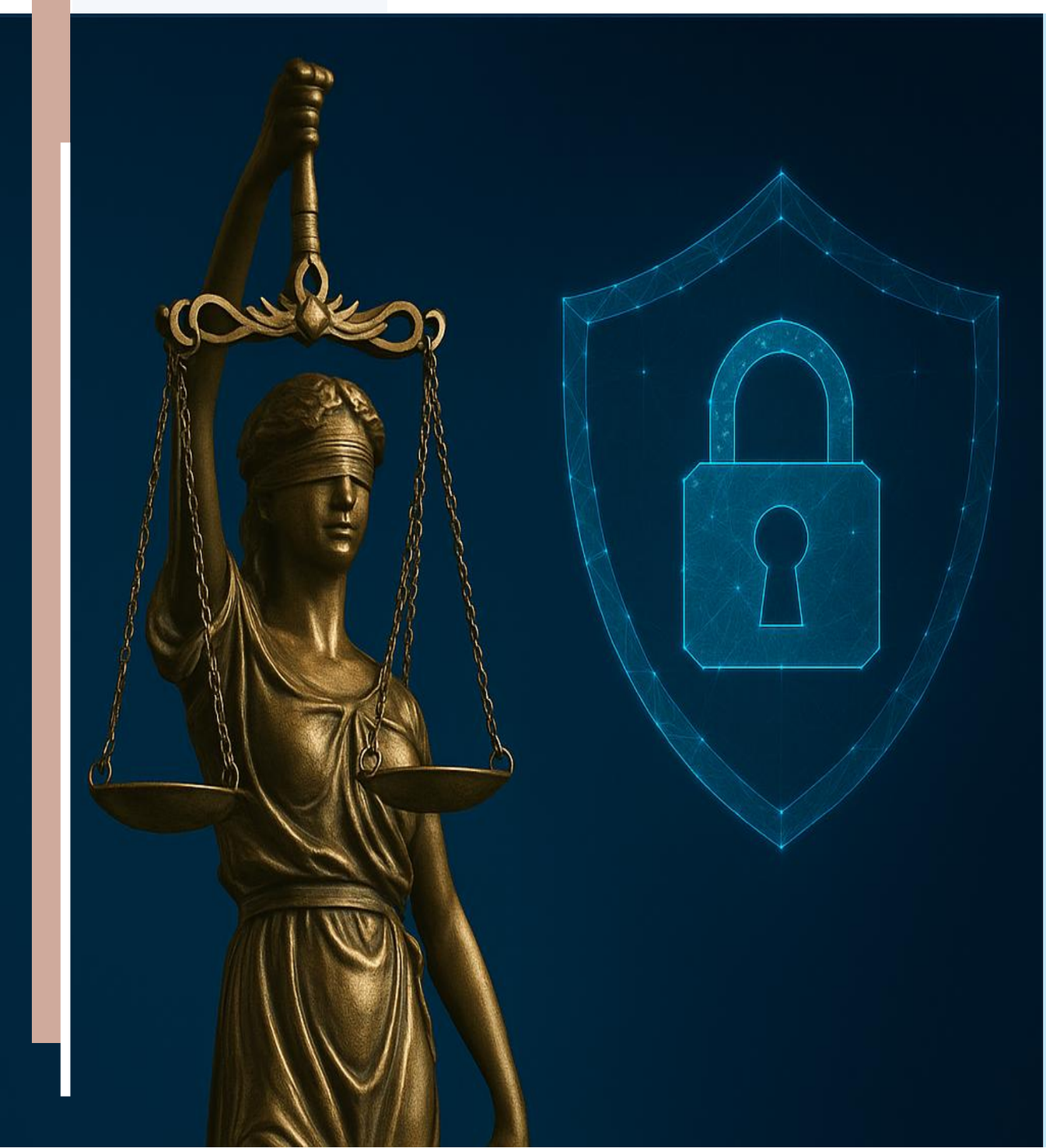
SHIVADASS & SHIVADASS®
LAW CHAMBERS

COMPETITION, DATA PROTECTION & PRIVACY SNIPPETS

3rd Ed.



Quarterly Update December 2025

INDIA

Regulatory

Competition Commission of India issues Market Study Report on AI and Competition

- The CCI released a "Market Study Report on Artificial Intelligence and Competition" on 06.10.2025.
- It suggests that rapid AI adoption is reshaping market behavior and regulatory challenges. While AI offers efficiency and innovation gains, it also poses competition risks.
- Important recommendations: Implementing self-audit frameworks to prevent unintended anti-competitive outcomes, enhancing transparency around AI-driven decisions and reducing entry barriers by expanding national AI computing infrastructure and developing high-quality non-personal data repositories.

