

RETHINKING THE INTERNATIONALIZATION OF THE GDPR: A COMPARATIVE STUDY ON THE US, THE EU, AND CHINA'S APPROACHES ON DATA PRIVACY LAW AND PENALTY AGAINST UBER AND DIDI

XI CHEN^{*}

ABSTRACT

The importance of data privacy has taken center stage. In response, nations worldwide are establishing data privacy protection legal systems or are renewing those outdated systems. Despite once taking different approaches, the European Union's (EU) model is now the most influential, as nations are following it with comprehensive and strict rules.

This article primarily uses the EU, the United States (US), and China as key examples to explore the historical development and evolving trends of data privacy law. It examines the similarities and differences in national approaches to data privacy legislation, highlighting a new trend of aligning with the European Union's comprehensive model. To illustrate, the article employs a case study approach, focusing on the EU and the US's penalty against Uber a major ride-hailing company headquartered in California, and the Chinese government's penalty against Didi, a giant ride-hailing company in China.

While the General Data Protection Regulation (GDPR) influences global data regulation, its expansion raises complex questions about legal transplantation. By critically analyzing cases about the GDPR Model's expansion, the article introduces the Brussels Model and the Gravity Assist Model as two explanations for the phenomenon. It argues that while the GDPR Model provides a powerful regulatory template, nations should selectively adapt it instead of replicating it wholesale.

^{*}J.D. Candidate 2026, University of Wisconsin Law School; LL.B. and B.A., China University of Political Science and Law. I would like to express my deep gratefulness to everyone who helped me in my law school journey.

Abstract.....	329
Introduction.....	331
I. Data Privacy Law in the EU, the US, and China.....	333
A. The EU's Approach: The General Data Protection Regulation (GDPR)	333
B. The US's Approach to Data Privacy Law	335
i. State Law	335
ii. Sector-Specific Law	336
iii. Regulatory Philosophy behind the Fragmented Data Privacy Law	336
C. China's Approach to Data Privacy Law	337
II. The Growing Convergence Toward the GDPR Model	339
A. The US's Modern Convergence towards the EU Model....	339
i. Federal Effort.....	340
ii. State Effort.....	340
B. China's Convergence Toward the EU Model	341
i. A Shift from Fragmented Laws to Comprehensive Legislation	341
ii. Stricter Regulations on Cross-Border Data Transfers ...	342
iii. Recognition of Privacy as a Fundamental Right	342
C. Global Trend: The EU Model is Becoming the Mainstream	342
III. Case Study: An Analysis Comparing the EU and the US's Penalty Against Uber and China's Penalty Against Didi	344
A. The EU's Strict Enforcement of the GDPR and EU's Wranglings with the US.....	344
B. US FTC Convergence Model with the GDPR Accountability Mechanism	345
C. China's Selective Alignment: GDPR-Like Structure with a National Security Core.....	347
IV. A Critical Appraisal on the Expansion of the GDPR Model	349
A. The Dominant Explanation of the GDPR Model's Global Expansion	349
B. The Gravity Assist Model: An Alternative Explanation and its Implication	351
V. Conclusion	352

INTRODUCTION

The importance of protecting data privacy through legislation has gained more attention as technological advances enabling attacks on data privacy become more common.¹ Countries once took different approaches to protect data privacy.² However, there is a clear trend towards adopting the comprehensive model for data privacy law used by the European Union (EU).³

The EU regards data privacy as a fundamental right and has established a comprehensive regulation to provide data privacy strong protection, notably through the General Data Protection Regulation (GDPR).⁴ Countries like the US and China have historically taken different approaches than the EU.⁵ Specifically, the US has traditionally taken a more fragmented and sectoral approach that lacks any comprehensive regulations on data privacy protection.⁶ Historically, China has followed the US approach by dispersing its rules in various fragmented regulations.⁷ However, recent legislative developments suggest that both the US and China, along with many other countries, are moving towards a more EU-like model of data privacy regulation.⁸ The US is shifting from a fragmented model of data privacy law toward a comprehensive one.⁹ China has already abandoned its US-style fragmented framework in favor of an approach with comprehensive data privacy law, and has established its own data privacy protection system with special focus on China's specific political and legal context.¹⁰

The government's penalties illustrate the difference in philosophies and approaches in the governments' regulation of Uber and Didi. Uber is a ride-hailing corporation headquartered in California that operates worldwide.¹¹ Didi is its counterpart ride-hailing corporation

¹ See Andrew P. Quay, Note and Comment, *Desperation for Legislation: The Need for the American Data Privacy and Protection Act*, 41 WIS. INT'L L.J. 707, 708 (2024).

² Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, 18 COLO. TECH. L.J. 25, 25 (2020).

³ *Id.* at 30.

⁴ Quay, *supra* note 1, at 708.

⁵ Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between The U.S. and the EU?*, 8 PENN. ST. J.L. & INT'L AFFS. 49, 52–53 (2020).

⁶ *Id.* at 53.

⁷ *Id.* at 53–54.

⁸ Pernot-Leplay, *supra* note 2, at 25.

⁹ *Id.* at 45–46.

¹⁰ Pernot-Leplay, *supra* note 5, at 55, 78–79.

¹¹ Uber Techs., Inc., Annual Report (Form 10-K) 4, 6 (Feb. 14, 2025).

which operates in China.¹² Despite the governments relying on different rationale when penalizing the two ride-sharing companies, one can observe the influence of the GDPR. The EU penalized Uber for failing to implement data privacy safeguards,¹³ revealing the EU's long-term concern towards the US's insufficient data privacy protection. The US government's penalty against Uber, which relies on the Federal Trade Commission (FTC) settlement model, shows the trend of convergence GDPR-style mechanism. China's penalty against Didi for its failure to implement data privacy safeguards relies on a penalty structure that closely aligns with the GDPR, with a special emphasis on national security.

Although the expansion of the GDPR is undeniable, scholars have introduced different theories to explain the phenomenon. The dominant theory is the Brussels Effect introduced by Professor Anu Bradford.¹⁴ Under this theory, the EU can export its legal standard to the whole world through its global influence on the economy.¹⁵ In the current case, the GDPR's expansion is due to the EU's huge market size and other countries' desires to enter the EU market.¹⁶ This mainstream explanation, however, cannot fully explain some cases in which countries selectively borrow rules in the GDPR instead of blindly following them. Some scholars have introduced the Gravity Assist Model as an alternative, under which countries make use of the GDPR but build their own rules.¹⁷ The Gravity Assist Model provides insight into how to accept the GDPR Model's expansion while avoiding the negative effects of blindly following.

