DATA PRIVACY IN INTERNATIONAL BUSINESS: ARE CURRENT LAWS SUFFICIENT FOR JUSTICE?

Isha Taneja & Bavya B, LL.M., Symbiosis International University, Pune

ABSTRACT

Accelerated digital globalization has made cross-border information sharing easier than ever, while also exposing long-standing gaps and inconsistencies in how various countries govern data privacy. Even though many regions have established their own privacy frameworks, such as the GDPR, Convention 108+, and several emerging national regulations, differences in scope, enforcement, and cooperation continue to hinder global progress toward justice and accountability for individuals whose data is processed. This paper is timely as it examines whether international privacy frameworks are strong enough to ensure fair protection, transparency, and accountability within the global digital economy. It also explores how disparities in legal, cultural, and political contexts, along with the rise of technologies like artificial intelligence and big data, impact global efforts to achieve justice in data management. The paper will be structured as a comparative doctrinal study, and will address the main regulatory instruments and relevant court decisions in order to analyse whether they ensure a substantive and procedural fairness, across the board. It will then attempt to summarise the existing approaches, highlight issues in their application and offer potential solutions in order to set a more equal level of protection of privacy globally. It will ultimately conclude that while privacy is more protected than ever, there are still issues of divergent enforcement and fragmentation, which hinder data development.

Keywords: Data Privacy, Global Regulation, Cross-Border Data, Digital Justice, AI Governance

Introduction

Rising public consciousness, a digital economy driven by technological innovation, and the prevalence of data flows across borders have all contributed to the dynamic nature of data privacy in the international arena. While more than 170 countries have passed data protection regulations, many of which were motivated by the EU's GDPR[1], the current legal system in which data privacy is managed on a global scale is non-uniform and fragmented[2]. This patchwork landscape has major repercussions for corporations, which are expected to comply with various and sometimes incompatible laws and standards while also maintaining their customers' trust.

In the United States, these problems are further exacerbated by a fragmented system of laws that vary from state to state and sector to sector[3]. In Europe, on the other hand, a human rights-based approach to privacy prioritizes individual rights. In nations like China and Russia, on the other hand, the state's ability is emphasized, and privacy is regulated primarily as a national security issue[4]. In nations in Latin America, Asia, and the Middle East, where the economy is expanding, new privacy laws are being put into place, and there is a general trend towards convergence on a global scale[5]. In practice, however, data privacy on an international scale has been unable to overcome inequalities in countries' enforcement capabilities, and there are thus variations in the amount of privacy protection and legal certainty that exists, especially in the event of data export.[6]

Jurisdictional issues, difficulties in holding corporations accountable, and a lack of organized cooperation on an international level are the factors that most weaken data privacy enforcement efforts. Existing legal systems also lack appropriate remedies for victims in cases of data breaches that affect large numbers of people[7]. Technologies, including cloud computing, AI, and the Internet of Things, will also give rise to new concerns[8]. With regard to compliance,

[1] Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World*, Council of Europe (2014)
[2] Ira S. Rubinstein, Global Data Privacy: The EU Way, 38 *Fordham Int'l L.J.* 902, 902–906 (2015).
[3] Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 833–35 (7th ed. 2021)
[4] Graham Greenleaf, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, 169 *Privacy Laws & Business Int'l Rep.* 1, 3–6 (2021)
[5] Christopher Kuner et al., The Rise of Privacy Law in Asia, Latin America, and the Middle East, 9 *Int'l Data Privacy L.* 1, 1–3 (2019).
[6]Jennifer Daskal, Borders and Bits, 71 *Vand. L. Rev.* 179, 184–90 (2018).
[7] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 150–55 (2018).
[8] Lilian Edwards, Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, 2 *Eur. Data Prot. L. Rev.* 28, 28–33 (2016).

transparency, consent, and fair, automated decision-making are all key areas of ambiguity.[9] Although certain instruments, such as bilateral agreements and adequacy decisions, help to fill some of these gaps, the reality is a non-uniform global data privacy system with varying approaches and interpretations of privacy governance[10]. Privacy laws are evolving at a slower, gradual pace as jurisdictions become more cognizant of the fact that any privacy governance should be adaptive, collaborative, and, most importantly, standardized to some extent. The actual system falls short of what would be truly just.[11] Providing individuals with appropriate, non-discriminatory redress, in addition to demanding openness and responsibility from key stakeholders in the digital ecosystem, requires global collaboration and effective and innovative regulation appropriate for the global digital economy of the 21st century.[12]

