XPLORE PUBLICATIONS
www.xplorepublications.com

IJCLR

Chapter 36

RIGHT TO PRIVACY AND THE ROLE OF PRIVATE ENTITIES AS INTERMEDIARIES Jaina Vora

In: *DSGE 2026 | University of Mumbai (Department of LAW) | IFIM College | Book of Abstract*. IJCLR. ISBN: 978-81-992602-2-0.

RIGHT TO PRIVACY AND THE ROLE OF PRIVATE ENTITIES AS INTERMEDIARIES

AUTHOR

Jaina Vora

BBA.LL.B[HONS] 1st year,

Saveetha School Of Law

Saveetha Institute of Medical And Technical Science

[SIMATS]

Chennai-600077

CO-AUTHOR

Juhi Bhutoria

B.COM.LL.B[HONS] 1st year,

Saveetha School Of Law

Saveetha Institute of Medical And Technical Science

[SIMATS]

Chennai-600077

RIGHT TO PRIVACY AND THE ROLE OF PRIVATE ENTITIES AS INTERMEDIARIES

Jaina Vora[1]

Juhi Bhutoria[2]

ABSTRACT

In the digital age, the right to privacy has become one of the most contested legal and ethical issues, especially considering the significant role that private entities play in managing personal data. In India, the Supreme Court's decision in K.S. Puttaswamy v. Union of India (2017) affirmed privacy as a fundamental right, which has further amplified discussions on privacy protection in the digital age. This paper explores the role of private entities in safeguarding the right to privacy and their legal and ethical responsibilities within India's evolving data protection landscape. The paper examines the role of social media platforms, e-commerce businesses, and cloud service providers in protecting user data, highlighting challenges related to data breaches, consent, and security. It also evaluates the implications of global frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), discussing their influence on Indian legal practices and private entities' obligations. Focusing on real-world case studies, including the Facebook-Cambridge Analytica scandal, the paper critically assesses the ethical and accountability issues surrounding private companies and their data handling practices. It also explores the complexities of cross-border data transfers and the protection of user privacy, especially in light of global data flow regulations. The role of artificial intelligence and big data in shaping privacy practices is examined, considering how private entities use personal data for commercial purposes, sometimes infringing on privacy rights. By providing an analysis of current legal frameworks, ethical challenges, and global precedents, this paper contributes to the ongoing discourse on privacy rights, data protection, and the responsibilities of private entities in balancing innovation with user protection in the digital age.

KEYWORDS: Right to Privacy, Data Protection, Private Entities, Accountability, Ethical Responsibility, India's Digital Ecosystem.

INTRODUCTION

The right to privacy has evolved significantly over time, transforming from a personal notion to a comprehensive legal and constitutional safeguard. In India, the concept was first articulated in cases like *Kharak Singh v. State of Uttar Pradesh*[3], where the Supreme Court recognized aspects of privacy under Article 21 of the Constitution. However, it was the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[4] that unequivocally established privacy as a fundamental right. Globally, privacy is enshrined in documents such as the Universal Declaration of Human Rights (Article 12)[5] and the General Data Protection Regulation (GDPR) of the European Union, which serves as a gold standard for data protection in the digital age.[6]

Recognizing the importance of privacy in a digital society, the Indian government has introduced several measures to protect personal data. The Digital Personal Data Protection Act, 2023, is a key legislative milestone, providing a framework for regulating data collection, processing, and sharing while ensuring individual consent.[7] The Aadhaar Act and its judicial scrutiny in *Justice K.S. Puttaswamy v. Union of India* highlighted the balance between privacy and public welfare.[8] Additional initiatives, such as the National Cyber Security Policy and the establishment of CERT-In, reflect the government's efforts to bolster digital trust and security.[9]

Several factors influence the protection of privacy in the digital era, particularly concerning private intermediaries. A key issue is data monetization, as many business models rely on collecting and using personal data for targeted advertising, raising concerns about informed consent, transparency, and potential misuse[10]. Cross-border data transfers further complicate privacy protection, as differing legal standards across jurisdictions create enforcement challenges and regulatory inconsistencies, especially when stringent frameworks like the EU's GDPR intersect with more lenient laws elsewhere[11]. Technological advancements, including artificial intelligence, machine learning, and big data analytics, have intensified concerns about profiling, surveillance, and algorithmic biases, which can disproportionately harm vulnerable groups[12]. Compounding these issues is the absence of uniform global privacy standards, leading to fragmented compliance obligations for intermediaries operating across multiple regions. This regulatory patchwork not only increases compliance burdens but also exposes users in jurisdictions with weaker protections to greater risks, highlighting the need for coordinated international efforts to address these challenges effectively.

India's approach to privacy is still evolving compared to global benchmarks. The European Union's GDPR emphasizes user rights, data minimization, and accountability, setting a high standard for data protection.[13] In contrast, the United States adopts a sectoral approach with laws like the Health Insurance Portability and Accountability Act (HIPAA) and state-level frameworks like the California Consumer Privacy Act (CCPA).[14] Countries such as South Korea and Japan have embraced hybrid models, aligning domestic laws with international principles.[15]

India's privacy framework is at a pivotal stage, aiming to strike a balance between safeguarding individual rights and fostering a thriving digital economy. The role of private intermediaries in navigating these challenges is critical. This research explores how India can strengthen its privacy framework by learning from international best practices while addressing its unique socio-economic and legal challenges.

FOCUS ON A SPECIFIC SECTOR OF PRIVATE ENTITIES

1. Social Media Platforms as Intermediaries

Social media platforms such as Facebook, Instagram, and Twitter are pivotal intermediaries that not only facilitate communication but also collect and process vast amounts of user data. This includes sensitive personal information like user preferences, behavior patterns, and location data, making them central to privacy discussions. A significant aspect of research here involves their legal obligations to protect user data, ensure transparency, and obtain informed consent. The platforms' practices of algorithmic profiling and targeted advertising, often involving data sharing with third parties, raise serious privacy concerns. Additionally, the role of social media platforms in content moderation—balancing privacy with free speech—is crucial, especially in cases of hate speech, misinformation, or state surveillance. The Cambridge Analytica scandal serves as a case study to analyze the platforms' accountability and compliance with privacy laws, highlighting the need for stricter regulatory frameworks and enforcement.[16]