¹² Cate Cadell, China's Didi to invest \$1 billion in its Auto Services Platform, REUTERS (Aug. 6, 2018), <https://ca.reuters.com/article/technologyNews/idCAKBN1KR0IG-OCATC> [https://perma.cc/478J-D77J].

¹³ Daniel Alvarez, Laura Jehl, Briony Pollard, Susan Rohol & Kari Prochaska, *Dutch DPA Fines Uber €290m for GDPR Data Transfer Violation*, WILLKIE FARR & GALLAGHER LLP (Sep. 12, 2024), <https://www.willkie.com/-/media/files/publications/2024/09/dutch-dpa-fines-uber-290m-for-gdpr-data-transfer-violation.pdf> [https://perma.cc/GF48-VW7G].

¹⁴ Lisa Haro, *A Book Review of Anu Bradford's "The Brussels Effect: How the European Union Rules the World"* (Aug. 19, 2025), <https://www.uni.lu/fdef-en/articles/a-book-review-of-anu-bradford-the-brussels-effect-how-the-european-union-rules-the-world/> [https://perma.cc/2VDS-6RZV].

¹⁵ *Id.* at 1.

¹⁶ Cara Mannion, Note, *Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets*, 53 VAND. J. TRANSNAT'L L. 685, 693 (2020).

¹⁷ Wenlong Li & Jiahong Chen, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China*, COMPUT. L. & SEC. REV., Sept. 2024, at 6.

This article proceeds in four parts. Part I offers an overview of the development and basic data privacy structures in the EU, the US, and China, as well as the philosophical choices behind each structure. Part II examines the trend of globalization of the GDPR Model. Part III presents two case studies to demonstrate the difference between the operation of data privacy law of the EU, the US, and China, and the trend of following the GDPR Model. Part IV introduces two models explaining the globalization of the GDPR and provides a critical appraisal of the GDPR's expansion.

I. DATA PRIVACY LAW IN THE EU, THE US, AND CHINA

The importance of enacting laws to protect data privacy is gaining attention worldwide. However, countries have taken different approaches in adopting their data privacy laws. This part examines the approach taken by the EU, the US and China. As discussed above, the EU has adopted an approach that regulates data privacy with a comprehensive law and regards data privacy as basic human rights.¹⁸ Contrarily, the US has taken an approach with mainly fragmented regulations.¹⁹ China, after initially adopting the US model, has now established its own comprehensive data privacy protection law.²⁰

A. THE EU'S APPROACH: THE GENERAL DATA PROTECTION REGULATION (GDPR)

The EU enacted the GDPR in 2018 as a comprehensive law regulating personal data protection issues.²¹ The EU enacted the law in response to the flaws in its Data Protection Directive, which is a legal act that requires member states to reach a certain outcome without proscribing the methods for doing so.²² This flexibility can be beneficial, as it allows for adaptation to different cultural and legal environments.²³ In the case of data privacy law, however, the disadvantages substantially outweighed the benefits, because member states had similar regulatory culture and data

¹⁸ Quay, *supra* note 1, at 708.

¹⁹ Pernot-Leplay, *supra* note 5, at 53.

²⁰ *Id.* at 78–79.

²¹ Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 772 (2019).

²² Julian Schneider, *The Origins and Future of International Data Privacy Law*, 47 U.C. L. SF INT'L L.J. 1, 19–20 (2024).

²³ *Id.* at 19.

could flow easily across the border.²⁴ Therefore, there was little benefit to allowing countries to adapt the law while sacrificing the uniformity of it. For these reasons, the GDPR replaced the Data Protective Directive on May 25, 2018 in the EU.²⁵

As is stated above, the GDPR is a comprehensive data privacy law.²⁶ The law is divided into eleven chapters.²⁷ It defines rights for data subjects and outlines obligations for data controllers and processors.²⁸ It also governs the cross-border data transfer and includes provisions for enforcement and regulatory cooperation within the EU.²⁹ Additionally, the GDPR allows for specific adaptations by member states in particular contexts, which ensures a robust framework for data protection across diverse scenarios.³⁰ Notably, Article 45 of the GDPR mandates that adequacy decisions of a third country's data privacy safeguards be based on a holistic assessment of that country's legal system.³¹

This comprehensive structure is consistent with the EU's stance on valuing data privacy as a fundamental human right, which is also reflected in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.³² Article 8 of the European Convention on Human Rights states that: "Everyone has the right to respect for his private and family life, his home and his correspondence."³³ Furthermore, The Charter of Fundamental Rights of the European Union strengthens the safeguard by promising the right to the protection of personal data.³⁴ It puts data protection at the same level of importance as rights on free speech or due process.³⁵ Article 8 in the Charter reads:

1. Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes

²⁴ *Id.* at 19–20.

²⁵ Schwartz, *supra* note 21, at 772, 784.

²⁶ Quay, *supra* note 1, at 708.

²⁷ See Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 [hereinafter GDPR].

²⁸ See *id.*

²⁹ See *id.*

³⁰ See *id.*

³¹ See *id.* art. 45.

³² Vanessa Perumal, *The Future of U.S. Data Privacy: Lessons from the GDPR and State Legislation*, 12 NOTRE DAME J. INT'L & COMPAR. L. 99, 104 (2022).

³³ Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

³⁴ Perumal, *supra* note 32, at 104.

