.S. is also among the strongest opponents to data localization restrictions, seen as trade barriers.[271] Experts from the country call for prohibiting

[271] John Selby, *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?*, 25 INT'L J. L. AND INFO. TECH. 213 (2017).

digital trade barriers such as data localization laws in trade agreements,[272] which has been recently illustrated in the now defunct proposed Trans-Pacific Partnership Agreement.[273] EU law is more restrictive but has no data localization requirement that would oblige certain personal information to remain within Europe. However, cross-border data transfers can happen only when respecting the level of protection set by the GDPR, therefore to third countries with a level of data protection which the European Commission recognizes as equivalent to the EU's, or by using appropriate safeguards such as standard contractual clauses or binding corporate rules.[274] This difference with the U.S. has been labelled as a "dramatic distinction" by legal scholars.[275]

In China, requirements on the matter were mostly absent from previous laws. Now, they are directly impacted by the principle of cyberspace sovereignty, or cyber-sovereignty, that the CSL establishes in its Article 1.[276] Cyber-sovereignty is part of the broader cyber-strategy of China and geopolitical stance.[277] Pursuant to this concept, the cyberspace is subordinated to the interests and values of a country within its borders, *i.e.* the application of state sovereignty to cyberspace; it's opposed to the multi-stakeholder governance model that supports a free and open Internet.[278] The cyber-sovereignty

---

[272] Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* ITIF (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

[273] GRAHAM GREENLEAF, *The TPP Agreement: An Anti-Privacy Treaty for Most of APEC*, UNSW L. RES. PAPER (2015), https://papers.ssrn.com/abstract=2736115 (last visited Aug 25, 2019).

[274] GDPR art. 46.

[275] Schwartz, *supra* note 24, at 1977.

[276] CSL art. 1: "This law is formulated in order to ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons and other organizations; and promote the healthy development of the informatization of the economy and society."

[277] Adeline Poisson traces back the concept's inception to the Golden Shield Project initiated in 1998, that notably gave birth to the Great Firewall of China, *see* Poisson, *supra* note 109, at 77.

[278] *See* Eric Rosenbach & Shu Min Chong, *Governing Cyberspace: State Control vs. The Multistakeholder Model*, Paper, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD KENNEDY SCHOOL (2019),

concept was spurred by Edward Snowden's revelations on foreign access to population and national security confidential data[279] and embraced by China. To ensure its sovereignty over the cyberspace, a country may exert control over the Internet architecture, content, and data flows (exports but also imports, *e.g.* by blocking foreign content), often for security purposes.

Regarding consequences on personal information protection, the cyber-sovereignty principle engenders requirements of localization of data storage and restrictions on cross-border data transfers. Article 37 of the CSL requires "critical information infrastructure operators" that gather or produce personal information or important data during operations in China to store it in China. Those can be transferred out of the country, when it is truly necessary and after passing a security assessment[280] (that has yet to be defined). A similar obligation to store personal information within the country is not found in either U.S. or EU law, but exists in other countries such as Russia.[281] China's government stance on data localization is that it protects individuals' privacy, but also China's economic development and reduces its exposure to foreign intelligence.[282] These sweeping provisions were lobbied against by foreign companies and groups of interests.

---

https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model. The authors note that "[t]he divide between nations that support governance models based on cyber sovereignty, primarily China and Russia, and those that believe in the multi-stakeholder model, including most liberal democracies, is one of the most prominent ideological conflicts dividing cyberspace."

279 Marie Baezner & Patrice Robin, *Trend Analysis: Cyber Sovereignty and Data Sovereignty*, CSS 7 (Nov. 2018), https://www.researchgate.net/publication/325335882_Trend_Analysis_Cyber_Sovereignty_and_Data_Sovereignty. The authors then introduce their differentiation between "strategic autonomy issues related to cybersecurity and cyber sovereignty as defined by International Law."

280 CSL art. 37.

281 Federal Law No. 242-FZ on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions), enacted July 21, 2014 and took effect on September 1, 2016. Retrieved from https://pd.rkn.gov.ru/authority/p146/p191 (last visited Aug 25, 2019).

282 Aimin Qi, Guosong Shao & Wentong Zheng, *Assessing China's Cybersecurity Law*, 34 COMPUTER L. & SECURITY REV. 1342, 1353 (2018).