2. E-Commerce Platforms in Protecting User Data

E-commerce platforms like Amazon, Flipkart, and eBay collect and process personal and financial data from users, such as payment information, contact details, and shopping preferences. This makes them particularly vulnerable to data breaches, unauthorized access, and misuse. The focus of doctrinal research here can include how these platforms adhere to legal standards, such as implementing robust security measures, encryption, and ensuring informed consent. Key issues include transparency in privacy policies, the risks of personalized marketing, and liability for breaches. Excessive data collection by e-commerce platforms also raises concerns about compliance with the principle of data minimization.[17] Recent cases of data breaches have exposed the inadequacy of existing safeguards and the need for enhanced regulatory mechanisms. Research could also analyze consumer redress mechanisms and the role of legal doctrines in holding these platforms accountable.[18]

3. Cloud Service Providers in Safeguarding Personal Information

Cloud service providers like Google Cloud, AWS, and Microsoft Azure play a critical role in storing and processing sensitive personal and corporate data. Their responsibility extends beyond storage to ensuring data security through encryption and protection against breaches or unauthorized access. Doctrinal research could explore their compliance with data localization laws, cross-border data transfer regulations, and encryption standards. Challenges arise when jurisdictional conflicts occur, especially when governments demand access to data stored on foreign servers.[19] Another area of focus could be their liability in cases of data breaches or ransomware attacks, where the legal frameworks governing their responsibilities are often ambiguous.[20] The case of Microsoft Corp. v. United States (2018), where the Supreme Court addressed cross-border data access, provides a landmark example of these challenges.[21] Research could also investigate the role of cloud providers in balancing data protection obligations with their operational and commercial interests.

ROLE OF PRIVATE ENTITIES AS INTERMEDIARIES IN INDIA

Indian Digital Ecosystem

India’s digital ecosystem has seen rapid growth in recent years, with significant advancements in internet access, mobile technology, e-commerce, and social media platforms. With the rise of digital transactions, communication platforms like WhatsApp, Facebook, and Twitter, as well as e-commerce platforms like Amazon and Flipkart, private entities have become pivotal in the collection, processing, and storage of personal data. These intermediaries handle massive amounts of user information, such as location data, payment details, and browsing behavior, which are essential to their operations. The Indian government’s push for initiatives like Digital India has further expanded this ecosystem, but it has also raised significant concerns regarding data security, privacy, and the regulatory frameworks governing these entities. Despite these advancements, the lack of a comprehensive and enforceable data protection law remains a critical issue, leaving individuals vulnerable to misuse of their data by private companies.[22]

Privacy Concerns in Intermediaries

The role of private entities as intermediaries in India, especially in handling personal data, has raised significant privacy concerns. Social media platforms, e-commerce websites, and other digital service providers gather vast amounts of sensitive information, making them susceptible to data breaches, unauthorized access, and misuse. The absence of robust privacy regulations allows companies to potentially exploit personal data for commercial gain, such as through targeted advertising and personalized content, often without users' explicit or informed consent. Moreover, intermediaries are often seen as facilitators of privacy violations, especially when they allow third-party access to user data without adequate protection measures. In addition to this, issues such as data retention practices, cross-border data flows, and the ease with which data can be accessed by governmental and private entities exacerbate privacy concerns. The Puttaswamy judgment, which recognized the right to privacy as a fundamental right under Article 21 of the Indian Constitution, underscored the need for safeguarding personal data and regulating the role of intermediaries in the digital space.[23]

Personal Data Protection Bill, 2011

The Personal Data Protection Bill, 2011 was one of the earliest attempts by the Indian government to address the growing concerns around privacy in the digital age. The Bill sought to regulate how both government and private entities collect, process, store, and share personal data. It proposed strict requirements for obtaining informed consent from individuals, ensuring data transparency, and implementing data protection measures like encryption. However, the Bill did not address the accountability of intermediaries effectively and failed to introduce enforceable penalties for data breaches. Moreover, the lack of provisions for cross-border data flows raised concerns about the protection of Indian citizens' data outside the country. The Bill, despite being a starting point, faced criticisms from privacy advocates for not providing sufficient protection for individual privacy and leaving too much discretion to the government and private entities. It was eventually replaced by the Personal Data Protection Bill, 2019, which addressed many of these shortcomings.[24]

Digital Personal Data Protection Act (DPDP), 2023

The Digital Personal Data Protection Act (DPDP), 2023, marks a significant step forward in the regulation of personal data protection in India. The Act aims to protect individuals' privacy by regulating the collection, processing, and storage of personal data by private entities and public bodies. It emphasizes the need for obtaining explicit consent from individuals before collecting their data and mandates the implementation of appropriate security measures by data processors. One of the key features of the DPDP Act is the establishment of a Data Protection Board to adjudicate grievances and impose penalties on entities that fail to comply with its provisions. The Act also introduces provisions for the processing of data in the public interest, such as for law enforcement, while ensuring that privacy rights are not unduly compromised. In terms of intermediaries, the DPDP Act holds companies accountable for the protection of data and mandates transparency in how personal data is collected, used, and shared. It further strengthens provisions for cross-border data transfers, ensuring that data protection standards are maintained even when personal data is stored or processed abroad. While the DPDP Act is a step toward strengthening privacy protections in India, questions remain about its effectiveness in enforcement and its potential impact on the operations of private entities.[25]

Transparency and Informed Consent

A critical issue in India's digital ecosystem is the transparency with which private intermediaries operate and the extent to which they inform users about the data they collect. In many cases, platforms' privacy policies are long, complex, and written in legalese, making it difficult for users to fully understand what they are agreeing to. This lack of clear and accessible information undermines the principle of informed consent, which is a cornerstone of data protection law.

Intermediaries often bury important details about data-sharing practices or fail to adequately inform users about how their data will be used beyond the primary service. For example, data may be shared with third-party advertisers or sold to other companies for further analysis. The absence of informed consent can lead to users unknowingly consenting to the extensive use of their data for purposes they might not approve of. In this context, intermediaries are not just service providers but also significant influencers of the user's privacy rights.[26]

Case Law: K.S. Puttaswamy v. Union of India (2017)

The landmark case of K.S. Puttaswamy v. Union of India (2017) fundamentally changed the legal landscape regarding privacy rights in India. In this case, the Indian Supreme Court declared the right to privacy to be a fundamental right under Article 21 of the Indian Constitution, affirming that privacy is intrinsic to the right to life and personal liberty. The Court highlighted the need for privacy protection in an era where personal data is increasingly collected, processed, and shared by both state and private entities.