³⁵ Charter of Fundamental Rights of the European Union, arts. 8, 11, 47, Dec. 18, 2000, 2016 O.J. (C 202) 389.

and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

2. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.³⁶

Following its approach holding that data privacy is a fundamental human right, the EU exerts a stricter policy on data privacy protection than most other countries, such as the US. This is reflected in the legislation. Some principles are taken by the EU but not the US.³⁷ For example, the GDPR gives sensitive data some additional protection, while the US does not have such a requirement.³⁸ On the other hand, some principles exist in both EU and US legislation, but the EU includes stricter rules than the US.³⁹

B. THE US'S APPROACH TO DATA PRIVACY LAW

There is not a comprehensive data privacy law in the US, and related regulations are split between state law or sector-specific federal data law.⁴⁰

i. State Law

Despite repeated attempts, Congress has yet to enact a comprehensive federal data privacy law.⁴¹ Due to the lack of a comprehensive federal law, several states have taken measures to enact their own legislation on data privacy law.⁴² For example, California passed the California Consumer Privacy Act as a comprehensive law with a similar structure to the GDPR soon after the GDPR was enacted.⁴³ Similarly, Colorado, Utah and Virginia passed their own comprehensive state laws.⁴⁴

³⁶ *Id.* art. 8(3).

³⁷ Pernot-Leplay, *supra* note 2, at 38.

³⁸ *See id.* at 31, 38.

³⁹ *Id.* at 38.

⁴⁰ Quay, *supra* note 1, at 711–712.

⁴¹ *Id.* at 713.

⁴² *Id.* at 712.

⁴³ *Id.* at 711–12.

⁴⁴ *Id.* at 712.

ii. Sector-Specific Law

In addition to state-level efforts, Congress has enacted sector-specific data privacy laws.⁴⁵ For example, the Health Insurance Portability and Accountability Act (HIPAA) restricts the disclosure of medical information without consent of the patient.⁴⁶ The Family Educational Rights and Privacy Act (FERPA) safeguards student records which allows children and parents the right to refuse to share information that may harm the children in the future.⁴⁷ The Children's Online Privacy Protection Act (COPPA) protects children's privacy by imposing special requirements on the processing of children's information under the age of thirteen.⁴⁸

iii. Regulatory Philosophy behind the Fragmented Data Privacy Law

The fragmentation of data privacy law in the US reflects a regulatory philosophy that favors market autonomy and innovation.⁴⁹ By opposing strict restrictions on data protection, entrepreneurs in the US gain more freedom and benefits.⁵⁰ Online intermediaries also benefit from the relatively weak privacy protections when they tailor advertisements to users' interests.⁵¹ Provided that they do not promise a higher level of data privacy protection than they actually provide, American companies are largely free to decide how they handle user data.⁵² In this way, advertisers gain more revenue from their advertisements.

Although the American government enacted some regulations to protect privacy, such as the Children's Online Privacy Protection Act of 1998, companies could easily avoid them.⁵³ The law forbids the collection of information from children under thirteen without parental consent, but millions of children avoid this limitation by entering a falsified birth date.⁵⁴ Accordingly, service providers are not responsible unless they have

⁴⁵ Rebecca Lipman, *Online Privacy and the Invisible Marker for Our Data*, 120 DICK. L. REV. 777, 787 (2016).

⁴⁶ Quay, *supra* note 1, at 712.

⁴⁷ *Id.* at 712.

⁴⁸ *Id.*

⁴⁹ W. Gregory Voss & Emmanuel Pernot-Leplay, *China Data Flows and Power in the Era of Chinese Big Tech*, 44 NW J. INT'L L. & BUS. 1 at 15.

⁵⁰ See Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 666–68 (2014).

⁵¹ See *id.* at 666–67.

⁵² *Id.* at 667.

⁵³ *Id.* at 666.

⁵⁴ *Id.*

actual knowledge that the children are lying about their age.⁵⁵ This loophole makes the law easily avoided and ineffective.

This philosophy was particularly pronounced during the 1990s.⁵⁶ The White House published a report highlighting the importance of electronic commerce.⁵⁷ Specifically, the report concludes that “existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.”⁵⁸ The report recommended that “the private sector should lead” and that “governments should avoid undue restrictions on electronic commerce.”⁵⁹

C. CHINA’S APPROACH TO DATA PRIVACY LAW

China has been much slower in creating data protection regulations than the EU and even the US.⁶⁰ China’s data protection regulations incorporate aspects of both the EU and the US models while developing its own special model of data privacy law.⁶¹

The Chinese government did not start developing data privacy laws until 2012.⁶² In 2012, China started to establish US-style data privacy law that was sector-specific.⁶³ One example is the Telecommunications and Internet Personal User Data Protection Regulation, enacted in 2013.⁶⁴ It establishes principles such as the requirements to limit data collection by service providers within China.⁶⁵ Similarly, China enacted the Cybersecurity Law in 2017 (which strengthened the control over network operators and telecom service providers) and the Data Security Law in 2021 (which reinstated the obligation on data processing and securing).⁶⁶

⁵⁵ *Id.*

⁵⁶ *Id.* at 647.

⁵⁷ A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, THE WHITE HOUSE (July 1, 1997), <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html> [https://perma.cc/T77T-XCQ6].

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ Pernot-Leplay, *supra* note 5, at 53.

⁶¹ *Id.* at 52.

⁶² *Id.* at 71.

⁶³ *Id.*

⁶⁴ *Id.* at 72.

⁶⁵ *Id.*

⁶⁶ Christopher Tan, The Great Cyberwall: Navigating China’s Cross-Border Data Laws, B.C. INTELL. PROP. & TECH. F., Aug. 6, 2024, at 6, 8.

Although China once followed the US model, it now mirrors the EU model with a national level, comprehensive data protection law.⁶⁷ In 2021, China enacted the Personal Information Protection Law (PIPL).⁶⁸ The PIPL is a comprehensive data privacy protection law whose structure is similar to the EU's GDPR.⁶⁹ The PIPL incorporates key data protection principles and acts as China's general data protection law.⁷⁰ The law contains extensive details governing rules on personal information processing, organizing, and controlling.⁷¹

Compared to the EU model, China's data privacy law is more state-centered and more oriented toward protecting national security.⁷² For example, under the PIPL, no group or individual may improperly gather, use, process, communicate, trade, supply, or reveal the personal information of another person, nor may they process personal information in a way that compromises national security.⁷³

The state-centered orientation is further illustrated by restriction on transferring data across borders.⁷⁴ Under the Data Security Law and the Chinese Cybersecurity Law, personal information or important data must be assessed on a national security perspective if the operators want them to be transferred abroad.⁷⁵ Other regulations, such as the Cybersecurity Review Measures and the Measures for the Security Evaluation of Outbound Data, set the standard for the amount of the data to be transferred before such a security assessment.⁷⁶ Besides, business data is classified under national security and public interest standards under the Data Security Law.⁷⁷ Despite having a structure similar to that of the GDPR, China's data privacy regulation imposes significantly

⁶⁷ *Id.* at 12.