Eventually, data localization requirements were part of the final version of the CSL, but they were set to take effect months later than the rest of the CSL to grant companies more time to adapt.[283] However, the enforcement of those dispositions have been postponed again, *sine die*. While the press reported that this is meant to avoid exacerbating tensions amid the trade war context,[284] the delay is also explained by the missing guidelines and texts that should bring more precision to the vague and ambiguous data-transfer provisions. Important questions are indeed still waiting for answers to decipher China's approach: what are "critical information infrastructure operators," do the requirements only apply to them, and what is the content of the prescribed "security assessment"? Two draft guidelines have been issued to provide some answers, the first in April 2017 never took effect, the second in June 2019.[285]

China's approach on cross-border data transfers is sensitive and spurs interest beyond the legal and privacy communities. These provisions are indeed at the crossroads of China's concerns involving privacy, surveillance, sovereignty and economic development, that are all addressed within the CSL. Compared with EU and U.S. rules, they serve the need to retain data within the jurisdiction based on a rationale that goes beyond data privacy. China is still unfolding its measures to concretize its views; how it is done and whether it is successful may inspire countries with the same motivations as China— for example, on cyber-sovereignty—to transplant these rules into their own framework, as did China with U.S. and EU rules while developing its own approach of data privacy.

---

283 Cross-border data transfers rules were set to enter into force on December 31, 2018, whereas the CSL took effect June 1, 2017.

284 Yuan Yang, *Trade war with US delays China's rules curbing data transfers*, FINANCIAL TIMES (Apr. 21, 2019), https://www.ft.com/content/c8f4b066-60df-11e9-b285-3acd5d43599e.

285 *Personal Information Outbound Transfer Security Assessment Measures* (Draft for Comment), June 2019. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/.

B. Surveillance and Privacy: The Data Protection Dichotomy in China

What is striking in China's system is the difference between the strengthening of protection against private entities and the parallel increase of government's access to personal data, as there is still no significant privacy protection against government intrusion.[286] Whereas the rights to privacy and data protection evolved favorably for the individuals/consumers in their relations with the private sector, considerable criticism still exists when those rights are assessed in the context of the relation between the citizen and the government, particularly for surveillance issues.[287] Surveillance is beyond the scope of this Article but, of course, it is far from being a Chinese practice only and the U.S. have been widely criticized for this, especially after Snowden's revelations. However, a previous comparative study made by James D. Fry, Hong Kong Faculty of Law Professor, found that many rules exist in the U.S. to regulate surveillance activities, whereas the very few dispositions existing in China are inoperative in practice.[288] In contrast, Chinese laws protect better and better individuals' rights against private entities holding their data and grant individuals more control over their data. However, this progress is counterbalanced by the increase of the government's access to data, spurred by innovations such as facial recognition. This dichotomy is observable in the CSL itself, which provides personal data protection but also contains articles limiting it on the basis of public and national security,[289] such as building backdoors into software.[290]

---

[286] Li, Bronfman, and Zhou, *supra* note 65, at 14; Lee, *supra* note 110. For example, there is no restriction on the Chinese government's power to request companies to provide access to personal information without the need for a court order, illustrating the priority of government interests over fundamental rights.

[287] *See, inter alia*, Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L. J. 853 (2013).

[288] James D. Fry, *Privacy, predictability and internet surveillance in the US and China: Better the devil you know*, 37 U. PA. J. INT'L L. 419 (2015).

[289] CSL art. 28: "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."

[290] Because the requirement for "technical support and assistance" to security organs is not defined, commentators from both business and legal

The Chinese rationale is different from both the EU and the U.S. approaches. As presented above, the EU is compelled to adopt a high level of data protection because it is guaranteed as a fundamental right within its legal system. These strong requirements on data privacy concern both private entities and the government in a similar manner. In the U.S. privacy protection is primarily conceptualized as protection against government activities, a liberty against the state power, even before rules were enacted to protect consumer privacy. In China, within this sensitive context with different conceptualizations and rationales, it is the Chinese consumer's data privacy protection that progresses, rather than a citizen's. Whereas in Western countries human rights do protect the individual from state power, human rights in China are conceived as being derived from the state itself, meaning that the state's interests remain above the individual's.[291] Moreover, the conditions to protect such rights are considered as not warranted in China today.[292] This understanding explains why individuals are gaining significant data protection rights in the private sectors but "cannot