Statement of the Problem

Worldwide trade in the information economy relies on the free movement of data across borders, but the development of international data privacy regulation, despite the number of data privacy laws, has been both slow and incomplete. Inconsistencies in legal traditions, the lack of effective global cooperation, and the uneven balance of power between private individuals and large private institutions all contribute to the weakness of meaningful privacy rights. In an interconnected digital world economy, one may then ask if it is possible to have a real, fair and non-discriminatory enforcement of protection and accountability within the current state of international data privacy law. The purpose of this paper is to investigate this question.

Research Gap

Despite the widespread use of data privacy laws, there is limited understanding of their effectiveness, particularly across jurisdictions. Fragmented standards and unequal institutional capacities hinder consistent justice in cross-border data flows. Unaddressed privacy risks arise from the outdated nature of the existing legal and regulatory frameworks in light of emerging technologies. Accountability and access to remedies are further weakened by the power imbalances between individuals and global corporations, particularly in developing countries. This highlights the importance of research on global collaboration for fairer justice in data

[9] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *Int'l Data Privacy L.* 76, 76–79 (2017).
[10] GDPR, art. 45–47
[11] Peter Swire & DeBrae Kennedy-Mayo, *U.S. Private-Sector Privacy: Law and Practice for Information Privacy Professionals* 589–91 (3d ed. 2020).
[12] Megan Richardson, *Advanced Introduction to Privacy Law* 110–12 (2020).

privacy governance.

Research Questions

1. What effects do disparities and fragmentation in international data privacy regulations have on the fairness of international data transactions for both individuals and corporations?
2. Are the privacy issues raised by cutting-edge technologies like artificial intelligence and big data analytics adequately covered by the legal frameworks in place now?
3. What effects do socio-political, cultural, and economic distinctions have on the formulation and application of data privacy regulations, as well as how do they affect international justice?
4. How might collaborative enforcement and international treaties harmonize data privacy standards and improve justice?

Research Objectives

1. To analyze the effect of enforcement variation and division of law on cross-border privacy justice.
2. In a bid to assess whether current privacy laws can address the threats posed by developing digital technologies.
3. To explore economic, political, and cultural influences on data privacy laws in a selection of countries.
4. In response to proposing ways to reinforce international cooperation and unify procedures so as to guarantee equitable protection everywhere.

Research Methodology

It analyzes if existing data privacy legislations support justice in international business applying a qualitative, comparative doctrinal analysis. The main aim of the study is to doctrinally compare international legislations, treaties, and court rulings. The regimes most commonly compared are the US sectoral regime, China's PIPL, India's DPDP Act, 2023, and the EU's GDPR. A comparison analysis is applied to understand how the regimes safeguard human rights while moving data across borders.It is assisted in identifying gaps between enforcement, remedial measures, and efficient delivery of justice between jurisdictions with

the comparative approach. Case studies are compared in order to find gaps between theory and practice in the administration of justice. This is supplemented with a qualitative content analysis of official reports, critical commentaries, and regulatory reports to analyze how companies enforce data protection standards. The analysis uses justice, fairness, accountability, and proportionality as evaluative benchmarks in testing the ability of each jurisdiction to deliver procedural and distributive justice.

Literature Review

With globalization and IT transformation, cross-border business data privacy debate has taken a new turn with researchers arguing on applicability of existing laws to deliver justice.[13]

Books

- Solove, Daniel J. (2021), Comprehending Privacy: The foundational framework of Solove presents privacy as a multifaceted concept of autonomy, dignity, and control. He contends that, particularly in international contexts, legal systems frequently provide inconsistent privacy protections.[14]
- Peifer, Karl-Nikolaus & Schwartz, Paul (2020), Transatlantic Data Privacy Relations: This essay examines the conflict between the market-oriented U.S. model and the rights-based EU approach. It demonstrates how divergent ideologies impede consistent justice procedures for data processing across borders.[15]
- Christopher Kuner, "Transnational Data Flows and Data Privacy Law," (2013) According to Kuner, the legal tools currently in use for data transfers are disjointed and fall short of offering comprehensive protection. To close these justice disparities, he supports international harmonization.[16]