⁶⁸ Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) [hereinafter PIPL].

⁶⁹ Tan, *supra* note 66, at 9.

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *Id.* at 12.

⁷³ PIPL art. 10.

⁷⁴ Gulbakyt Bolatbekkyzy, *Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation*, 11 GRONINGEN J. INT'L L. 129, 144 (2024).

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ Chi Chen & Leo Zhou, *How China's Data Privacy and Security Rules Could Impact Your Business*, EY (July 18, 2022), [https://www.ey.com/en_gl/insights/forensic-integrity-services/how-chinas-data-privacy-and-security-rules-could-impact-your-business#:~:text=The%20Personal%20Information%20Protection%20Law,\(DSL\)%20came%20into%20force](https://www.ey.com/en_gl/insights/forensic-integrity-services/how-chinas-data-privacy-and-security-rules-could-impact-your-business#:~:text=The%20Personal%20Information%20Protection%20Law,(DSL)%20came%20into%20force) [https://perma.cc/F6NZ-6MZ4].

heavier restrictions on the free flow of data because of its focus on national security.⁷⁸

Another example highlighting the PIPL's state-centered character is that the enforcement of the PIPL is carried out by the Chinese Cyberspace Administration, which serves as a national department overseeing the whole data privacy regulation process.⁷⁹ Unlike its EU counterpart, the Chinese Cyberspace Authority is directly handling law enforcement-related tasks, directing evaluating significant national security issues, and creating relevant regulations to supplement the PIPL.⁸⁰ In the EU, Data Protection Officers and Data Protection Authorities typically carry out data privacy enforcement and compliance, rather than a state-directed body.⁸¹ Under the GDPR, even third-party service providers may serve as Data Protection Officers.⁸²

II. THE GROWING CONVERGENCE TOWARD THE GDPR MODEL

Although countries have historically taken different approaches on data privacy laws, a notable trend in global data privacy regulation is that diverse jurisdictions are increasingly aligning with the EU's comprehensive approach to data protection.⁸³ The EU's GDPR serves as a global model for both developed and developing jurisdictions to follow when considering their data privacy frameworks.⁸⁴ This Part explores how various regions, including the US and China, are converging towards the EU model, and how this trend is manifesting globally, reflecting a broader shift towards standardized data privacy practices.

A. THE US'S MODERN CONVERGENCE TOWARDS THE EU MODEL

The level of data privacy protection in the US is low compared to the EU.⁸⁵ Despite the former success of the US approach, it has become increasingly difficult to respond effectively to the arising challenges in

⁷⁸ Bolatbekkyzy, *supra* note 74, at 144.

⁷⁹ *Id.* at 145.

⁸⁰ *Id.*

⁸¹ *Id.* at 142.

⁸² *Id.*

⁸³ Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIV. L. 68, 77 (May 2012).

⁸⁴ *Id.*

⁸⁵ Pernot-Leplay, *supra* note 2, at 26.

data processing.⁸⁶ Several scandals, such as the Uber scandal—which will be discussed further in Part III—brought the concern that the US approach on the matter has been insufficient and is hurting the online economy.⁸⁷ This new concern resulted in a trend toward convergence between US data privacy laws and the EU model.⁸⁸ There are two aspects of such a convergence: the federal efforts and the state efforts.⁸⁹

i. Federal Effort

The federal government of the US is now considering the implementation of new laws at the national level.⁹⁰ The US Government Accountability Office, an independent government agency that serves Congress, once reported that “recent developments regarding internet privacy suggest that this is an appropriate time for Congress to consider comprehensive internet privacy legislation.”⁹¹ The federal government introduced the Social Media Privacy Protection and Consumer Rights Act and the American Data Dissemination Act in January 2019.⁹² The former set the notification duty for entities that are involved in a data breach.⁹³ The latter extends the Privacy Act of 1974, which was formerly applied to the federal agencies, to internet service providers.⁹⁴

ii. State Effort

Separate from the federal effort, states in the US are also enacting data privacy laws similar to the GDPR Model.⁹⁵ California is at the forefront of these developments.⁹⁶ It enacted the California Consumer Privacy Act in 2018, which takes the form of a comprehensive data privacy law similar to the structure of the GDPR.⁹⁷

⁸⁶ *Id.* at 39.

⁸⁷ *Id.* at 39–40.

⁸⁸ *Id.* at 40.

⁸⁹ *Id.*

⁹⁰ Pernot-Leplay, *supra* note 2, at 45.

⁹¹ *Id.*

⁹² *Id.* at 46.

⁹³ S. 189, 116th Cong. (2019).

⁹⁴ S. 142, 116th Cong. (2019).

⁹⁵ Pernot-Leplay, *supra* note 2, at 40.

⁹⁶ *Id.*

⁹⁷ *Id.* at 41.

The California Consumer Privacy Act shows many signs of convergence with the GDPR.⁹⁸ For example, “personal information” under CCPA § 1798.140 (v)(1) is defined as follows:

“Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.⁹⁹ This definition is unlike any previous US and California law; instead, it is similar to the EU law.¹⁰⁰

California is not the only state that is enacting statutes related to personal data protection.¹⁰¹ Other states, such as Arizona, Nevada, and Colorado are also enacting laws that govern multiple dimensions of data protection.¹⁰² These regulations address a wide range of issues related to subjects like data privacy protection for specific groups and employee supervision.¹⁰³

B. CHINA’S CONVERGENCE TOWARD THE EU MODEL

Although China initially adopted a US-style sectoral approach to data privacy, China’s recent legislative developments indicate a clear shift toward the EU’s comprehensive data protection model.¹⁰⁴ The enactment of the PIPL in 2021, alongside the Cybersecurity Law and the Data Security Law, mirrors key aspects of the General Data Protection Regulation and demonstrates China’s growing alignment with the EU framework.¹⁰⁵

i. A Shift from Fragmented Laws to Comprehensive Legislation

Historically, China regulated data privacy through sector-specific laws, similar to the US approach.¹⁰⁶ However, with the introduction of the PIPL, China has adopted a unified and comprehensive data protection

⁹⁸ *Id.* at 42.