CCI seeks clarification from NCLAT on WhatsApp-Meta judgment

- The CCI has approached the NCLAT seeking clarification from the Tribunal on whether the order implies that user consent is needed in cases where data is used for advertising or for non-advertising purposes.
- The NCLAT had held that user data is paramount, and that user consent must be taken irrespective of whether the data is sued for advertising or non-advertising purposes. However, in para 264, the NCLAT held that para 247.1 of the CCI's order is set-aside, while para 247.2 is upheld. The effect of this being that user consent is required for WhatsApp sharing data for non-advertising purposes, but there is no clarity on consent for sharing user data for advertising purposes.
- The CCI seeks clarity on whether user consent must be taken for advertising purposes, or is the protection restricted to data collected for non-advertising purposes.

EUROPE

Regulatory

European Commission opens antitrust investigation into Meta's new policy regarding AI providers' access to WhatsApp

- The European Commission has launched an antitrust investigation into whether Meta's new policy restricting third-party AI providers from accessing the WhatsApp Business Solution violates Article 102 TFEU and Article 54 European Economic Agreement (EEA).
- As per Meta's New Policy, which was announced in October 2025, AI providers are prohibited from using the WhatsApp Business Solution API when AI is the primary service being offered. AI use is still allowed for ancillary or support functions.
- The Commission suspects that the policy may block competing AI providers from offering their services through WhatsApp in the EEA, foreclose downstream markets for conversational AI services and favor Meta's own conversational AI tool (Meta AI), which will remain accessible.
- This may constitute self-preferencing by a dominant platform under Article 102 TFEU and Article 54 EEA.

EU opened a formal investigation into whether Google is breaching DMA

- On 13.11.2025, the EU initiated an investigation into whether Google is violating Digital Markets Act (DMA) by unfairly downgrading news and other publisher's content in its search results.
- This is primarily centered around Google's "site reputation abuse policy" which is alleged to be used to target and manipulate search rankings by Google.
- EU is currently looking into whether these demotions restrict publisher's freedom to conduct business, innovate and collaborate with third-party content providers

EU Fines X for Deceptive Practices and Lack of Transparency Under DSA

- The European Commission on 05.12.2025, fined X Platform, 120 million euros for breaching the Digital Services Act.
- The Commission found that 'blue checkmark' did not entail actual verification and could be obtained by anyone in lieu of payment.
- It also found a lack of transparency in its advertising repository as X incorporates design features and access barriers, such as excessive delays in processing, which undermine the purpose of ad repositories. X's ads repository also lacks critical information, such as the content and topic of the advertisement, as well as the legal entity paying for it
- It found X fails to meet its DSA obligations to provide researchers with access to the platform's public data. X's processes for researchers' access to public data impose unnecessary barriers, effectively undermining research into several systemic risks in the European Union.
- X must submit action plans within 60-90 working days to address these infringements or face further penalties

European Commission fines fashion brands Gucci, Chloé and Loewe over €157 million for anticompetitive pricing practices

- European Commission fines fashion brands Gucci, Chloé and Loewe over €157 million for anticompetitive pricing practices.
- The companies restricted independent retailers, both online and offline, from setting their own prices by enforcing adherence to recommended prices, discount limits, specific sales periods and, at times, total bans on discounts. Gucci also imposed an online sales restriction for a specific product line.
- These practices, in place between 2015 and 2023 depending on the brand, formed single and continuous infringements of Article 101 TFEU and Article 53 EEA. However, fines were later reduced due to cooperation.

UNITED STATES OF AMERICA

Regulatory

FTC issues order prohibiting noncompete enforcement by gateway services

- The FTC, on 26.11.2025, issued a final order barring Gateway Services from using or enforcing noncompete clauses affecting nearly 1800 employees nationwide.
- The agency found the company's agreements which blocked workers from joining any rival pet-cremation provider for a year, unlawfully restricted mobility and harmed labor-market competition.
- Following a public comment period, the Commission approved the settlement.
- Gateway must notify workers and is permanently prohibited from imposing similar noncompete in future.

FTC endorses Texas rule change to end ABA monopoly on Bar admissions

- The FTC on 02.12.2025, endorsed a proposed Texas Supreme Court rule eliminating ABA's control over law school approval for bar admission due to reasons like competitive harms from ABA's monopoly.
- The change aims to lower barriers, expand access to legal education and benefit prospective lawyers and consumers by encouraging other states to consider similar reforms.