Journal Articles

- "Extraterritorial Application of Data Protection Law" by Catherine Donnelly (2019): Donnelly highlights the ongoing enforcement issues while outlining how the extraterritorial application of laws like the GDPR aims to extend justice across

[13] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies* 7–8 (2021)
[14] Daniel J. Solove, *Comprehending Privacy* 32–38 (2021).
[15] Karl-Nikolaus Peifer & Paul Schwartz, *Transatlantic Data Privacy Relations* 15–20 (2020).
[16] Christopher Kuner, *Transnational Data Flows and Data Privacy Law* 95–97 (2013).

borders.[17]

- Graham Greenleaf, "Global Data Privacy Laws 2022": According to Greenleaf's empirical survey, privacy laws are widely distributed throughout the world, but they are not effectively enforced, only offering symbolic rather than substantive justice.[18]
- Samantha Bradshaw and Christopher Millard (2018), "'Contracts for Clouds': This article discusses how effective redress for privacy violations is frequently hampered by contractual and jurisdictional ambiguities in cloud computing.[19]

Reports and Institutional Publications

- **OECD (2021),** ***Enhancing Access to and Sharing of Data***: Insufficiently balanced access to the range of available means of redress for individuals seeking to protect their data as it crosses international borders is a result of imperfectly consistent international laws, as acknowledged by the OECD.[20]
- **UNCTAD (2022),** ***Data Protection Regulations and International Data Flows***: UNCTAD points out that although the majority of nations have privacy laws, justice is not equally distributed throughout the world due to differences in enforcement capabilities.[21]
- **World Economic Forum (2021),** ***Advancing Data Justice in the Global Digital Economy***: This report on a new idea of data justice shows how current legislation isn't enough to protect vulnerable people. It also argues for a better global governance of data. (above is the synchronous summary of WEFs report)[22]

CHAPTER 2 - RELEVANT LAWS, TREATIES, AND INTERNATIONAL RESOLUTIONS ON DATA PRIVACY

A combination of national laws, international agreements, and resolutions aimed at regulating

[17] Catherine Donnelly, *Extraterritorial Application of Data Protection Law*, 70 *Int'l & Comp. L.Q.* 87, 88–90 (2019).
[18] Graham Greenleaf, *Global Data Privacy Laws 2022: Despite COVID Delays, 157 Laws Show GDPR Dominance*, 176 *Privacy Laws & Bus. Int'l Rep.* 10, 11–13 (2022).
[19] Samantha Bradshaw & Christopher Millard, *Contracts for Clouds: Legal Issues in Cloud Computing Agreements*, 26 *Int'l Rev. L. Computers & Tech.* 187, 192–94 (2012).
[20] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies* 28–30 (2021)
[21] UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* 13–15 (2022)
[22] World Econ. F., *Advancing Data Justice in the Global Digital Economy* 4–7 (2021)

cross-border data flows and individual rights in the information economy have shaped the protection of data privacy into a cross-border issue. The flow of personal and business information across borders is becoming increasingly important to international business, so this set of laws provides the framework for holding jurisdictions responsible and fostering equity. However, inconsistent enforcement and unequal protection for data subjects result from national differences in strategy and the lack of a single universal treaty. Understanding these tools is essential to determining whether current legislation is adequate to deliver justice in a situation involving international trade.

1. Global Foundations of the Right to Data Privacy

The United Nations (UN) has played a significant role in establishing privacy as a fundamental human right on a global scale. Articles 12 of the Universal Declaration of Human Rights (UDHR) [23]and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) [24]are reaffirmed in the UN General Assembly and Human Rights Council Resolutions on "The Right to Privacy in the Digital Age" (2013–2023)[25]. These resolutions acknowledge privacy as fundamental to equality, justice, and human dignity and extend traditional privacy protections to digital environments. These resolutions, while not legally binding, have had a significant normative impact because they call on governments to enact efficient oversight, openness, and legal recourse against capricious monitoring and improper use of data. Thus, the UN framework creates the ethical and political framework for modern, cross-jurisdictional data protection laws.

