CORPORATE LAW WATCH

WELCOME TO THE CORPORATE LAW WATCH

We are pleased to present the latest edition of the Corporate Law Newsletter, which explores India's evolving data privacy landscape in the context of rapidly advancing AI technologies.

This edition offers a corporate perspective on the implications of the Digital Personal Data Protection Act, 2023, highlights key misuse cases, and outlines practical steps for businesses to navigate AI-related privacy risks in India.

NAVIGATING INDIA'S DATA PRIVACY CHALLENGES IN THE AGE OF AI: A CORPORATE PERSPECTIVE

India's Shifting Data Privacy Landscape Amidst the AI Revolution

The rapid adoption of artificial intelligence (AI) tools such as ChatGPT, Gemini, and DeepSeek continues to redefine personal and professional digital interactions in India. While the convenience and power of these platforms are undeniable, their proliferation exposes users to pressing concerns regarding data exploitation, privacy breaches, and gaps in regulatory oversight.

Introduction

The pervasive integration of AI-driven solutions into daily life is reshaping how individuals access information, seek counsel, and interact online. ChatGPT, in particular, stands out as a transformative force, delivering conversational support on diverse issues ranging from education and work to mental health and legal queries. However, the increasing reliance on such AI platforms brings the adequacy of India's data privacy laws sharply into focus.

OpenAI CEO, Sam Altman, recently issued a cautionary note about over-reliance on tools like ChatGPT for highly sensitive matters. He emphasized that conversations with AI do not benefit from the confidentiality privileges granted to professional relationships with doctors, lawyers, or therapists. Notably, information shared with AI tools may be subpoenaed and disclosed in legal proceedings.

As AI becomes embedded in more aspects of personal and organizational decision-making, India's existing legal framework still evolving to address the nuances of digital privacy faces mounting pressure. This moment calls for a clear-eyed assessment of how these tools collect, process, and repurpose personal data, and for an urgent strengthening of regulatory mechanisms and enforcement capacity. Only by confronting these challenges head-on can India ensure that the benefits of AI are realized without compromising the fundamental right to privacy.

I. Current Legal Framework

India's data protection regime is anchored in the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the "DPDP Act"), which requires explicit user consent for data collection, limits processing to lawful purposes[1], and mandates deletion of data once its purpose is fulfilled[2]. It

further requires data fiduciaries to ensure the accuracy and completeness of personal data during processing[3] and implementing reasonable security safeguards and breach notification obligations in the event of unauthorized access or disclosure[4]. However, DPDP Act is yet to be fully operationalized, and it currently lacks provisions tailored to the latest suite of AI tools, particularly with respect to emotional or sensitive user data (including non-verbal cues such as facial expressions, vocal tone, body language, and even physiological responses like heart rate). The older Information Technology Act, 2000 (hereinafter referred to as the "IT Act"), continues to function in parallel, but its provisions are largely inadequate for present-day AI-related privacy concerns.

II. How Privacy is Misused in India

Despite evolving data protection norms, misuse of personal data in India remains common. Many AI-enabled apps, especially in mental health and finance, collect sensitive data without clear consent, violating the provisions of DPDP Act. Reports show some AI therapy platforms store user conversations without confidentiality safeguards, with data often sold to third parties including advertisers and insurers, raising serious ethical concerns[5]. Moreover, while the IT Act criminalized the transmission of 'offensive' or 'menacing' messages via electronic communication, the said provision was struck down by the Supreme Court in Shreya Singhal v. Union of India[6] for violating the fundamental right to freedom of speech, however its remnants and related
provisions continue to be used to justify broad state surveillance without judicial oversight.[7]

III. AI Conversations aren't private- Data Security Threats for Indian Businesses

AI chatbots like ChatGPT, Gemini, Deep seek pose unique privacy risks under India's emerging legal regime. Unlike privileged communication with doctors or lawyers, AI chats lack confidentiality and may be subject to disclosure in legal proceedings. Users often share sensitive mental health data, which platforms can repurpose without safeguards. Many Indian apps, especially in health-tech and fintech, use deceptive "dark patterns" to obscure consent, 79% showed privacy deception, and 52 out of 53 used manipulative interface designs[8]. In combination, these risks highlight systemic gaps in protecting sensitive user data within India's current privacy regime.

IV. The AI and Copyright Nexus

India is a signatory to inter alia (a) the Berne Convention for the Protection of Literary and Artistic Works, 1886; (b) the Universal Copyright Convention, 1952; and (c) the World Intellectual Property Organization (WIPO) Copyright Treaty, 1996.