INDIA

Court Room Updates

NCLAT partially upholds CCI's order against WhatsApp-Meta – *WhatsApp LLC v. CCI, Competition Appeal No. 1 of 2025*

The NCLAT considered two appeals filed against orders of CCI, finding WhatsApp and Meta in contravention of the Competition Act, 2002. On 18.11.2024, the CCI found that WhatsApp (Meta) abused dominance by using a 2021 privacy policy to impose unfair conditions on users leverage dominance in OTT messaging Apps through smartphones in India to strengthen Meta's position in online display advertising and imposed an INR 213.14 crore penalty and remedy of a 5-year restriction on sharing WhatsApp user data with other Meta companies for advertising.ad leveraged its dominant position to benefit its subsidiary in the downstream market.

Key Violations Found	Decision
Imposition of a non-negotiable 2021 privacy policy, eliminating users' ability to opt out of data sharing.	NCLAT upheld monetary penalty of INR 213.14 crore upheld for coercive implementation of the 2021 privacy policy
Abuse of dominance in the market for OTT messaging apps on smartphones in India, driven by network effects and user lock-in.	The five-year ban on data sharing between WhatsApp and Meta was set-aside.
Leveraging dominance in OTT messaging to strengthen Meta's position in the online display advertising market.	NCLAT also affirmed that privacy-related conduct can fall within CCI's jurisdiction when linked to abuse of dominance.
Exploitation of non-price parameters such as data, privacy, transparency and user choice.	Clarified that remedies exclusively concerning data protection lie under the DPDP Act, 2023, not competition law.

CCI dismisses abuse of dominance complaint against Google Play for unilateral termination of account, In re: *Liberty Infospace, Case No. 07/2025 dt. 06.10.2025*

The informant, Liberty Infospace Pvt. Ltd. (Liberty) an MSME in the productivity tools development industry, launched a HR and payroll app on the Google Play store in 2021. Liberty's developer account was terminated in 2024 citing "prior violations of the Developer Program Policies and Developer Distribution Agreement by this or associated previously terminated Google Play Developer Accounts" as the reason for termination.

Key Violations Found	Decision
Alleged unilateral termination of Liberty's developer account without clear notice or reasons, contrary to the Play Store agreement.	The CCI defined the relevant market as the market for app stores for Android OS in India and found Google to be dominant due to network effects and lack of substitutes.
Opaque and automated enforcement and appeal mechanisms, allegedly denying effective redressal to developers.	However, it held that the account termination was in line with Google's standard-form contractual policies, applied uniformly across developers.
Denial of market access to an MSME app developer, causing economic hardship and amounting to abuse of dominance	The automated enforcement and appeal mechanisms involved human review and were not arbitrary or unfair.
	Did not amount to abuse of dominance under Section 4.

CCI justifies 10% penalty on global turnover for tender cartel– In re: Nagrik Chetna Manch, Case No. 50/2015 dt. 10.11.2025

- An information was filed in 2015 by Nagric Chetna Trust, a public charitable trust, alleging bid rigging and collusive bidding by the Opposite Parties (OPs). On examination of the information, the Director General (DG) was directed to investigate the matter. The DG found the involvement of additional bidders. Four more OPs were impleaded, and the CCI was in receipt of several Lesser Penalty applications.

Key Violations Found	Decision
Bid rigging and collusive bidding by OPs across five tenders, violating Section 3(3)(d) read with Section 3(1) of the Act.	NCLAT upheld the finding of cartelisation, noting that sufficient evidence was on record and that leniency applications constituted an implicit admission of guilt.
Cartelisation through coordinated conduct, including submission of cover bids to defeat competitive tendering.	However, it remanded the matter to the CCI for re-quantification of penalty due to lack of justification for imposing the maximum penalty.
Repeated anti-competitive conduct across multiple tenders, indicating sustained intent rather than isolated behavior.	Following dismissal of the CCI's SLPs, the CCI reaffirmed the maximum penalty of 10% of average global turnover, holding that reliance on relevant turnover would lead to anomalous results as several OPs were not operating in the relevant market.
Lack of awareness of the law cannot be justified, especially when the bid-rigging conduct is repeated several times.	• Given the deliberate and repeated nature of the conduct aimed at manipulating tenders, the CCI held the imposition of the maximum penalty to be justified.