The Puttaswamy case also provided a framework for balancing the right to privacy with other competing interests, such as national security and public order. It emphasized that any interference with the right to privacy must be in accordance with the law, pursue a legitimate aim, and be proportionate in nature. The implications of this ruling for private entities in India are profound, as it mandates that these companies respect the privacy of their users and ensure that their data handling practices are lawful, transparent, and accountable.

The Puttaswamy ruling also laid the foundation for the Personal Data Protection Bill (PDPB), 2019, which seeks to regulate how personal data is handled by private entities in India. The decision underscores the need for a robust legal framework to protect citizens' privacy in the face of increasing data collection and digital surveillance by private companies.[27]

Case Law: Shreya Singhal v. Union of India (2015)

The Shreya Singhal case (2015) is another significant case related to the responsibilities of private entities in India. Although the case focused primarily on the validity of Section 66A of the Information Technology Act, 2000 (which dealt with offensive online content), it raised key issues concerning the accountability of intermediaries such as social media platforms.

The Supreme Court struck down Section 66A, declaring it unconstitutional due to its overreach and the chilling effect it had on free speech. However, the Court also emphasized the responsibility of intermediaries to act reasonably when it comes to regulating content and handling user data. This judgment has implications for private entities, as it highlights their role in ensuring that the data shared by users is not exploited for malicious purposes, including the spread of misinformation or political

manipulation.[28]

Case Law: Google India Private Ltd vs M/s Visakha Industries (2019)

In 2008, defamatory articles were posted on a Google Group that accused Visakha Industries, an asbestos cement sheet manufacturer, of corruption. Visakha Industries sent a takedown notice to Google India and filed a criminal defamation case against them.

Google India argued that it was an intermediary and should be protected under Section 79 of the Information Technology Act. However, the Supreme Court ruled that Google India could not claim exemption from liability as they failed to remove the defamatory content despite receiving a notice. The court held that an intermediary capable of removing content and refusing to do so could be considered a publisher.

This case highlights the complex issue of intermediary liability and the balance between freedom of speech and the right to reputation. It emphasizes that while intermediaries have certain protections, they also have a responsibility to take reasonable steps to prevent the misuse of their platforms.

*The Visakha Industries case has significant implications for the right to privacy and the role of private entities as intermediaries***.**

Right to Privacy: The case highlights the potential for online platforms to be used to disseminate false and harmful information, which can infringe on an individual's right to privacy and reputation. The Supreme Court's ruling underscores the importance of intermediaries taking proactive steps to protect users' privacy and prevent the spread of misinformation.

Role of Private Entities as Intermediaries: The case clarified the role of private entities as intermediaries. It established that while intermediaries have certain protections, they cannot be passive bystanders. They have a responsibility to take reasonable steps to prevent the misuse of their platforms. This includes removing harmful content upon receiving notice, implementing effective content moderation policies, and cooperating with law enforcement when necessary.

In essence, the Visakha Industries case emphasizes the delicate balance between freedom of speech and the protection of individual rights. It underscores the need for a robust legal framework that holds intermediaries accountable while safeguarding fundamental rights.[29]

EXAMINE SPECIFIC PRIVACY LAWS OR REGULATIONS

General Data Protection Regulation (GDPR): A Global Benchmark

The GDPR, which came into effect on May 25, 2018, represents the gold standard for data protection. Article 83 of the GDPR outlines stringent penalties for non-compliance, emphasizing the importance of transparency, accountability, and user control in data processing. Companies can face fines of up to €20 million or 4% of global annual turnover for severe breaches, such as failing to secure consent for data processing or violating data subject rights.

Private entities, particularly intermediaries like social media platforms and cloud providers, must implement measures to protect personal data. This includes obtaining explicit consent, conducting data protection impact assessments, and notifying regulators of breaches within 72 hours. Moreover, cross-border data transfers are tightly regulated, requiring mechanisms such as Standard Contractual Clauses (SCCs) or adequacy agreements to ensure equivalent protection standards.[30]

California Consumer Privacy Act (CCPA): Empowering U.S. Consumers

The CCPA, effective January 1, 2020, is a landmark U.S. legislation granting California residents greater control over their personal data. The law mandates businesses to disclose the types of personal data collected, the purposes for collection, and details of third-party sharing. Consumers also have the right to opt out of data sales and request data deletion.

Businesses must implement robust compliance frameworks, including user-friendly systems to manage consumer requests, such as “Do Not Sell My Personal Information” links on websites. Penalties for non-compliance, enforced by the California Attorney General, can reach $7,500 per intentional violation. Unlike the GDPR, the CCPA targets businesses meeting specific revenue or data-processing thresholds, creating a more targeted regulatory scope.[31]

Personal Information Protection and Electronic Documents Act (PIPEDA): A Canadian Framework

PIPEDA governs the use, collection, and disclosure of personal information in commercial activities across Canada. The Act requires businesses to obtain meaningful consent for data collection and ensures individuals have the right to access and correct their data.

The Office of the Privacy Commissioner (OPC) oversees PIPEDA compliance, providing guidelines for businesses on implementing strong privacy practices. Security safeguards must be proportional to the sensitivity of the data, and organizations are accountable for the information under their control, even when shared with third-party processors. Non-compliance can lead to OPC investigations and reputational damage for businesses.[32]

Proposed American Privacy Rights Act (APRA): Towards a National Standard

The fragmented state of privacy regulations in the United States has led to calls for a federal framework, culminating in the proposed American Privacy Rights Act (APRA). Introduced in 2024, APRA aims to harmonize privacy protections across states, addressing inconsistencies arising from laws like the CCPA and Virginia Consumer Data Protection Act (VCDPA).