communities have raised concerns over the need to provide backdoor access in order to comply with this provision. *See* Hannah Ji & Jerry Fang, *Costs and unanswered questions of China's new cybersecurity regime*, THE PRIVACY ADVISOR (Jan. 24, 2017), https://iapp.org/news/a/costs-and-unanswered-questions-of-chinas-new-cybersecurity-regime/; Samuel Stolton, *Chinese cybersecurity law is a "loaded weapon," senior US official says*, EURACTIV (Feb. 27, 2019), https://www.euractiv.com/section/cybersecurity/news/chinese-cybersecurity-law-is-a-loaded-weapon-senior-us-official-says/; Lee, *supra* note 110, at 72–3. Lee notes as well that similar concerns exist about the Counterterrorism Law, but also adds that these issues are not unique to China.

[291] Lee, *supra* note 110, at 99–103. "[. . .] fundamentals of China's human rights are different from those of the Western world. In the Western world, human rights were designed to protect individuals from state power since the beginning. However, China has viewed human rights as derived from the state, which reigns supreme over the individual. Therefore, human rights are never considered to represent an individual's rights over those of the Chinese state."

[292] Paul De Hert & Vagelis Papakonstantinou, *The Data Protection Regime in China*, EUROPEAN PARLIAMENT 7 (2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

claim any remedies for the infringements of their privacy carried out by the state government."[293]

To reinforce the issue, cybersecurity is conceptualized as a component of national security. The CSL indeed follows the enactment of the National Security Law,[294] which touches on personal data aspects where it allows the government to access information,[295] and the Counterterrorism Law[296] which also contains provisions related to cybersecurity and data protection.[297] The inherent consequence of this political and legal framework is that the collective interest outweighs individual freedoms and data privacy. The social credit system rating citizens based on their behavior and facial recognition in public areas for law enforcement purposes are the results of such balancing of interests. As says Xue Lan, former dean of the School of Public Policy and Management at Tsinghua University, "facial recognition may infringe on personal privacy to a certain degree, but it also brings a collective benefit, so it is a question of how to balance individual and societal benefits."[298]

This balance also goes the way of personal data protection. Despite this context and in contrary to a popular belief, Chinese people worry about the privacy of their personal data. According to a recent survey by the China Consumers Association, eighty-five percent of

---

[293] Lee, *supra* note 110, at 101. Lee further states that "While the government has endeavored to continuously enhance the human rights protection it offers, the actions of the state government itself is mostly unconstrained by fundamental human rights." The lack of access to effective remedies goes against another fundamental right in the EU, the right to an effective remedy and to a fair trial, which, at a higher level, is also part of the EU approach on data protection.

[294] National Security Law, promulgated the Standing Committee of the National People's Congress on July 1, 2015, effective on July 1, 2015.

[295] Lee, *supra* note 110, at 65.

[296] The Counterterrorism Law passed by the NPC on December 27, 2015 and came into effect on January 1, 2016.

[297] *See, e.g.* ISPs are required to provide technical support to the authorities for the purposes of preventing and investigating terrorist activities, such as decryption, pursuant to Article 18 of the Counterterrorism Law.

[298] Jane Zhang, *Privacy vs social good: AI must balance responsibilities, China governance expert says*, SOUTH CHINA MORNING POST (Aug. 20, 2019), https://www.scmp.com/tech/policy/article/3023407/old-problem-balancing-individual-rights-social-good-just-important-ai.

people suffered a data leak, spurring public anger.[299] The leakage of personal data indeed grew to unbearable levels. In 2016, it caused an 91.5 billion RMB loss to the Chinese economy (about 13 billion USD).[300] In addition, dramatic cases making the headlines move the public opinion and stimulate the debate around personal data protection. One such example is the Xu Yuyu case: following the disclosure of personal information, a scammer stole this eighteen-year-old student's money that her family had saved for her to go to college. The young girl then died of heart attack on the way back from the police station.[301]

Facing this situation, China's government has to act to better protect individuals' data privacy. With a dual objective: Chinese consumers trust in the digital economy strengthens while the government becomes a privacy protector. China's challenge is to secure the flow of personal data that is vital for the development of the digital economy, while ensuring the government's control. This explains why, on the one hand, concerns rise about surveillance—for example around the social credit system[302] and facial recognition—while on the other hand, new rules go beyond the minimalist protections as found in the U.S., and towards the more protective EU model, forming China's dual approach on personal data protection.