⁹⁹ Cal. Civ. Code § 1798.140(v)(1) (West 2024).

¹⁰⁰ Pernot-Leplay, *supra* note 2, at 42.

¹⁰¹ *Id.* at 43.

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ Pernot-Leplay, *supra* note 5, at 54.

¹⁰⁵ Tan, *supra* note 66, at 9.

¹⁰⁶ Pernot-Leplay, *supra* note 5, at 54.

framework, much like the GDPR.¹⁰⁷ The PIPL establishes a series of legal principles mirroring those of the GDPR governing data processing.¹⁰⁸

ii. Stricter Regulations on Cross-Border Data Transfers

One of the most significant ways that China is converging with the EU model is through its strict regulation of cross-border data transfers. Although not as strict as the EU model, the Chinese government is determined to enact stricter rules than those in the US.¹⁰⁹ For example, under the PIPL, personal data collected in China cannot be transferred abroad and must meet adequacy requirements, similar to those in the GDPR.¹¹⁰ China also introduced additional requirements that more closely align with the EU standard, such as requiring data controllers to transfer personal data at the data subject's request.¹¹¹ This marks a departure from the US approach, where cross-border data flows are less restricted, and aligns China more closely with the EU's emphasis on data sovereignty and protection of domestic user data.

iii. Recognition of Privacy as a Fundamental Right

While China's data privacy laws are still closely tied to national security concerns and state power, individual rights on data privacy against private sector actors have received an increasing amount of attention.¹¹² China's data privacy law is gaining success in enhancing individual control of their data.¹¹³

C. GLOBAL TREND: THE EU MODEL IS BECOMING THE MAINSTREAM

Besides the US and China, other countries have recognized an increasing need to promote data privacy protection. Against this background, the EU model is gaining more attention and becoming

¹⁰⁷ See Tan, *supra* note 66, at 9 (explaining that PIPL includes extensive provisions concerning personal information processing, its extraterritorial scope, general processing responsibilities, data subject rights, relationships between controllers and processors, and organizational accountability requirements).

¹⁰⁸ *Id.*

¹⁰⁹ Pernot-Leplay, *supra* note 5, at 82.

¹¹⁰ Compare Tan, *supra* note 67, at 10, and GDPR art. 45(2) b.

¹¹¹ Pernot-Leplay, *supra* note 5, at 101.

¹¹² See *id.* at 107.

¹¹³ *Id.*

mainstream.¹¹⁴ The development of the Council of Europe Convention No. 108 on data protection—its modern version known as Convention 108—exemplifies the spread of the EU model.¹¹⁵ In 1981, the EU adopted a global treaty to address the rising personal data protection concerns, which was later known as Convention 108.¹¹⁶ Originally, it served primarily as the treaty between members in the EU Council.¹¹⁷ But as it developed, the Council of the EU modernized by adopting Convention 108+.¹¹⁸ Despite the European origin of Convention 108+, non-European countries such as Argentina, Cabo Verde, Mauritius, Mexico, and others have also joined Convention 108+.¹¹⁹

The modern Convention 108+ requirements cover most new EU GDPR requirements, such as the proportionality requirement in data processing.¹²⁰ There are also principles in the new Convention that other countries have enacted.¹²¹ For example, countries like Ghana, and Chad followed the Convention 108+ approach, which requires notification of serious data breaches.¹²² Countries such as Canada, India, and Korea followed the approach of direct liability for processors.¹²³

The spread of EU-style data privacy laws to over 120 countries underscores this trend.¹²⁴ An example of its influence outside Europe is Argentina's Data Protection Act, which mirrors the GDPR in a series of elements.¹²⁵ Similarly, Senegal enacted the Act on the Protection of Personal Data in 2017, which also shares similar elements with the GDPR.¹²⁶ This global shift indicates a significant movement towards standardized data privacy practices, influenced heavily by the EU's regulatory framework.

¹¹⁴ See Greenleaf, *supra* note 83, at 13.

¹¹⁵ Graham Greenleaf, *Convention 108+ and the Data Protection Framework of the EU* (speaking notes for conference presentation, June 21, 2018), <https://ssrn.com/abstract=3202606> [<https://perma.cc/ZP2Y-U94D>].

¹¹⁶ Cécile de Terwangne, *Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data*, 40 COMPUT. L. & SEC. REV. 1, 1 (2021).

¹¹⁷ See *id.* at 2.

¹¹⁸ *Id.*

¹¹⁹ Council of Eur., *Chart of Signatures and Ratifications of Treaty 108* (Feb. 22, 2026), <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108> [<https://perma.cc/42MW-9WRU>].

¹²⁰ See Greenleaf, *supra* note 115, at 3.

¹²¹ *Id.* at 3.

¹²² *Id.* at 4.

¹²³ *Id.*

¹²⁴ *Id.* at 2.

¹²⁵ See Greenleaf, *supra* note 83, at 10.

¹²⁶ See *id.*

III. CASE STUDY: AN ANALYSIS COMPARING THE EU AND THE US'S PENALTY AGAINST UBER AND CHINA'S PENALTY AGAINST DIDI

Despite the EU, the US, and China once taking different approaches on data privacy law, there is a clear convergence toward the EU model. This tendency is revealed in the three governments' penalties against Uber and Didi. Uber was penalized in the EU and the US, while Didi was penalized in China for data leaks. This Part uses the case study approach to illustrate that although the underlying philosophies differ in those penalties, there is a clear trend toward convergence with the EU penalty model.

A. THE EU'S STRICT ENFORCEMENT OF THE GDPR AND EU'S WRANGLINGS WITH THE US

The EU has strict regulations on outbound transfer of personal data. Under Article 44 of the GDPR,

any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor. . .¹²⁷

To that end, the EU recognizes a limited set of mechanisms that render such transfers lawful, and the Standard Contractual Clause is one of them.¹²⁸ Standard Contractual Clauses are model contractual clauses pre-approved by the European Commission that serve as a legal mechanism to ensure appropriate safeguards for transferring personal data from the EU to third countries under the GDPR.¹²⁹

On August 26, 2024, the Dutch authorities fined Uber €290 million for violating the GDPR.¹³⁰ The case arose after a French human rights organization filed a complaint representing 172 Uber drivers.¹³¹ The

¹²⁷ GDPR art. 44.