APRA would create uniform rights for consumers, such as data access, deletion, and portability, while imposing strict obligations on businesses regarding data processing and sharing. It proposes a national enforcement agency, strengthening oversight and ensuring compliance with the evolving digital landscape. This legislation signifies a major step toward aligning the U.S. with global privacy standards, such as the GDPR.[33]

China's Data Security Law (DSL) and Personal Information Protection Law (PIPL): Implications for Private Intermediaries

China's Data Security Law (DSL)[34] and Personal Information Protection Law (PIPL)[35] represent a comprehensive regulatory framework aimed at enhancing data governance while balancing national security interests with individual privacy rights. The DSL, effective since September 1, 2021, establishes strict requirements for data classification, storage, and cross-border transfers, particularly concerning critical data in sectors like finance, healthcare, and energy. Private intermediaries, including technology companies, e-commerce platforms, and data processors, are obligated to conduct regular risk assessments, ensure data localization, and obtain government approval for cross-border data transfers unless specific exemptions are granted. Violations of the DSL can result in severe penalties, including fines, license suspensions, and even criminal liability. The PIPL, effective November 1, 2021, mirrors the GDPR's approach by emphasizing individual rights to personal data, requiring private intermediaries to obtain explicit consent, providing clear data processing notices, and facilitating individuals' rights to access, correct, and delete their data. Cross-border data transfers are heavily regulated under the PIPL, requiring compliance with government assessments, standard contractual clauses, or certification. Private intermediaries are further mandated to designate data protection officers and establish internal compliance mechanisms, leading to increased operational burdens and compliance costs. Non-compliance with both laws can result in substantial fines, reaching up to 50 million yuan or 5% of the previous year's revenue under the PIPL. Together, these laws impose stringent obligations on private intermediaries, emphasizing their role as key actors in ensuring data protection and compliance, particularly in the context of global data flows. **EXPLORE EMERGING TECHNOLOGIES**

The rise of emerging technologies such as artificial intelligence (AI), big data analytics, the Internet of Things (IoT), and blockchain has transformed the landscape of data collection, processing, and storage. These technologies have expanded the capabilities of private entities as intermediaries, enabling them to process vast amounts of personal data in ways that were previously unimaginable. However, they have also raised significant challenges in terms of privacy protection, accountability, and ethical responsibility.

Artificial Intelligence and Data Privacy

AI-driven algorithms, machine learning, and predictive analytics have become central to how private entities process and interpret personal data. These technologies can enhance personalized services, improve efficiency, and enable automated decision-making. However, they also raise concerns about bias, discrimination, and privacy violations. Private intermediaries leveraging AI are often unable to ensure full transparency regarding how data is collected, processed, and used. The opaque nature of AI systems can lead to unintended consequences, such as profiling, targeted advertising, or algorithmic discrimination, raising questions about the accountability of intermediaries under privacy laws like the GDPR[36] and CCPA[37].

For instance, under the GDPR, companies must conduct data protection impact assessments (DPIAs) to assess the risks of AI-based data processing activities and mitigate those risks. Similarly, the CCPA requires businesses to provide consumers with access to information about automated decision-making processes, giving individuals control over their personal data. Intermediaries must ensure that AI-driven data practices comply with these regulatory requirements to avoid penalties.

Internet of Things (IoT) and Privacy Challenges

The proliferation of IoT devices, such as smart home assistants, connected cars, wearables, and smart health devices, has further expanded the data collection capabilities of private intermediaries. IoT generates vast amounts of personal data, often collected without the user's explicit consent or full understanding of how their data is being processed and shared. The sheer volume and variety of data collected by IoT devices complicate data governance frameworks and heighten privacy risks, particularly when sensitive data such as health, location, or financial information is involved.

Regulations like the PIPL[38] and GDPR[39] impose strict requirements on IoT intermediaries, mandating transparency about data collection practices, data security measures, and the purposes for which data is used. Intermediaries must ensure data is processed with security safeguards proportionate to the sensitivity of the data, and must obtain consent from users for data collection and sharing. Moreover, under the CCPA[40], businesses are required to offer consumers control over their IoT-related data, such as the right to access, delete, and opt out of data sales.

Blockchain and Privacy in Decentralized Environments

Blockchain, with its decentralized and distributed nature, introduces both opportunities and challenges for data privacy. Private intermediaries increasingly utilize blockchain technology to enhance transparency, data integrity, and security. Blockchain's immutability and decentralized ledger systems ensure that data cannot be easily altered or tampered with, which can foster trust in data handling practices.

However, blockchain's transparency also raises concerns regarding privacy, especially in scenarios involving sensitive personal data. Intermediaries operating in blockchain ecosystems must comply with privacy regulations such as the GDPR, which mandates that personal data be processed lawfully, fairly, and transparently. The PIPL imposes additional requirements for data localization, restricting cross-border data flows and ensuring that blockchain-based data is handled in a manner compliant with Chinese standards.

Private intermediaries using blockchain must address challenges related to pseudonymization, data minimization, and user consent. These principles are crucial to ensure that while data is transparent and immutable, individuals still have control over their personal information. **CASE STUDY APPROACH**

Flipkart Data Breach (2018)

In 2018, e-commerce giant Flipkart experienced a significant data breach that exposed millions of users' personal and financial information. The breach, which was allegedly caused by vulnerabilities in Flipkart's database, raised serious concerns about the platform's data security practices. As one of the largest e-commerce companies in India, Flipkart holds vast amounts of sensitive customer data, including payment details, addresses, and browsing habits. The breach prompted public backlash and legal scrutiny, highlighting the need for stricter data protection measures for e-commerce platforms. The case underlined the vulnerability of private entities handling personal data and the necessity for compliance with privacy regulations to safeguard users' rights. It also sparked debates about the effectiveness of India's existing data protection laws and the urgent need for comprehensive legislation, such as the Personal Data Protection Bill, to ensure user privacy. This case demonstrated that e-commerce platforms must adopt stringent security measures and transparency in how they collect, store,

and process personal data.[41]

Amazon Web Services (AWS) Data Localization Debate

The issue of data localization has been a significant challenge for cloud service providers in India. In particular, Amazon Web Services (AWS), a leading global cloud service provider, faced pressure from the Indian government and privacy advocates over its data storage practices. India has been pushing for data localization, which requires companies to store Indian users' data within the country's borders to ensure better data security and privacy protection. AWS, like many other cloud providers, traditionally stored data across multiple global data centers, raising concerns over the protection of Indian citizens' personal data when it was transferred and stored outside India. The debate culminated in regulatory pressures for AWS to build more local data centers and comply with India's privacy expectations. This case study illustrates the ongoing conflict between global business operations and local regulatory frameworks aimed at ensuring data sovereignty. The legal and privacy concerns related to cross-border data flows emphasize the importance of creating clear, enforceable laws for cloud service providers, balancing international business practices with national privacy concerns.[42]