2. Regional and Multilateral Treaties

a. Council of Europe Convention 108 and Convention 108+

The Council of Europe Convention for the Protection of Individuals with respect to Automatic Processing of Personal Data (Convention 108)[26], agreed upon in 1981 and updated as a modern version, Convention 108+, in 2018, is still the sole world-wide legally binding instrument that is solely focused on data protection. Convention 108+ follows the values of lawfulness, fairness, limitation of purpose, data minimization, transparency, and accountability. It also

[23] Universal Declaration of Human Rights art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
[24] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.
[25] G.A. Res. 68/167, *The Right to Privacy in the Digital Age* (Dec. 18, 2013)
[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108.

facilitates cross-state cooperation among supervisory states and permits transfers between states of personal data that are kept in states with comparable standards. By applying non-European states, quasi-global coverage can be achieved, with a bearing on national laws throughout Africa, Asia, and Latin America. In fact, Convention 108+ performs the interstitial role between data rule-making and human-rights law and allows both cross-frontier cooperation and the protection of individuals.

b. Budapest Convention on Cybercrime (2001)

Though a traditional criminal-law treaty, even the Budapest Convention on Cybercrime (2001) [27]also intersects with privacy since cross-frontier access to electronic evidence in the course of cybercrime investigations is regulated thereby. It employs modalities of mutual legal assistance and information exchange between states that have to be set against safeguarding private information and privacy. Its connection to justice is that it tries to balance state security interests with the rights of individuals to privacy, even as continuance tensions between data protection and surveillance powers remain.

3.Comprehensive Framework of the European Union

It is the world's largest and most comprehensive privacy law and took effect in 2018. The GDPR[28] has a significant extraterritorial impact since it applies to all EU citizens as well as non-EU organizations that handle EU citizens' data.

It institutionalizes data-subject rights like access, correction, erasure ("right to be forgotten"), and data portability and puts strict requirements on controllers and processors. International business is most directly impacted with cross-boundary data flows governed under GDPR with consent either where the destination country has an "adequate level of protection" or approved Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) are in effect. Historic CJEU ruling in Schrems II (2020)[29] affirmed substantial similarity of protection and effective recourse by data subjects, invalidating the EU–U.S. Privacy Shield agreement. The

[27] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[29] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems* (Schrems II), ECLI:EU:C:2020:559.

agreement is replaced by the EU–U.S. Data Privacy Framework (2023)[30] that tries to revamp cross-Atlantic data flows under heightened oversight and personal redress programs.

By such instruments, not only citizens' data are protected by the EU, but also the world standard for the protection of privacy and cross-border data justice is set.

4. National Laws Beyond Europe

a. China: Personal Information Protection Law (PIPL), 2021[31]

China's inaugural exhaustive data protection act is the 2021 Personal Information Protection Law (PIPL) of the People's Republic of China. Similar in structure to the GDPR, the PIPL stipulates consent, transparency, and limitation of purpose principles with a mechanism for oversight by the State incorporated into them. Characteristically, the PIPL emphasizes data sovereignty, national security, and localization needs for critical or sensitive data. The PIPL has stringent regulations regarding cross-border transfers that require government approval or security scrutiny. The strategy emphasizes a unique conception of justice based on group governance and security, which is in line with China's emphasis on state-based control rather than individual liberty.

b. India: The 2023 Digital Personal Data Protection Act (DPDP Act)

Data fiduciaries are envisioned by India's Digital Personal Data Protection Act (DPDP Act, 2023)[32], which also grants rights to access, correction, erasure, and redress. Jurisdictions that have been deemed "trusted," or having an active, sovereignty-oriented policy, by the Indian government are allowed to allow cross-border flow.

Although the DPDP Act is a milestone in bringing India to the world standard of privacy, enforcement potential together with regulation detail and public sensitization are the points of concern. The role of justice in the Act is the capability to successfully counter its right to privacy against digital economic growth and sustainability in administration.

[30] U.S. Dep't of Com., *EU–U.S. Data Privacy Framework* (2023)
[31] *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) (China).
[32] *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, INDIA CODE (2023).

5. Asia's Evolving Regional Arrangements

Many Southeast Asian nations have introduced new privacy laws that comply with to international directives.

- Indonesia's Personal Data Protection Act 2022[33]
- Thailand Personal Data Protection Act 2022 (PDPA)[34]
- Sri Lanka Personal Data Protection Act 2022[35]

These laws incorporate cross-border flow controls, accountability principles, and consent-based processing. They are a sign that the region is heading toward more stringent privacy laws and interregional cooperation, even though their implementation is inconsistent.