¹²⁸ GDPR art. 46(3); *Standard Contractual Clauses (SCC)*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [<https://perma.cc/EUA8-EURX>] [hereinafter SCC].

¹²⁹ SCC, *supra* note 128.

¹³⁰ Alvarez et al., *supra* note 13, at 1.

¹³¹ Joanna Boag-Thomson, *290 Million Reasons to Comply: Fine Imposed on Uber for Non-Compliant Third-Party Transfers*, LEXOLOGY (Oct. 15, 2024),

complaint asserted that sensitive information such as Uber drivers' personal information related to identity, location, and even medical or criminal history, was transferred without protection.¹³² It was concluded that Uber transferred personal data to its headquarters in the US without appropriate data safeguarding measures in place.¹³³

Uber once followed the Standard Contractual Clause mentioned above, but later stopped doing so.¹³⁴ Uber claimed that they did not violate the law because no transfer occurred, since Uber BV (Uber's operation in the Netherlands) jointly controlled the data with Uber's headquarters in the US.¹³⁵ However, the Dutch Data Protection Authority rejected this reasoning.¹³⁶ The institution concluded that Uber was still required to follow the requirement on data transfer in the GDPR even if the transfer happens within the joint controllers.¹³⁷ Thus, the Dutch Data Protection Authority decided that Uber's action was a violation of the GDPR, and imposed a punishment in the amount of €290 million against the company.¹³⁸

The penalty reflects the long-standing discrepancy between the EU and the US regarding data privacy protection.¹³⁹ The Chairman of the Dutch Data Protection Authority mentioned that the GDPR "protects people's fundamental rights by requiring companies and governments to handle personal data with care."¹⁴⁰ However, such a standard is not widely recognized outside of the EU.¹⁴¹

B. US FTC CONVERGENCE MODEL WITH THE GDPR ACCOUNTABILITY MECHANISM

Despite lacking a comprehensive data privacy law like the GDPR, the US shows a tendency to converge toward the GDPR Model in their

https://www.lexology.com/library/detail.aspx?g=6f58c801-1eed-460f-81b9-147d3d303f4d&utm_source=perma.cc/XY77-JMR3].

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ *Id.*

¹³⁶ *Id.*

¹³⁷ Boag-Thompson, *supra* note 131.

¹³⁸ *Id.*

¹³⁹ Phil Muncaster, *Uber Hit With €290m GDPR Fine*, INFOSECURITY MAG. (Aug. 27, 2024), <https://www.infosecurity-magazine.com/news/uber-hit-with-290m-gdpr-fine/> [https://perma.cc/MY9T-6UW7].

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

penalty and accountability mechanisms. The 2016 Uber penalty illustrates an example of this convergence toward the GDPR Model. In 2016, the Federal Trade Commission (FTC) imposed a penalty against Uber for a data breach.¹⁴²

The FTC initiated the investigation against Uber for the data breach which happened in 2014.¹⁴³ While the investigation is ongoing, it is estimated that the hackers stole data from approximately fifty-seven million Uber users.¹⁴⁴ Joseph Sullivan, Uber's Chief Security Officer at the time, learned of the breach just ten days after testifying under oath before the FTC about Uber's cybersecurity measures.¹⁴⁵ Instead of reporting the breach, Sullivan arranged to pay off the hackers in exchange for their promise to avoid disclosing the leak.¹⁴⁶ He also had them sign a non-disclosure agreement.¹⁴⁷ Sullivan then continued to withhold information about the breach from Uber's legal team and the FTC.¹⁴⁸ The FTC ultimately imposed a three-year probationary sentence and a fine of \$50,000 on Sullivan.¹⁴⁹

Beyond individual liability, Uber as a corporation faced institutional scrutiny. In response to the scandal, Uber entered into a settlement with the FTC for a \$148 million fine in 2018.¹⁵⁰ As part of the settlement, Uber was obliged to strengthen its data privacy framework.¹⁵¹ The specific requirements include setting a standard to notify appropriate authorities of the breach of law, initiating a program to promote the corporate integrity, and recruiting an impartial third-party to supervise its data protection.¹⁵²

¹⁴² See Press Release, U.S. Att'y's Off., N.D. Cal., Former Chief Security Officer of Uber Sentenced to Three Years' Probation for Covering Up Data Breach Involving Millions of Uber User Records (May 5, 2023), <https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data> [https://perma.cc/X3JH-74GW] [hereinafter Uber Press Release].

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ Uber Press Release, *supra* note 142.

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*

¹⁴⁹ *Id.*

¹⁵⁰ Naomi Eide, *Uber's Record \$148M Fine Highlights Harsh Repercussions for Data Breach Disclosure Failures*, CIO DIVE (Sept. 27, 2018), <https://www.ciodive.com/news/ubers-record-148m-fine-highlights-harsh-repercussions-for-data-breach-dis/533387/?> [https://perma.cc/9NEB-4L6L].

¹⁵¹ *Id.*

¹⁵² *Id.*

Though many punishments still rely on existing consumer protection and criminal law, FTC settlements reflect a growing alignment with the GDPR punishment model.¹⁵³ Modern FTC consent orders go beyond reactive punishment.¹⁵⁴ Instead, they now require companies to take corrective steps such as supervising, assessing, ongoing monitoring, and training employees.¹⁵⁵ These mirror the accountability mechanisms in the GDPR.¹⁵⁶ For instance, in most FTC settlements (including the Uber settlement discussed) the FTC imposes a duty on the violator to notify the FTC of the breach.¹⁵⁷ Similarly, Article 33 in the GDPR requires data breach notification.¹⁵⁸ Likewise, the FTC has required that Uber adopt and maintain comprehensive data security and breach notification programs under multi-year oversight.¹⁵⁹ Article 24 in the GDPR implies a similar rule, which provides “the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.”¹⁶⁰

C. CHINA’S SELECTIVE ALIGNMENT: GDPR-LIKE STRUCTURE WITH A NATIONAL SECURITY CORE

According to a report, since July 2015, Didi has collected “nearly 12 million screenshots, millions of pieces of passenger facial recognition data, and more than 167 million records of location data, as well as other information.”¹⁶¹ As a result of violating data privacy, data security, and cybersecurity laws, the company was fined approximately 8 billion yuan (approximately 1.2 billion USD).¹⁶²

The Chinese government’s penalty against Didi is different from its counterpart in the Uber case due to the Chinese government’s emphasis on national security. In the press conference, the officers repeatedly

¹⁵³ Ctr. Int’l Pol’y Leadership, *Organizational Accountability in Light of FTC Consent Orders* (Working Paper No. 13, 2019), at 1–2.