---

[299] As reported by the Financial Times, Yuan Yang, *China's data privacy outcry fuels case for tighter rules*, FINANCIAL TIMES (2018), https://www.ft.com/content/fdeaf22a-c09a-11e8-95b1-d36dfef1b89a. The original report in Chinese from the China Consumers Association being available at http://www.ce.cn/xwzx/gnsz/gdxw/201811/28/t20181128_30892018.shtml.

[300] CHINA DAILY, *Online infringements cost $13.8b a year*, (June 24, 2016), http://www.chinadaily.com.cn/business/2016-06/24/content_25841504.htm (last visited Aug. 25, 2019).

[301] In China, consumers are becoming more anxious about data privacy, THE ECONOMIST, (Jan. 25, 2018), https://www.economist.com/china/2018/01/25/in-china-consumers-are-becoming-more-anxious-about-data-privacy (last visited Aug. 25, 2019).

[302] Yongxi Chen & Anne S. Y. Cheung, *The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System*, 12 J. COMP. L. 356 (2017); Martin Chorzempa, Paul Triolo & Samm Sacks, *China's Social Credit System: A Mark of Progress or a Threat to Privacy?*, Policy Brief, PETERSON INST. FOR INT'L ECON. (June 2018), https://ideas.repec.org/p/iie/pbrief/pb18-14.html.

C. Artificial Intelligence Regulations as a Next Step and Consequences on EU and U.S. Policies

EU, U.S., and China all take a different path on data protection, but they all support that it will foster the development of new business models related to personal data and new fields such as artificial intelligence ("AI"). AI indeed requires the collection and processing of large amounts of personal data to learn and make decisions, which conveys that data protection rules are—or will be—a central part of AI regulation.

The last couple of years have seen the development of a race for the leadership in AI, which is fueled on personal data (*e.g.* facial recognition systems). As previously underlined here, China was a latecomer in data privacy regulation. But this is not the case for AI, which is a crucial part of China's cyber strategy. In regard to this, opponents of stronger data protection laws in the U.S often use China as a convenient argument. According to the narrative developed, strengthening data privacy in the U.S. would be like a millstone around the neck of American companies, whereas their Chinese counterparts thrive from a lack of privacy regulation on their domestic market. For example, during Mark Zuckerberg's Senate hearing following the Cambridge Analytica scandal, Facebook's CEO called for avoiding regulations that would hurt U.S. innovation and favor Chinese competitors.[303] "[W]e still need to make it so that American companies can innovate in [areas such as facial recognition], or else we're going to fall behind Chinese competitors and others around the world who have different regimes."[304] Or, as a Credit Suisse executive puts, "what will make China be big in AI and big data is: China has no serious law protecting data privacy."[305] This narrative has started being disproved

---

[303] Natasha Lomas, *Zuckerberg urges privacy carve outs to compete with China*, TECHCRUNCH (Apr. 10, 2018, 4:48 PM), http://social.techcrunch.com/2018/04/10/zuckerberg-urges-privacy-carve-outs-to-compete-with-china/.

[304] WIKISOURCE, *Zuckerberg Senate Transcript 2018*, https://en.wikisource.org/wiki/Zuckerberg_Senate_Transcript_2018 (last visited Aug. 25, 2019).

[305] Yen Nee Lee, *China will win the A.I. race, according to Credit Suisse*, CNBC (Mar. 22, 2018, 2:08 AM EDT), https://www.cnbc.com/2018/03/22/credit-suisse-china-will-win-the-ai-race-due-to-lack-of-serious-laws-on-data-protection.html.

by experts in the U.S.,[306] and the present Article demonstrates that China lacks data protection rules but is now rapidly catching up, with a clear tendency towards requirements higher than the minimalist approach favored by the U.S. The fact that this progress undermines a common argument of opponents to the strengthening data privacy protection in the U.S. is a first important consequence of China's new approach.

The CSL is one of the laws that should build the relevant legal framework that China needs for a healthy development of AI. China outlined its strategy to become the leading AI power by 2030, through the Next Generation Artificial Intelligence Development Plan[307] that the State Council released in July 2017. The plan outlines the need to "develop laws and regulations and ethical norms that promote the development of AI," privacy being explicitly mentioned, as the first of six supporting measures.[308] In March 2019, the Ministry of Science and Technology established the New Generation AI Governance Expert Committee (a committee composed with experts from academia and AI industry, tasked with researching policy recommendation for AI governance[309]) which released, in June 2019, eight governance

---

306 Graham Webster & Scarlet Kim, *The Data Arms Race Is No Excuse for Abandoning Privacy*, FOREIGN POLICY (Aug. 14, 2018, 11:43 PM), https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/.