Healthy data flows across economies with different regimes are facilitated by the voluntary, certification-based Asia-Pacific Economic Cooperation (APEC)[36] Cross-Border Privacy Rules (CBPR) framework at the regional level. The CBPR, which is not a treaty in and of itself, promotes corporate accountability and interoperability while offering a workable substitute for strict regime-of-adequacy strategies such as the GDPR.[37]

6.New Devices and the Data Justice Future

It became a signatory to the Framework Convention on Artificial Intelligence (AI Convention) in 2024 that combined values of protection and privacy of data with human rights and regulation of technologies that are powered by AI. Algorithmic accountability that considers that privacy and fairness are to be applied to processes that are machine learning and automated decision-making is a departure from typical data privacy requirements.

7.Perpetuating Gaps and Implications for Justice

Even with a growing rule and treaty infrastructure, cross-data protection justice across borders is still grossly imbalanced. Due to the heterogeneity of enforcement powers, the discrepancy in the definition of what “adequacy” means, and the limited access to remedial proceedings, individuals are still left with little redress in practice. The extraterritorial application of the

[33] *Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection* (2022).
[34] *Thailand Personal Data Protection Act*, B.E. 2562 (2019) (effective 2022).
[35] *Sri Lanka Personal Data Protection Act*, No. 9 of 2022.
[36] Asia-Pacific Economic Cooperation (APEC), *Cross-Border Privacy Rules (CBPR) System*, APEC Privacy Framework (2015).
[37] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 250–53 (2013).

territoriality of national laws like the GDPR continues to be challenged by states such as China and India on the basis of sovereignty-driven considerations resulting in regulatory fragmentation.

Secondly, enforcement authorities in many developing nations often lack the financial and institutional resources to effectively oversee and regulate the actions of large multinational corporations operating within their borders. Although the global privacy framework is built on strong ethical and legal principles, it remains fragmented in structure, leaving significant gaps where injustices persist in practice.

Taken together, it can be said that UN resolutions, Convention 108+, the GDPR, China's PIPL, India's DPDP Act, the Budapest Convention, the APEC Cross-Border Privacy Rules, and the Framework Convention on AI[38], along with other international instruments, form a fragmented international privacy regime, which, at a minimum, conveys recognition of privacy as a human right (universal) and due process (normative) in the collection and trans-border processing of data; however, the real-world efficacy of such a regime depends on more active institutional collaboration and coordination, mutual recognition of remedies, and mutual accountability by states and corporate bodies.

CHAPTER 3: JUDICIAL PRONOUNCEMENTS AND CASE STUDIES ADDRESSING THE IDEA OF JUSTICE

Judicial decisions provide the practical application of standards enshrined in legislation into workable, enforceable models of justice. Major international decisions demonstrate how legal regimes impact global commercial activities, determine the reach of data protection and attempt to balance the rights of individuals and commercial needs.

1. European Union

Case: Schrems II (2020)[39] The Court of Justice of the European Union (CJEU) struck down the EU–U.S. Privacy Shield on the basis that U.S. surveillance laws provided neither sufficient protection, nor an effective right to judicial redress to EU citizens.

Summary: The decision was grounded in a concept of justice that demanded equal protection of personal data no matter where it was processed. It reinforced the view that privacy is a

[38] Council of Europe, *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law* (May 17, 2024), C.E.T.S. No. 218.
[39] *Case C-311/18, Schrems II*, ECLI:EU:C:2020:559.

fundamental human right and that no matter how it is processed, due process must include both proper oversight and access to an effective remedy.

Impact: The decision forced multinational companies to be more diligent in their cross-border data transfers between the EU and U.S., ensuring that both states and corporations are equally obligated to uphold a universal standard of privacy and due process.

Case: Google Spain (2014)[40] The Court of Justice of the European Union (CJEU) established the "Right to be Forgotten", which gave people the ability to ask search engines to remove links with personal information when it is "inadequate, irrelevant or no longer relevant."

Summary: By protecting the information of individuals from persistent reputational damage and ensuring their ability to control what personal information about them can be seen, the decision served the cause of justice in the digital era.