¹⁵⁴ *See id.* at 1.

¹⁵⁵ *Id.* at 2.

¹⁵⁶ *Id.*

¹⁵⁷ *Id.* at 9.

¹⁵⁸ GDPR art. 33(3).

¹⁵⁹ Eide, *supra* note 150.

¹⁶⁰ GDPR art. 24(1).

¹⁶¹ Scott Warren & Lindsay Zhu, *China’s Didi Fined Over US \$1B by Chinese Data Regulators*, SQUIRE PATTON BOGGS (July 22, 2022), <https://www.privacyworld.blog/2022/07/chinas-didi-fined-over-1b-by-chinese-data-regulators/> [<https://perma.cc/ZB5A-VHJL>].

¹⁶² *Id.*

emphasized that Didi violated national data security.¹⁶³ In the conference, the Chinese Cyberspace Authority announced that two of its bases for punishment are to “safeguard against national data security risks” and “uphold national security.”¹⁶⁴ Although Uber had similar scandals in the EU and the US, similar expressions cannot be found in the two governments’ punishment reports.¹⁶⁵

While China places a special emphasis on national security in data privacy law, the structure of China’s enforcement under PIPL resembles the GDPR Model. For instance, the Chinese Cyberspace Authority follows the GDPR principle to punish the controller, and fined both the CEO and executive of Didi in the amount of 1 million yuan (148,000 USD).¹⁶⁶

Moreover, penalties under the GDPR are not limited to monetary penalties, but emphasizes ratifications and corrections measures.¹⁶⁷ A comparable logic can be found in penalties under PIPL. In the Didi case, a spokesman of the Cyberspace Administration of China (CAC) emphasized the rectifications, warnings and notifications besides fines as measures to strike against illegal activities.¹⁶⁸ In this sense, despite divergent regulatory priorities, the legal structure and enforcement basis of China’s data privacy law closely aligns with the GDPR model.

¹⁶³ See Graham Webster, *Translation: Chinese Authorities Announce \$1.2B Fine in DiDi Case, Describe ‘Despicable’ Data Abuses*, DIGICHINA (July 21, 2022), <https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/> [https://perma.cc/N7RQ-M3JV].

¹⁶⁴ *Id.*

¹⁶⁵ See European Data Protection Board, *Dutch SA Imposes a Fine of 290 Million Euro on Uber Because of Transfers of Drivers’ Data to the US* (Aug. 26, 2024), https://www.edpb.europa.eu/news/news/2024/dutch-sa-imposes-fine-290-million-euro-uber-because-transfers-drivers-data-us_en [https://perma.cc/3A68-3NXX]; see also Uber Techs., Inc., FTC Docket No. C-4662 (2018), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf [https://perma.cc/9BNC-G3N2].

¹⁶⁶ Todd Liao, *Cyberspace Administration of China Issues Statement on Didi’s \$1.2B Fines for Cybersecurity Law Violations*, MORGAN LEWIS (July 28, 2022), <https://www.morganlewis.com/pubs/2022/07/cyberspace-administration-of-china-issues-statement-on-didis-1-2b-fines-for-cybersecurity-law-violations/> [https://perma.cc/5AMT-EUB2]; CDPR art. 82(2).

¹⁶⁷ Angelos G. Paphitis & Andrea Hadjigeorgiou, *How GDPR Fines are Calculated when an EU Company is Found in Breach*, AGPLAW (Aug. 25, 2025), <https://www.agplaw.com/how-gdpr-fines-are-calculated-when-an-eu-company-is-found-in-breach/> [https://perma.cc/R9YX-3R4Q].

¹⁶⁸ Webster, *supra* note 163.

IV. A CRITICAL APPRAISAL ON THE EXPANSION OF THE GDPR MODEL

While the expansion of the GDPR Model is undeniable, it deserves scrutiny. The EU model cannot be uniformly applied globally due to the disparity in legal systems across jurisdictions. This Part critically evaluates the Brussels Effect as the dominant explanation for the GDPR model's expansion and examines the negative effects of blindly replicating the GDPR. This Part then introduces the Gravity Assist Model as an alternative explanation for the selective convergence toward the GDPR Model and discusses the Gravity Assist Model's insights on the benefits of adoption instead of replication.

A. THE DOMINANT EXPLANATION OF THE GDPR MODEL'S GLOBAL EXPANSION

Different theories explain the expansion of the GDPR Model. The dominant theory explaining the GDPR's global reach is the Brussels Effect, introduced by Professor Anu Bradford.¹⁶⁹ Under this theory, the EU, by virtue of its market power and regulatory capacity, exports its legal standards to third countries via market pressure.¹⁷⁰ Specifically, a country or region's influence over the global economy is largely determined by the size of its internal market.¹⁷¹ With an estimated GDP of about 16 trillion USD, the EU is the largest economy in the world.¹⁷² Many producers rely on this lucrative market, and few can abandon it without loss.¹⁷³ The extensive dependence compels producers to align with the GDPR principles.¹⁷⁴ This reality has led to the widespread internalization of GDPR-style regulations.¹⁷⁵

¹⁶⁹ Haro, *supra* note 14.

¹⁷⁰ *Id.*

¹⁷¹ *Id.* at 11.

¹⁷² *Id.*

¹⁷³ *Id.* at 12.

¹⁷⁴ See generally Hai Chi Nguyen, *The Impacts of GDPR on Global Organizations After 6 Years of Implementation*, CLOUDI-FI (Sept. 9 2025), <https://www.cloudi-fi.com/blog/the-impacts-of-gdpr-on-global-organizations-after-6-years-of-implementation> [<https://perma.cc/VND5-LN9T>] (discussing how Brazil, China, Japan, the U.K., the U.S., and India have modeled their data protection laws based on the GDPR).