307 New Generation of Artificial Intelligence Development Plan, issued by the State Council on July 8, 2017. Retrieved from https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf (last visited Aug. 26, 2019).

308 The five other supporting measures are, in order, "Improve the key policies that support AI development"; "Establish standards and the intellectual property system for AI technology" (where privacy is mentioned); "Establish safety supervision and evaluation systems for AI" (where privacy is also mentioned); "Vigorously strengthen training for the labor force working in AI"; "Carry out a wide range of AI science activities."

309 For the composition of the committee, *see* Lorand Laskai and Graham Webster, *Translation: Chinese Expert Group Offers 'Governance Principles' for 'Responsible AI'*, NEW AMERICA (June 17, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/ (last visited Aug 26, 2019).

principles to develop responsible AI.[310] The fourth principle being to "respect privacy" and the related individuals' rights.[311] Privacy is also part of the draft Joint Pledge on Artificial Intelligence Industry Self-Discipline, issued by China's Artificial Intelligence Industry Alliance in May 2019.[312] This year, guidelines have been issued in various other countries and organizations, such as the UN, the Council of Europe, the OECD (China and Russia did not take part in it), the G20 and the European Union. So far, they remain general declarations that AI should be ethical. Going further, the EU also recently stated its goal to pass legislation that "should set a world-standard for AI regulation" with rights building on the GDPR.[313] In China, the above-mentioned principles and official plan show that the country is decided to participate in laying out the theoretical foundations on which AI will evolve, with privacy among its fundamental principles and within the framework established by the CSL and the forthcoming Chinese personal data protection law.[314] However, and pursuant to the Chinese dichotomy on data privacy identified in this Article,[315] domestic companies working with the government on AI technologies involving privacy issues such as live facial recognition may be able to develop solutions within a less restrictive context than those working with the EU or U.S. governments—and successfully so, if one considers the example of Megvii, a Beijing-based startup specialized in facial

---

310 Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence (AI Principles), issued by the National New Generation Artificial Intelligence Governance Expert Committee on June 17, 2019, *see* Laskai and Webster, *supra* note 310.

311 AI Principles, IV: "AI development should respect and protect personal privacy and fully protect the individual's right to know and right to choose. In personal information collection, storage, processing, use, and other aspects, boundaries should be set and standards should be established. Improve personal data authorization and revocation mechanisms to combat any theft, tampering, disclosure, or other illegal collection or use of personal information."

312 Joint Pledge on Artificial Intelligence Industry Self-Discipline (Draft for Comment), issued by the Artificial Intelligence Industry Alliance on May 31, 2019. Retrieved from newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-ai-alliance-drafts-self-discipline-joint-pledge/ (last visited Aug 26, 2019).

313 Mehreen Khan, *EU plans sweeping regulation of facial recognition*, FINANCIAL TIMES (Aug. 22, 2019), https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9.

314 *See supra* section II.C.

315 *See supra* section IV.B.

recognition, that may raise 1 billion USD in its coming initial public offering.[316]

Therefore, the reinforcement of China's rules on data protection bears meaning for both the EU and the U.S. The policy recommendation that can be made for each regime is largely different and reflects their opposite approaches. For the EU, China's new direction ought to be seen favorably and both should collaborate on future AI regulation. However, the persisting dichotomy between privacy from companies and privacy from the government clashes with the EU value of personal data as a fundamental right, while data transfers from the EU to China are growing exponentially. In this context, the question is whether the current set of safeguards existing under the GDPR for these data flows, mainly contractual clauses, are sufficient and appropriate. A few initiatives to ignite a debate have been undertaken, such as an oral question to the European Commission from members of the EU Parliament,[317] or a call from the president of Italy's data protection authority for an EU-China Privacy Shield.[318] The issue has received very little interest so far,[319] and all the attention seems to be addressed at controversies over data flows from Europe to the U.S. instead (for problems akin to those of data flows from the EU to China), but observers tend to think that EU's attention

---

316 Julie Zhu, *Chinese AI start-up Megvii files for Hong Kong IPO of at least $500 million*, REUTERS (Aug. 26, 2019), https://www.reuters.com/article/us-megvii-ipo-idUSKCN1VG05I .