WhatsApp Privacy Policy Changes (2021)

In 2021, WhatsApp, a leading social media platform owned by Facebook, faced a backlash in India following changes to its privacy policy. The updated policy proposed sharing more user data with its parent company, Facebook, including information about transactions and user behavior on the platform. This move raised concerns among users and privacy advocates, who feared it would infringe on their right to privacy. In India, where WhatsApp is a dominant communication platform, the update sparked widespread protests, with users and regulatory bodies questioning the company's handling of personal data. The Indian government also intervened, demanding clarification and asserting that the changes violated users' privacy rights. The controversy resulted in WhatsApp delaying the enforcement of the policy and prompted broader discussions on the role of private entities in protecting user privacy. This case serves as an example of how social media platforms, as intermediaries, are often at the center of the tension between data-driven business models and individuals' privacy rights. It underscores the need for stronger data protection frameworks to ensure that platforms prioritize user consent and transparency in their data handling practices.[43]

Facebook-Cambridge Analytica Scandal

The Facebook-Cambridge Analytica scandal emerged in 2018 as one of the most significant data privacy controversies of the digital age. The scandal involved the unauthorized collection and use of personal data from over 87 million Facebook users worldwide, including a substantial number from India, by the political consulting firm Cambridge Analytica. The data was allegedly exploited to influence voter behavior in political campaigns, including the 2016 U.S. presidential election and the Brexit referendum.

For Indian users, this scandal raised serious concerns about how private intermediaries like Facebook handle personal data and ensure its security. It exposed gaps in user consent mechanisms, as the data was collected through a third-party app disguised as a personality quiz, which also harvested data from users' friends without their knowledge. This breach highlighted the lack of transparency and

accountability among global tech giants operating in India, where Facebook has a massive user base.

The incident intensified demands for stronger data protection laws in India, leading to the introduction of stricter provisions in the Personal Data Protection Bill, 2019, and subsequently the Digital Personal Data Protection Act, 2023. It also brought attention to the importance of explicit user consent, stringent oversight on data-sharing practices, and the responsibility of intermediaries to prevent unauthorized access and misuse of personal data.[44]

FINDINGS

Erosion of Privacy Rights

Research consistently highlights that the rise of digital technologies has significantly eroded individual privacy rights. The pervasive data collection practices employed by private entities often occur without users' full understanding or consent. Many individuals unknowingly agree to extensive data collection through complex and lengthy terms of service agreements, which are rarely read in detail. This phenomenon raises critical questions about informed consent and the ethical implications of data practices, as users may not be aware of the extent to which their personal information is being collected, analyzed, and shared. The erosion of privacy rights is not just a legal issue; it reflects a broader societal challenge in balancing technological advancement with individual autonomy and dignity.

Inadequate Regulatory Frameworks

The findings indicate that existing legal frameworks are often insufficient to protect privacy in the context of private entities. Many privacy laws are outdated and fail to keep pace with the rapid evolution of technology and data practices. For instance, regulations that were designed for a pre-digital age may not adequately address the complexities of data sharing and processing in today's interconnected world. This inadequacy leaves individuals vulnerable to privacy violations and exploitation, as there are often limited legal recourses available for those whose rights have been infringed. The need for comprehensive and adaptive regulatory frameworks that can respond to technological advancements is a recurring theme in the literature.

Role of Trust

Trust is identified as a critical factor in the relationship between individuals and private entities. Research shows that users are more likely to share personal information with companies they trust, which underscores the importance of transparency and ethical data practices. When companies are open about their data collection methods and demonstrate a commitment to protecting user privacy, they can foster a sense of trust that encourages users to engage more freely. Conversely, a lack of transparency can lead to skepticism and reluctance to share information, ultimately hindering the potential for beneficial interactions between users and companies. This finding emphasizes the need for private entities to prioritize building and maintaining trust through ethical practices.

Impact on Vulnerable Populations

Studies frequently reveal that marginalized and vulnerable populations are disproportionately affected by privacy violations. These groups often lack the resources, knowledge, or access to legal support

necessary to protect their privacy effectively. As a result, they may be more susceptible to exploitation by private entities that engage in aggressive data collection practices. The implications of this disparity are profound, as privacy violations can exacerbate existing inequalities and further marginalize these populations. Research highlights the importance of developing targeted strategies to protect the privacy rights of vulnerable groups, ensuring that they are not left behind in the digital age.

Corporate Responsibility and Accountability

The findings emphasize the need for private entities to adopt a more responsible approach to data management. This includes implementing robust data protection measures and being held accountable for breaches or misuse of personal information. Companies are increasingly expected to act as stewards of the data they collect, prioritizing user privacy and security. Research suggests that establishing clear accountability mechanisms, such as regular audits and transparent reporting practices, can help ensure that companies adhere to ethical standards and legal requirements. This shift towards corporate responsibility is essential for rebuilding trust and protecting individual privacy rights.

Public Awareness and Education

Research indicates a significant gap in public awareness regarding privacy rights and data practices. Many individuals are unaware of how their data is collected, used, and shared, which underscores the need for better education and resources. Increasing public awareness about privacy rights can empower individuals to make informed decisions about their data and advocate for their rights. Educational initiatives that focus on digital literacy and privacy awareness can play a crucial role in equipping individuals with the knowledge they need to navigate the complexities of the digital landscape.

Technological Solutions

Some studies explore the potential of technological solutions, such as encryption and decentralized data storage, to enhance privacy. These technologies can empower individuals to have greater control over their personal information by providing tools that protect data from unauthorized access and misuse. For instance, encryption can safeguard sensitive information during transmission, while decentralized storage solutions can reduce reliance on centralized entities that may mishandle data. However, the implementation of these technologies also raises questions about accessibility and usability, as not all individuals may have the technical expertise to utilize them effectively.

Ethical Considerations

Ethical considerations surrounding data collection and usage are frequently discussed in the literature. Research highlights the moral obligations of private entities to prioritize user privacy and the ethical implications of surveillance practices. The increasing normalization of surveillance technologies raises important questions about consent, autonomy, and the potential for abuse. Ethical frameworks that guide data practices can help ensure that companies operate in a manner that respects individual rights and promotes social good. This focus on ethics is essential for fostering a culture of accountability and responsibility in the digital age.