Authors of original literary, dramatic, musical and artistic works, cinematographic films, sound recordings, including computer programs, tables and compilations have been known to increasingly distance themselves from AIgenerated copies or look-alikes. More recently, the use of AI generated images on a popular social media application, which made users look similar to images created by Japanese animation studio Studio Ghibli, Inc., brought this issue to attention once again.

When AI-generated images or artwork are used for commercial purposes and/or widely disseminated, the public is often misled as to the author of such images or artwork. The AI artwork or image in such cases will unduly benefit from the author's notoriety and creative efforts. Consequently, such use could constitute acts of parasitism / passing-off and unfair competition.[9]

V. Recent Misuse Cases

Several high-profile incidents in India have underscored the urgent need for stronger data privacy safeguards. A 2023 study by Mozilla revealed that over 90% of Indian mental health apps shared sensitive user data, including emotional and behavioral information with third-party advertisers, often without clear or informed consent*[10]*. In the private sector, ransomware attacks have intensified, according to a 2023 report by Sophos, over 60% Indian organisations experienced data breaches, many involving exfiltration of customer information and extortion attempts*[11]*.

The AI-altered re-release of a film raises important questions about the scope of authors' moral rights*[12]*

under the Copyright Act, 1957, particularly concerning postrelease modifications. While producers hold broad economic rights under the Copyright Act[13], authors retain moral rights and may object to distortions that compromise the integrity of their work. As AI-generated alterations become more common, studios, OTT platforms, and financiers will need to revisit existing and future contracts to address such changes, balancing creative integrity with commercial flexibility. Content agreements are likely to incorporate explicit provisions for AI-driven adaptations, clearly defined approval processes for postrelease modifications, and, where enforceable, waivers of moral rights to mitigate the risk of legal disputes[14].

V. Recommendations

Addressing AI-related privacy risks requires a multipronged approach. Regulators must fully enforce the DPDP Act and consider AI-specific amendments for regulating how emotional, biometric and sensitive data is utilized by commercial platforms. Users should avoid sharing sensitive information on AI platforms and opt for encrypted services. Developers must be held to higher standards of transparency, with mandatory privacy by design practices and penalties for non-compliance to ensure ethical data use. These measures are crucial to bridge the gap between technological innovation and fundamental privacy rights in India.

VI. Conclusion

The DPDP Act marks a pivotal milestone in India's data governance landscape. However, in the absence of timely implementation and AI-specific legislative refinements, platforms like ChatGPT may continue to operate in a grey regulatory area, heightening the risk of large-scale privacy violations. Sam Altman's cautionary remarks underscore a critical reality that interactions with AI systems are not shielded by legal privilege and must, by default, be treated as non-confidential. To safeguard individual privacy in an era of accelerating AI integration, it is imperative to strengthen regulatory oversight, promote digital literacy, and embed accountability mechanisms within AI development and deployment.

[1] Section 5, Digital Personal Data Protection Act, 2023. https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act_2023.pdf
[2] Section 7, ibid
[3] Section 6, ibid
[4] Section 8, ibid
[5] Mozilla Foundation, Privacy Not Included Report, 2023 – State of Online Privacy Reaches 'Very Creepy' Level, Finds Mozilla's First-Annual Consumer Creep-O-Meter - Mozilla Foundation
[6] Shreya Singhal v. Union of India, (2015) 5 SCC 1
[7] Supreme Court 'shocked' over scrapped Section 66A law's use in FIRs, issues notice to Centre - India Today
[8] ASCI-Parallel HQ "Conscious Patterns" study: 79% of Indian apps deploy privacy deception; 52 of 53 apps use dark patterns, The Indian Express, business-standard.com
[9] Generative AI and copyright: The Studio Ghibli effect - https://www.novagraaf.com/en/insights/generative-ai-and-copyright-studioghibli-effect#:~:text=Ideas%2C%20methods%20or%20concepts%20are,of%20its%20author%20is%20prohibited
[10] Mozilla Foundation, Privacy Not Included: Mental Health Apps Report (2023) – Shady Mental Health Apps Inch Toward Privacy and Security Improvements, But Many Still Siphon Personal Data - Mozilla Foundation
[11] Sophos, The State of Ransomware in India 2023, Over 60% Indian Organizations Vulnerable to AI-Driven Ransomware Attack: Sophos
[12] Section 57 https://www.indiacode.nic.in/handle/123456789/1367
[13] Section 2(uu) ibid
[14] https://indianexpress.com/article/explained/explained-law/raanjhanaa-ai-re-release-director-aanand-l-rai-unhappy-law-10159524/
[15] NITI Aayog, Responsible AI for All (2021); OECD, Principles on Artificial Intelligence – Part2-Responsible-AI-12082021.pdf, AI principles | OECD

Contributed by:

Sameena Jahangir
Partner

Nischala Maruvada
Senior Associate