CCI finds liquor trade associations in violation of the Competition Act, 2002 – In re: XYZ (Confidential), Case No. 43/2019 dt. 11.12.2025

- The Informant alleged that several associations of licensed retail liquor vendors or wine shop owners (OPs) had been operating as a cartel, stipulating that the companies engaged in the manufacture, distribution or sale of alcoholic beverages must adhere to terms such as in relation to retail margins, new product launching schemes, transport delivery terms, cash discount rates, credit period, mandatory launching fees, donations etc., in violation of Sections 3(3) and 4(2) of the Competition Act, 2002. It was also alleged that OPs fixed the selling terms and prices of any new product to ensure their fixed margins.

Key Violations Found	Decision
Price fixing through trade association circulars, prescribing uniform discounts, margins and payment terms.	The CCI held that trade associations are amenable to the Competition Act as their decisions influence industry conduct.
Limitation of supply and market access by mandating NOCs from the OPs for introduction of new products, violating Section 3(3)(b).	It rejected efficiency and industry-practice defenses, holding that coordination on price and trading terms strikes at the core of Section 3.
Coordination among competitors through association-led communications restricting independent commercial decision-making.	On merits, it found the OPs' circulars and NOC requirements to violate Sections 3(3)(a) and 3(3)(b) read with Section 3(1) and directed the OPs to cease and desist from such practices.
Lack of awareness of the law cannot be justified, especially when the bid-rigging conduct is repeated several times.	Considering mitigating impact on small retailers and welfare activities, the CCI refrained from imposing a monetary penalty..

NCLAT upholds CCI's observation that it lacks power to examine dispute over patented products– Swapan Dey v. CCI, Competition Appeal (AT) No. 5 of 2023

- The Appellant, a CEO of a hospital that provides free dialysis to patents under a PPP scheme, argued that patients undergoing dialysis frequently suffered from Iron Deficiency Anemia. The treatment, an injection of Ferric Carboxymaltose, was not accessible or affordable for patients due to the alleged anti-competitive and abusive conduct of the patent holder Vifor International. An appeal was preferred before the NCLAT challenging the CCI's order under Section 26(2) of the Act holding that there was no violation of Section 3 and 4 of the Act.

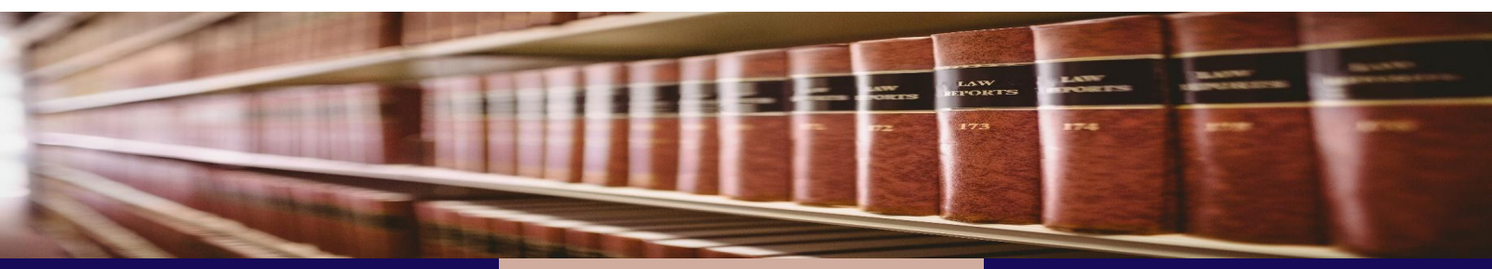
Key Violations Found	Decision
Alleged abuse of dominance by a patent holder through pricing and licensing practices restricting access to injections..	The NCLAT dismissed the appeal and upheld the CCI's finding of no violation of Sections 3 or 4 of the Act. .
Alleged anti-competitive agreements limiting manufacture and supply of an essential drug used in dialysis treatment.	It noted that the patent expired in October 2023, placing the drug in the public domain.
Coordination among competitors through association-led communications restricting independent commercial decision-making.	Relying on the Delhi High Court's ruling in Ericsson v. CCI, LPA 247/2016, and the Supreme Court's dismissal of the SLP in CCI v. Monsanto, SLP No. 25026/2023, the NCLAT held that issues relating to patent licensing and exploitation fall within the domain of the Patents Act, 1970.
Denial of affordable access to patients under a PPP healthcare scheme due to patent-based restrictions.	In view of Section 3(5) of the Competition Act, which protects reasonable conditions imposed by patent holders to safeguard their rights, the CCI was found to lack jurisdiction to examine the allegations against Vifor International.