Global Perspectives

Comparative studies often reveal significant differences in privacy protections across countries. Research shows that cultural, legal, and political contexts shape how privacy is understood and protected, leading to varied outcomes for individuals. For example, some countries have robust privacy laws that prioritize individual rights, while others may have more permissive frameworks that allow for extensive data collection. Understanding these global dynamics is crucial for developing effective privacy protections that can be adapted to different contexts. The variations in privacy regulations highlight the need for international cooperation and dialogue to establish best practices and harmonize standards that protect individuals' privacy rights globally.

Future Directions for Research

Many papers conclude with calls for further research into emerging technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), and their implications for privacy. As these technologies continue to evolve, they present new challenges and opportunities for privacy protection. There is a pressing need for interdisciplinary approaches that combine legal, technological, and social perspectives to address the complexities of privacy in the digital age. Future research should focus on understanding the long-term impacts of these technologies on individual privacy rights and exploring innovative solutions that can enhance privacy protections while fostering technological advancement.

LIMITATION

Its doctrinal based research on Right to Privacy and the Role of Private Entities as Intermediaries, is limited by the absence of uniform legal definitions and frameworks across jurisdictions, making it challenging to develop universally applicable conclusions. The evolving nature of privacy jurisprudence often lags behind technological advancements, leaving gaps in addressing emerging issues like AI or data-driven technologies. Ambiguities in defining the exact role and responsibilities of intermediaries further complicate the analysis, especially when privacy rights conflict with other interests like security or free expression. Additionally, over-reliance on judicial precedents and limited access to private entities’ opaque policies constrain a comprehensive understanding of the topic.

SUGGESTIONS

To enhance privacy protection in India, it is essential to establish a comprehensive and enforceable data protection law that addresses the unique challenges posed by the digital landscape. This law should incorporate principles of accountability, transparency, and user empowerment, ensuring that private entities are held responsible for safeguarding personal data.

Comprehensive Data Protection Legislation should be enacted to provide a clear framework for data collection, processing, and storage. This legislation must define the rights of individuals regarding their personal data and outline the obligations of private entities in handling such data. It should also include provisions for penalties and enforcement mechanisms to ensure compliance.

User Empowerment Initiatives should be implemented to educate individuals about their privacy rights and the importance of data protection. Public awareness campaigns can help users understand how their data is collected, used, and shared, enabling them to make informed choices about their online activities. This empowerment can also encourage users to demand better privacy practices from companies.

Strengthening Accountability Mechanisms is crucial for ensuring that private entities are held responsible for data breaches and misuse of personal information. This could involve establishing independent regulatory bodies with the authority to investigate complaints, impose fines, and mandate corrective actions. Such bodies should also have the power to conduct audits and assessments of data protection practices within organizations.

Cross-Border Data Transfer Regulations need to be established to ensure that personal data is protected when transferred outside India. These regulations should align with international standards while considering local contexts, ensuring that Indian users' data is treated with the same level of protection regardless of where it is processed.

Ethical Guidelines for Data Use should be developed to address the ethical implications of data collection and processing, particularly in the context of artificial intelligence and big data. These guidelines should promote responsible data practices, ensuring that companies prioritize user consent and transparency in their operations.

Collaboration with International Bodies can help India align its data protection framework with global standards. Engaging with international organizations and participating in global discussions on data privacy can provide valuable insights and best practices that can be adapted to the Indian context.

Regular Review and Updates of Legislation are necessary to keep pace with technological advancements and emerging privacy challenges. A dynamic legal framework that can adapt to changes in the digital landscape will be more effective in protecting individuals' privacy rights.

By implementing these suggestions, India can create a robust data protection framework that not only safeguards individual privacy rights but also fosters trust in the digital economy, encouraging innovation and growth while ensuring that personal data is treated with the respect and care it deserves.

CONCLUSION

The right to privacy has become essential in the digital age, with personal data increasingly managed by private entities like social media platforms and e-commerce websites. In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognized privacy as a fundamental right, laying the groundwork for data protection. However, India still lacks a comprehensive legal framework to address challenges such as cross-border data transfers, data breaches, and ethical concerns around artificial intelligence.

This paper examines the responsibilities of private entities in safeguarding privacy, identifying gaps in India’s legal and ethical frameworks. The Information Technology Rules, 2011 provide limited protection but fail to address the complexities of today’s digital economy. The proposed Personal Data Protection Bill, 2019 remains under review, delaying critical reforms. In contrast, global frameworks like the GDPR and CCPA offer valuable insights into accountability and transparency in data handling, emphasizing user consent and data security.

Case studies, such as the Facebook-Cambridge Analytica scandal, highlight the risks of commodifying personal data without adequate safeguards. India must adapt global models like the GDPR to its socio-economic context, ensuring stronger accountability for private entities managing user data. The ethical

implications of AI-driven data processing further underline the need for robust regulations.

This paper argues for a comprehensive data protection law that balances privacy rights, business interests, and government oversight. By critiquing existing laws, analyzing global frameworks, and addressing ethical concerns, it offers practical recommendations to enhance privacy protections in India. Strengthening corporate accountability and fostering a culture of ethical data use are essential for safeguarding individual rights while supporting innovation and economic growth in the digital age.

REFERENCES

Books and Articles

1. Duggal, Pavan. Cyber Law in India. Universal Law Publishing, 2017. ISBN: 978-9350356153
2. Solove, Daniel J.. Understanding Privacy. Harvard University Press, 2008. ISBN: 978-0674026701
3. Kuner, Christopher. Transborder Data Flows and Data Privacy Law. Oxford University Press, 2017. ISBN: 978-0198732546
4. Bennett, Colin J.. The Privacy Advocates: Resisting the Spread of Surveillance. MIT Press, 2008. ISBN: 978-0262122917