Significance: The case set a global standard for technology companies to carefully balance the public's right to know with the individual's right to privacy. It also recognized that at its best, justice should empower people with the freedom, choice, autonomy, and dignity to participate in the digital economy.

2. United States

- **Case: FTC v. Facebook (2019)[41]** – This case, along with similar ones, reflects a growing international understanding that achieving justice in data privacy requires both protective measures and active enforcement. However, equality in justice continues to be undermined by inconsistent enforcement and the absence of a unified global standard. For data justice to become a true part of international trade, privacy standards must be harmonized across jurisdictions. The case highlighted the path that justice should take demanding stronger corporate accountability and effective legal remedies for violations.
- **The case Relevance is** The ruling demonstrated the potential for enforcement regulation to provide justice due to the absence of comprehensive laws, enhancing corporate accountability throughout international digital markets.

[40] *Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317.
[41] *Federal Trade Commission v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. 2019).

3. India

- Case: Justice K.S. Puttaswamy v. Union of India (2017)[42]: The Supreme Court of India unanimously ruled that privacy is a constitutional right, and any privacy breach must be legal, necessary, and proportional. Conclusion: The judgment entrenched privacy as a right to dignity and freedom within the Constitution and was the catalyst behind India's DPDP Act (2023). Importance: Puttaswamy obliges each information processing company dealing with information related to Indian citizens to be governed by the values of the Constitution such that the rights of citizens will prevail even over commercial or administrative interests and sets India at par with international standards for human rights.

4. Australia

- Case: ABC v. Lenah Game Meats (2001)[43]: The High Court of Australia was debating whether screening privately recorded videos had violated privacy in the case of ABC v. Lenah Game Meats (2001). The court acknowledged that the law could change and offer protection against harassing public exposure, even though it declined to sanction a traditional tort of privacy. Analysis: The court also acknowledged that in order to ensure justice, the law must change to keep up with emerging technologies. Relevance: It shows that justice is a moral and legal norm that requires businesses to act responsibly and that there can be a sense of ethical obligation even in the absence of statutory implementation.

Together, these cases show a global trend toward the belief that data privacy justice necessitates both protection and corrective measures. Parity in justice is still hampered, however, by differences in enforcement and a lack of a universal global paradigm. To truly implement data justice in cross-border trade, these principles must be standardized.

CHAPTER 4 - A CRITICAL EXAMINATION OF JUDICIAL METHODS FOR INTERNATIONAL DATA PRIVACY JUSTICE

The rapid growth of digital technologies and cross-border data flows has brought privacy and data protection to the center of global legal and ethical discussions. Courts around the world now face increasing pressure to interpret, apply, and, at times, expand data privacy standards

[42] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2017) 10 SCC 1 (India).
[43] *Australian Broadcasting Corp. v. Lenah Game Meats Pty Ltd.*, (2001) 208 CLR 199 (Austl. H.C.).

while balancing individual rights, corporate interests, and state security concerns. This chapter critically examines how the judiciary delivers justice in matters of cross-border data privacy how it recognizes privacy as a right, ensures both substantive and procedural fairness, adapts to technological developments, and navigates the conflicts created by differing legal systems. By reviewing landmark rulings and enforcement methods, the chapter highlights both the progress achieved and the setbacks encountered in the ongoing effort to secure meaningful justice in a globalized, data-driven age.

- Normative Improvement of Privacy: Court affirmations of the right to privacy, such as Puttaswamy and EU case law, reinterpreting it as adherence to a requirement of justice, in connection with human autonomy and dignity. It is also a means to put privacy at the forefront of human rights issues by making governments and businesses accountable to courts to justify any interference under strict standards and by reinforcing the ability of courts to strike down government measures that do not offer protections considered "essentially equivalent".

- Substantive and procedural justice: Justice demands real, effective redress which goes beyond the formalities of legality and substantive parity in protection in light of decisions such as Schrems II. One of the forgotten case law is the right to informational self-determination. An example of enforcement action is the FTC fine against Facebook. Justice is about long-term change in governance, not a small fine.

- Adapting to Technological Change: Privacy law is shifting toward standards for algorithmic accountability and transparency as a result of courts' growing challenges with algorithmic obscurity and persistent web data. Legal safeguards must therefore change to address machine-mediated threats in cross-border situations, which is consistent with new principles of AI governance.