¹⁷⁵ See *id.*

Due to the influence of the Brussels Effect, countries in Africa are shifting their values substantially regarding data privacy regulation.¹⁷⁶ Different from the strict regulatory approach in the EU, many African countries once had relaxed regulations on data privacy, which helped them to attract companies to enter the market without a requirement to comply with data privacy regulations.”¹⁷⁷ Kenya was one such country.¹⁷⁸ The loose regulatory environment in Kenya made it a hub for numerous start-up companies.¹⁷⁹ From 2021 to 2018, nearly 3,500 tech ventures were established in Kenya, leading to more than 1 billion USD in capital investment..¹⁸⁰

However, more African countries are now enacting laws that comply with the GDPR Model.¹⁸¹ Under the EU’s approach, data controllers have to follow the requirements under the GDPR to gain access to EU’s market.¹⁸² South Africa is one of the countries passing the legislature that mirrored the GDPR.¹⁸³ It passed the Protection of Personal Information Act in 2013.¹⁸⁴ The law established citizen’s constitutional right to data privacy.¹⁸⁵ Besides, the Protection of Personal Information Act contains principles that mirrors those in the GDPR, such as the duty to report data breaches and the duty to collect personal data.¹⁸⁶ The Protection of Personal Information Act also imposes strict penalty mechanisms, including imprisonment of up to ten years and a heavy fine, for those companies who violating the duty to protect personal data.¹⁸⁷

Under this new of following the GDPR Model, African countries are losing the competitive advantages derived from the previously flexible regulatory market environment.¹⁸⁸ Previously, some countries benefited

¹⁷⁶ See generally Mannion, *supra* note 16, at 706 (discussing how Kenya would no longer be able to have a lax regulatory environment as a result of the EU’s equivalency standard).

¹⁷⁷ *Id.* at 701.

¹⁷⁸ See *id.* at 698–99.

¹⁷⁹ *Id.* at 699.

¹⁸⁰ *Id.* at 701.

¹⁸¹ See *How Does Africa’s Data Laws Stack Up Against Worldwide Standards Like the GDPR?*, AFRICA HR. (Sept. 2, 2025), <https://africa-hr.com/blog/data-laws-across-africa/> [<https://perma.cc/ZK67-S6C3>].

¹⁸² Mannion, *supra* note 16, at 693.

¹⁸³ See generally *id.* at 697–98 (discussing how South Africa, which conducts a significant amount of trade with the EU, passed regulations that mirror several provisions in the GDPR, although these regulations have not yet been put into effect).

¹⁸⁴ *Id.* at 697.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ *Id.* at 697–98.

¹⁸⁸ *Id.* at 701.

from the absence of strict regulations on data privacy law because this created an attractive environment for business and investment.¹⁸⁹ With the new approach, small companies may find it hard to adopt the complex privacy standards and may be restrained from conducting business effectively.¹⁹⁰ If African countries were to adopt GDPR-style regulations, the results could be disastrous for their competitiveness in the industry.¹⁹¹

B. THE GRAVITY ASSIST MODEL: AN ALTERNATIVE EXPLANATION AND ITS IMPLICATION

Although it is undeniable that the EU can export its rules to other countries using its global influence, some scholars have considered some alternative models to account for some cases that the Brussels Effect cannot fully explain. One alternative model is the theory of Gravity Assist.¹⁹² This theory takes its metaphor from physical orbital motion.¹⁹³ Under this theory, countries can make use of the gravitational pull from existing law, like the GDPR, but adjust the previous regulations according to their unique legislative context.¹⁹⁴

China's PIPL is a good example of the Gravity Assist Model. As discussed, the PIPL borrows heavily from GDPR regulations.¹⁹⁵ The PIPL contains a similar regulatory structure to the GDPR, but is more state-centered and emphasizes national security and the interests of the public.¹⁹⁶ The PIPL would operate in a different way from the GDPR.¹⁹⁷ Special priority aligns with China's philosophy of emphasizing state interests and social stability.

This alternative explanation shows that the Brussels Effect cannot fully explain all cases of the GDPR's expansion. Its expansion is not a one-way process that countries must follow; some countries accept it out of pressure to comply while others selectively borrow it and build their own systems of data privacy law.

¹⁸⁹ *See id.*

¹⁹⁰ *See id.*

¹⁹¹ *See id.* at 701–02.

¹⁹² Li & Chen, *supra* note 17, at 3.

¹⁹³ *Id.*

¹⁹⁴ *See id.*

¹⁹⁵ Hinshaw & Culbertson LLP, *China's New Privacy Law: Both a Shield and a Sword* (Sept. 17, 2021), <https://www.hinshawlaw.com/en/insights/hinshaw-alert/chinas-new-privacy-law-both-a-shield-and-a-sword> [<https://perma.cc/ZXW2-P9RX>].

¹⁹⁶ Li & Chen, *supra* note 17, at 10–11.

¹⁹⁷ *See id.* at 11.

Countries blindly following the GDPR rules may face disastrous outcomes. The Gravity Assist Model thus offers a corrective approach by allowing countries to reconcile the tension between the regulatory convergence to the GDPR Model and the need to protect regional interests, instead of simply replicating GDPR rules. The internationalization of GDPR Model is most effective when combined with a country's own culture, politics, and society.

V. CONCLUSION

As data privacy becomes the center of the world's attention, the GDPR Model has become the dominant model of data privacy law because of its strict standard and its comprehensive scope. Its influence is not limited to the EU, having expanded to other areas of the world. Recent cases in which the US and China imposed penalties against Uber and Didi show the two countries' convergence toward the EU model. Other regions, such as South America and Africa, have followed similar trends. While the Brussels Effect provides an explanation for the GDPR Model's expansion, the theory is neither uniform nor uncontested. Some countries have selectively adopted the GDPR Model, while countries in Africa have been negatively affected by GDPR-style legislation.

The Gravity Assist Model provides an approach for rethinking the GDPR Model's global expansion. The expansion of the GDPR is undeniable, but countries adapting it should consider their differences in political and economic background and try to reinterpret the GDPR, instead of passively accepting it. The future of data privacy law lies in the balance between the appeal of GDPR Model and the need for local responsiveness.