Journal Articles

1. Agarwal, D. "The Privacy Paradox in India: Regulatory Challenges and the Role of Private Entities." Indian Journal of Law & Technology, Vol. 13, Issue 1, 2021, pp. 55-71. ISSN: 0973-0256
2. Pillai, M., and R. Choudhury. "Private Entities and the Digital Privacy Dilemma: A Legal Analysis of the Role of Corporations in Data Protection." Journal of Cyber Law and Policy, Vol. 8, Issue 2, 2022, pp. 82-98. ISSN: 2044-9455
3. Kumar, R., and G. Verma. "The Role of Private Companies in Upholding the Right to Privacy under Indian Law." Indian Journal of Constitutional and Administrative Law, Vol. 6, Issue 3, 2019, pp. 1-22. ISSN: 2348-9778
4. Tripathi, Karan. "Private Sector and Privacy: Analyzing the Impact of Data Protection Laws on Digital Businesses." International Journal of Privacy Law, Vol. 6, Issue 1, 2021, pp. 45-67. ISSN: 2049-7526
5. Prakash, P. (2020). "Digital India and the Privacy Paradox: A Legal Perspective." Indian Journal of Law and Technology, 15(1), 72-89.
6. Gandhi, S. (2019). "Data Protection in India: Challenges and Opportunities." Data Privacy Journal, 2(4), 45-58.
7. Choudhury, S. (2018). "The Facebook-Cambridge Analytica Scandal and the Threat to Privacy." The Journal of Digital Privacy, 7(2), 120-133.

Reports and Policy Papers

1. Ministry of Electronics and Information Technology (MeitY). Personal Data Protection Bill, 2019. Government of India. https://meity.gov.in
2. European Union. General Data Protection Regulation (GDPR), 2016. https://gdpr.eu

3. Data Security Council of India (DSCI). National Strategy on Data Protection. https://www.dsci.in
4. Personal Data Protection Bill, 2019, Ministry of Electronics and Information Technology, Government of India.

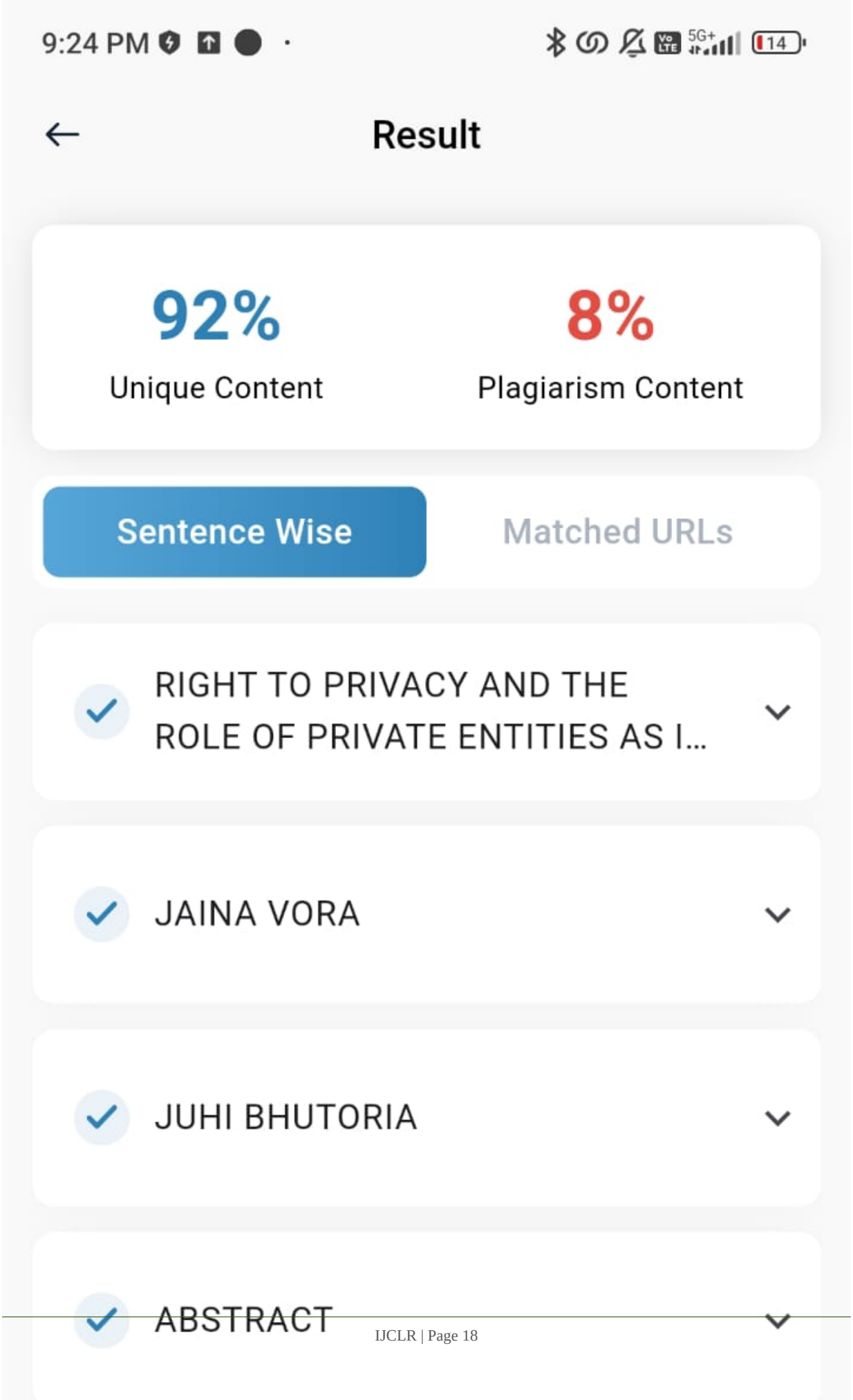
Legal Cases

1. K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
2. Shreya Singhal v. Union of India (2015) 5 SCC 1.
3. Google India Private Ltd vs M/s Visakha Industries

Web Articles and News Sources

1. Jain, P. "The Privacy Breach Epidemic: A Close Look at Private Entities' Accountability." The Hindu, July 22, 2021. https://www.thehindu.com
2. Singh, R. "Privacy and Data Protection in the Digital Age." LiveMint, March 10, 2021. https://www.livemint.com

PLAGIARISM


9:24 PM
Result
92%
Unique Content
8%
Plagiarism Content
Sentence Wise
Matched URLs
RIGHT TO PRIVACY AND THE ROLE OF PRIVATE ENTITIES AS I...
JAINA VORA
JUHI BHUTORIA
ABSTRACT