317 Axel Voss et al., *Oral question with debate - Personal data transfers to China - what protection for EU citizens? - O-000036/2016*, EUROPEAN PARLIAMENT - PARLIAMENTARY QUESTIONS (2016), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bOQ%2bO-2016-000036%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN (last visited May 5, 2019).

318 Antonello Soro, *Contro il totalitarismo digitale serve un Privacy Shield Ue-Cina*, GARANTE PRIVACY (May 15, 2019), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9113810.

319 Zhao and Mifsud Bonnici, *supra* note 199, at 129.

may be more balanced between concerns on China and the U.S. in the near future.[320]

The consequences that China's approach on data protection should have on the U.S. are different. Opponents to the strengthening of data privacy in the U.S. cannot rely anymore on the argument saying that Chinese companies do not have to face privacy regulation in their domestic market. In addition to that, China intends to build privacy inside its AI regulation framework, as does the EU. If the U.S. does not depart from its minimalist approach, it risks letting the EU and China shape the future of AI regulation and the ethical use of personal data, as it did let the EU set the global standard for data privacy. However, the U.S. is now leading in the protection of personal data on the basis of national security. The concept of national security and its protection through limiting acquisition of American companies by foreign entities has recently been extended to include large controllers of personal data, as exemplified by the failed acquisition of Moneygram by China's Ant Financial (part of Alibaba group).[321] The Committee on Foreign Investment in the United States ("CFIUS") that reviews proposed deals for national security issues, now has jurisdiction over companies handling sensitive personal data, following the enactment of the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA").[322]

---

[320] Laurens Cerulus, *Europe eyes privacy clampdown on China*, POLITICO (Apr. 2, 2019, 2:48 PM CET), https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/ (last visited Sept. 5, 2019).

[321] Louise Lucas, Shawn Donnan & Don Weinland, *Data take centre stage as Ant Financial fails in MoneyGram bid*, FINANCIAL TIMES (2018), https://www.ft.com/content/fd22dd9c-f06d-11e7-b220-857e26d1aca4 .

[322] Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), effective on August 13, 2018. Section 721 of the Defense Production Act of 1950, as amended, is codified at 50 U.S.C. § 4565. Retrieved from https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf (last visited Aug. 6, 2019). China transplanted the CFIUS mechanism into its legal framework but does not yet expressly include concerns over the privacy of personal data into the national review's scope. The EU recently passed a regulation for the screening of foreign direct investment, which includes issues related to personal data, but it relies on each Member States existing mechanism. Regulation 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing a Framework for the

China, for its own part, should materialize and further its new direction into the forthcoming personal data protection law, which could help close the gap on consumer privacy with the most developed countries. This would help Chinese companies to better compete on the global market, where data protection laws are also improving, and place China in a better position to shape out the theoretical foundations of AI for its future development.

VI. CONCLUSION

China's stance on data protection is the source of a lot of fear, controversies and skepticism. They build on the assumption that the use of personal data in China is unrestricted, causing a lack of privacy protection and giving an edge to Chinese companies in the field of innovation. Whereas the protection of personal information was indeed lacking until recently, the country is now building its framework at a rapid pace but scholarly literature on the topic is still relatively scarce.

This Article has demonstrated that China gradually builds a data privacy system through the legal transplantation of both the EU and the U.S. reference models. It started from a path resembling the U.S. minimalist approach and now shows significant signs of convergence with the more stringent and comprehensive EU model. There are high chances that this trend will continue, and the law dedicated to data privacy that is on China's legislative agenda should be the next milestone in that direction.

This study has also underlined that China's approach is not merely in between the EU and the U.S. It features important specificities that will make China's approach, once the framework becomes more mature, a model itself that third countries sharing the same rationale may choose to transplant. Cyber-sovereignty and the dichotomy between privacy from private actors and privacy from the state are the most salient elements of the model that China is building. Given the country's economic and political ambitions related to its

---

Screening of Foreign Direct Investments into the Union, 2019 O.J. (L 79I) 1–14. It will become applicable on October 11, 2020.

cyber strategy, China's voice on data privacy will have an increasing impact.

To further build up this finding, China shapes the related AI regulations that are intertwined with personal data usage. Unlike for personal data protection *stricto sensu*, China is not a latecomer here and will now be able to push its vision on AI rules, and participate with the EU and the U.S to the competition for global regulatory clout. The significant improvements identified in this study concerning consumer privacy will, hopefully, infuse into China's future AI regulations.