- Long-Term Fragmentation and Contestation Over Sovereignty: Judicial practices involving requirements for consent, monitoring, and information transfers are inconsistent with rights-based, market-based, and sovereignty-first approaches. Legislative extraterritoriality, such as that found in the GDPR, collides with sovereignty-first regimes, causing regulatory friction that makes it harder for corporations to be held accountable and prevents a predictable remedy.

- Enforcement and Remedy Asymmetries: Institutional power has a significant impact on access to justice. Although resourceful DPAs provide cross-border enforcement, power

imbalances are highlighted by the fact that citizens in developing countries lack effective recourse due to capability gaps. Procedural barriers typically amount to restricting redress and deterrence, even in cases where paper rights are in place.

- Private Ordering Limitations: The use of contractual tools like standard contractual clauses (SCCs) shifts too much of the responsibility onto private entities to guard against large-scale risks, such as government electronic surveillance. While courts are right to insist on thorough risk assessments, these measures can only partially improve protection unless they are paired with stronger public law oversight and control.

RECOMMENDATIONS AND CONCLUSION

Recommendations

1. **Harmonize International Law:** Create legally binding global agreements to reduce regulatory uncertainty, encourage multinational corporations to comply, and establish shared standards for data privacy.
2. **Develop Unified Enforcement Systems:** Introduce reciprocal recognition of judicial decisions and coordinated investigations between data protection authorities (DPAs) to strengthen cross-border enforcement and overcome jurisdictional barriers.
3. **Promote Access to Justice:** Use procedural reforms such as class actions and simplified complaint mechanisms to make remedies more accessible, particularly for individuals in developing countries where access to justice remains limited.
4. **Set New Technology Standards:** Incorporate rules that promote privacy by design, accountability, and transparency in emerging technologies such as artificial intelligence, big data, and automated decision-making.
5. **Encourage Multi-Stakeholder Cooperation:** Governments, businesses, and civil society organizations must work together to create transparent governance frameworks that strike a careful balance between fostering innovation and safeguarding privacy.

Conclusion

The global data protection framework has made significant progress in promoting the right to privacy within international trade. Through case law, the GDPR, and other related directives, privacy has been recognized as a fundamental human right, and greater responsibility has been placed on corporations. However, persistent jurisdictional fragmentation, uneven enforcement, and the rapid pace of technological innovation often outpacing the capacity of regulators have

hindered the consistent application of justice. In many developing countries, power imbalances between individuals and large corporations further restrict access to effective legal remedies. Despite efforts toward standardization, the creation of a single, universal global data privacy system remains unrealistic, making uniform protection impossible. True data justice can only be accomplished through sustained international collaboration and the continuous development of adaptable legal frameworks that balance privacy rights with evolving commercial and social needs.

REFERENCES

1. Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World*, Council of Europe (2014)
2. Ira S. Rubinstein, Global Data Privacy: The EU Way, 38 *Fordham Int'l L.J.* 902, 902–906 (2015).
3. Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 833–35 (7th ed. 2021)
4. Graham Greenleaf, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, 169 *Privacy Laws & Business Int'l Rep.* 1, 3–6 (2021)
5. Christopher Kuner et al., The Rise of Privacy Law in Asia, Latin America, and the Middle East, 9 *Int'l Data Privacy L.* 1, 1–3 (2019).
6. Jennifer Daskal, Borders and Bits, 71 *Vand. L. Rev.* 179, 184–90 (2018).
7. Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 150–55 (2018).
8. Lilian Edwards, Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, 2 *Eur. Data Prot. L. Rev.* 28, 28–33 (2016).
9. andra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *Int'l Data Privacy L.* 76, 76–79 (2017).
10. GDPR, art. 45–47
11. Peter Swire & DeBrae Kennedy-Mayo, *U.S. Private-Sector Privacy: Law and Practice for Information Privacy Professionals* 589–91 (3d ed. 2020).
12. Megan Richardson, *Advanced Introduction to Privacy Law* 110–12 (2020)
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
14. Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems* (Schrems II), ECLI:EU:C:2020:559.
15. U.S. Dep't of Com., *EU–U.S. Data Privacy Framework* (2023)
16. *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) (China).

17. Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Nw. J. Tech. & Intell. Prop.* 239, 250–53 (2013).
18. Council of Europe, *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law* (May 17, 2024), C.E.T.S. No. 218.