EUROPE

Court Room Updates

Stichting Right to Consumer Justice, Stichting App Stores Claims v. Apple Distribution International Ltd, Apple Inc., Case C-34/24, 02.12.2025

- Two Dutch consumer foundations filed representative actions alleging that Apple's App Store practices caused harm to users in the Netherlands by imposing excessive commissions on app developers, which were ultimately passed on to consumers. Apple contested the jurisdiction of Dutch courts, arguing that no harmful event occurred in the Netherlands as its relevant conduct was carried out outside the country. The dispute required the European Court of Justice to examine whether damage arising from purchases made via the App Store by Dutch users could be said to occur in the Netherlands for the purposes of jurisdiction under the Brussels I Recast Regulation.



Key Violations Found	Decision
Alleged abuse of dominant position through imposition of excessive 15–30% commissions on app sales.	The ECJ held that Dutch courts have jurisdiction to hear the representative actions under Article 7(2) of the Brussels I Recast Regulation.
Harm to Dutch consumers arising from Apple's App Store pricing and distribution practices.	It found that the App Store accessible to users holding a Netherlands Apple ID constitutes a virtual space specifically targeting the Dutch market, and that any damage suffered by users purchasing apps on that platform materialises in the Netherlands.
Dispute over territorial localisation of damage caused by digital platform conduct	Accordingly, the place where the damage occurred was the Netherlands, making Dutch courts the appropriate forum to adjudicate the claims.

Amazon EU v Commission, T-367/23, 19.11.2025

- Amazon EU Sàrl, which operates the Amazon Store marketplace in the European Union, challenged the European Commission's April 2023 decision designating its platform as a "Very Large Online Platform" (VLOP) under the Digital Services Act (DSA). Under the DSA, online services with more than 45 million monthly active users in the EU (10 % of the population) may be designated VLOPs and subject to enhanced obligations, including systemic risk assessments, transparency measures and data access requirements. Amazon sought annulment of the designation and argued that the resulting VLOP obligations infringed several rights protected by the EU Charter of Fundamental Rights, including the freedom to conduct a business, the right to property, equality before the law, freedom of expression and information, and the protection of confidential information.

Key Violations Found	Decision
Alleged infringement of freedom to conduct a business due to the burdens imposed by VLOP obligations	The General Court dismissed Amazon's action in full, upholding the European Commission's designation of the Amazon Store as a VLOP under the DSA.
Alleged violation of right to property and protection of confidential information through obligations such as transparency and data access..	It held that the interference with fundamental rights cited by Amazon, including the freedom to conduct a business and the right to property, was provided for by law, pursued legitimate objectives such as mitigating systemic risks and protecting users, and was proportionate and justified within the EU legislature's broad discretion.
Alleged breach of equality before the law and freedom of expression and information by applying DSA obligations to a marketplace platform.	• The court found no manifest error in the EU legislature's assessment that very large online platforms could pose systemic risks warranting specific obligations under the DSA, and that these obligations did not breach the EU Charter of Fundamental Rights.

INDIA

Regulatory

The reversal of Sanchar Saathi mandate

- On 28.11.2025, the Government of India ordered smartphone makers to preload the Sanchar Saathi cyber safety app on all new devices and prevent users from disabling it. However, facing intense criticism from opposition parties and digital rights groups, the Government reversed the mandatory pre-installation on 03.12.2025. Sanchar Saathi, already downloaded over 14 million times, helps block stolen phones and identify fraudulent mobile connections.

Notification of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025

- The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025, were notified on 22.10.2025 and effective from 15.11.2025.

- It introduces safeguards to ensure transparent and proportionate content removal. Only senior officers (Joint Secretary/DIG-level) may issue removal intimations. All such directions undergo monthly review by an officer of the rank of Secretary.

- Intimations must be reasoned, specify the legal basis, nature of unlawfulness and precise URLs.

Draft Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, relating to synthetically generated information

- On 22.10.2025, MeitY released draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021to address risks from synthetically generated information, including deepfakes and misinformation.

- Public feedback was initially invited until 06.11.2025, later extended to 13.11.2025.

- The Amendments were proposed to plug a regulatory gap in the IT Rules, 2021 by expressly addressing the rapid rise of AI-generated and deepfake content, which has been increasingly used for misinformation, impersonation, fraud, and reputational harm, posing risks to public trust, democratic processes, and online safety.