--- 1. Jaina Vora, BBA.LL.B\\\[HONS\\\], Saveetha School Of Law, Saveetha Institute of Medical And Technical Science \\\[SIMATS\\\], Chennai-600077\[??\](#fnref1) 2. Juhi Bhutoria, B.COM.LL.B\\\[HONS\\\], Saveetha School Of Law, Saveetha Institute of Medical And Technical Science \\\[SIMATS\\\], Chennai-600077\[??\](#fnref2) 3. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295\[??\](#fnref3) 4. *Justice K.S. Puttaswamy v. Union of India*, (2018) 3 SCC 797.\[??\](#fnref4) 5. Universal Declaration of Human Rights, 1948, Article 12.\[??\](#fnref5) 6. European Union, General Data Protection Regulation, 2018.\[??\](#fnref6) 7. Digital Personal Data Protection Act, 2023 (India).\[??\](#fnref7) 8. *Justice K.S. Puttaswamy v. Union of India*, (2018) 3 SCC 797.\[??\](#fnref8) 9. National Cyber Security Policy, 2013 (India); CERT-In guidelines\[??\](#fnref9) 10. Data Transfer Challenges under GDPR, European Data Protection Board Reports.\[??\](#fnref10) 11. Cross-Border Data Privacy Challenges, OECD Reports\[??\](#fnref11) 12. AI Ethics and Data Privacy, World Economic Forum Report, 2022\[??\](#fnref12) 13. European Union, General Data Protection Regulation, 2018\[??\](#fnref13) 14. California Consumer Privacy Act (CCPA), 2018; HIPAA, 1996.\[??\](#fnref14) 15. South Korea’s Personal Information Protection Act (PIPA); Japan’s Act on the Protection of Personal Information (APPI).\[??\](#fnref15) 16. Cambridge Analytica: The Fallout of a Data Breach,” Harvard Law Review, 2019.\[??\](#fnref16) 17. Schwartz, Paul. “The Importance of Data Minimization in E-Commerce,” Journal of Law and Technology, 2021.\[??\](#fnref17) 18. Bhardwaj, Anurag. “Liability of E-Commerce Platforms in Data Breaches,” Indian Law Journal, 2020.\[??\](#fnref18) 19. Susan Landau, “Jurisdictional Conflicts in Data Localization,” Yale Law Review, 2020.\[??\](#fnref19) 20. “Liability in Cloud Computing: The Emerging Legal Framework,” Stanford Technology Law Review, 2021.\[??\](#fnref20) 21. Microsoft Corp. v. United States, 584 U.S. (2018).\[??\](#fnref21) 22. NASSCOM, “India’s Digital Economy,” National Association of Software and Service Companies, accessed December 2024.\[??\](#fnref22) 23. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.\[??\](#fnref23) 24. Personal Data Protection Bill, 2011, Government of India.\[??\](#fnref24) 25. Digital Personal Data Protection Act, 2023, Government of India.\[??\](#fnref25) 26. Personal Data Protection Bill, 2019, Government of India.\[??\](#fnref26) 27. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.\[??\](#fnref27) 28. Shreya Singhal v. Union of India, (2015) 5 SCC 1.\[??\](#fnref28) 29. Google India Private Ltd v. Visakha Industries, (2019) 10 SCC 1.\[??\](#fnref29) 30. European Union, *General Data Protection Regulation (GDPR): Article 83: General Conditions for Imposing Administrative Fines*, Official Journal of the European Union, 2018, available at: \[https://gdpr-info.eu/art-83-gdpr/\](https://gdpr-info.eu/art-83-gdpr/)\[??\](#fnref30) 31. California Civil Code §1798, *The California Consumer Privacy Act (CCPA): Compliance Requirements*, California Legislature, 2020, available at: \[https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100 \](https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100)\[??\](#fn 32. Office of the Privacy Commissioner of Canada, *Privacy Act Guidelines: PIPEDA*, 2018, available at: \[https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/\](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/)\[??\](#fnref32) 33. White & Case LLP, *Proposed American Privacy Rights Act: Establishing Comprehensive National Framework*, 2024, available at: \[https://www.whitecase.com/publications/insight/american-privacy-rights-act \](https://www.whitecase.com/publications/insight/american-privacy-rights-act).\[??\](#fnref33) 34. National People’s Congress of China, *Data Security Law (DSL)*, 2021, available at: \[https://npcobserver.com/data-security-law/\](https://npcobserver.com/data-security-law/)\[??\](#fnref34)

35. National People’s Congress of China, *Personal Information Protection Law (PIPL)*, 2021, available at: \[https://npcobserver.com/personal-information-protection-law/ \](https://npcobserver.com/personal-information-protection-law/)\[??\](#fnref35) 36. European Union, *General Data Protection Regulation (GDPR)*, Article 35, Official Journal of the European Union, 2018, available at: \[https://gdpr-info.eu/art-35-gdpr/\](https://gdpr-info.eu/art-35-gdpr/)\[??\](#fnref36) 37. California Civil Code §1798.185, *The California Consumer Privacy Act (CCPA)*, 2020, available at: \[https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.185 \](https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.185)\[??\](#fn
38. National People’s Congress of China, *Personal Information Protection Law (PIPL)*, 2021, available at: \[https://npcobserver.com/personal-information-protection-law/ \](https://npcobserver.com/personal-information-protection-law/)\[??\](#fnref38) 39. European Union, *General Data Protection Regulation (GDPR)*, Articles 5, 24, and 25, Official Journal of the European Union, 2018, available at: \[https://gdpr-info.eu/art-5-gdpr/\](https://gdpr-info.eu/art-5-gdpr/)\[??\](#fnref39) 40. European Union, *General Data Protection Regulation (GDPR)*, Articles 5, 24, and 25, Official Journal of the European Union, 2018, available at: \[https://gdpr-info.eu/art-5-gdpr/ \](https://gdpr-info.eu/art-5-gdpr/)\[??\](#fnref40) 41. Flipkart Data Breach (2018), The Economic Times, “E-commerce giant Flipkart faces backlash after breach of consumer data”.\[??\](#fnref41) 42. Amazon Web Services Data Localization Debate, The Hindu, “India’s data localization push sparks debate over privacy and cross-border data flow”.\[??\](#fnref42) 43. WhatsApp Privacy Policy Controversy (2021), The New York Times, “WhatsApp’s privacy policy update faces backlash in India”.\[??\](#fnref43) 44. Cambridge Analytica Scandal, BBC News, “Cambridge Analytica and Facebook: The Scandal Explained.”\[??\](#fnref44)