- The draft introduces a definition of “synthetically generated information ,” grants safe-harbour protection for good-faith removal of harmful synthetic content, mandates labelling and permanent metadata for all AI-generated content and imposes enhanced SSMI obligations like requiring user declarations, technical verification, and prominent synthetic-content labels.

- This definition is intended to bring AI-generated content squarely within the regulatory framework, enable enforceable labelling and due-diligence obligations on intermediaries, and ensure users can clearly distinguish synthetic content from authentic information.

INDIA

Regulatory

Study on 'AI for Inclusive Societal Development' released by NITI Aayog

- On 8.10.2025, NITI Aayog published a study titled "AI for Inclusive Societal Development", examining how AI and frontier technologies can support India's 490 million informal workers.
- It proposes the Mission Digital ShramSetu, a national mission to make AI accessible and impactful for informal workers through immersive learning tools, digital platforms, research, data-driven insights and strong policy support.
- The roadmap aligns with the Viksit Bharat 2047 vision and emphasises urgent, coordinated action to prevent income stagnation and ensure inclusive growth.

FIU-IND issues notices to 25 offshore VDA service providers for PMLA non-compliance (1 October 2025)

- The Financial Intelligence Unit-India (FIU-IND) has issued notices under Section 13 of the Prevention of Money Laundering Act, 2002 to 25 offshore Virtual Digital Asset Service Providers (VDA SPs) for operating in India without mandatory registration and compliance. These entities, such as Huione, Paxful, CEX.IO, BingX, BitMex, and others, have also been directed under Section 79(3)(b) of the IT Act to take down illegal applications/URLs accessible to Indian users.
- FIU-IND noted that while 50 VDA SPs are currently registered, several offshore platforms continue serving Indian users without meeting AML/CFT obligations, which apply irrespective of physical presence in India. VDA SPs engaged in exchange, transfer, safekeeping, or administration of virtual digital assets must register as reporting entities and comply with PMLA requirements. The release also reiterates that crypto assets and NFTs remain unregulated and pose significant financial risks.

Telecommunications (Telecom Cyber Security) Amendment Rules, 2025

- On 22.10.2025, the Department of Telecommunications has notified the Telecommunications (Telecom Cyber Security) Amendment Rules, 2025, introducing key additions to strengthen telecom identifier security.
- The amendments define new entities like licensees, TIUEs (Telecommunication Identifier User Entities) and the Mobile Number Validation (MNV) platform. Government and authorised agencies may now require TIUEs and licensees to validate user identifiers through the MNV platform. They empower the Government to temporarily suspend or permanently disconnect identifiers in public interest.

Europe

Regulatory

Digital Omnibus Notification

- On 19.11.2025, the European Commission presented its much anticipated "Digital Omnibus" package which intends to ease the administrative and compliance burden facing European businesses. Alongside this, the Commission is running a Digital Fitness Check to evaluate the combined impact of EU digital rules. The proposals mainly focus on four areas, i.e., Cybersecurity, Data Protection, E-Privacy and Data use and governance.

- The package has two primary proposed Omnibus laws, i.e., (1) Digital Omnibus (a general regulation simplifying and consolidating parts of the EU's digital acquis, making targeted amendments to data, privacy and cyber laws) and (2) Digital Omnibus on AI (a regulation on the simplification of the implementation of harmonized rules on AI).

- The notification includes proposal to amend the definition of personal data provided in the GDPR to an entity-dependent definition, possibly narrowing the conception of personal data. The new definition is based on the decision of Court of Justice of the European Union (hereinafter referred to as "***CJEU***"), C-413/23 ***EDPS v. SRB*** dated 04.09.2025, where the CJEU found that data to be considered personal only if the controller has actual means to identify a natural person.

Child Sexual Abuse Regulation (CSAR) (also known as "the Chat Control Law")

On 26.11.2025, the Council of the EU approved a revised version of CSAR. The revised proposal removes the original requirement for mandatory, blanket scanning of all private communications and replaces it with a voluntary detection model for messaging platforms. While mandatory scanning is gone, providers must still assess how their services could be misused for child sexual abuse, implement mitigation measures, and cooperate with a new EU Centre on Child Sexual Abuse. High-risk services may still be required to build or use scanning tools, including AI-based detection systems. Support for the proposal varies across the EU.

New rules to improve cooperation between national data protection bodies when they enforce GDPR

- The EU Council adopted new rules to improve cooperation between national data protection bodies when they enforce the General Data Protection Regulation (GDPR) in order to speed up the process of handling cross-border data protection complaints. The new rules aim to streamline cooperation among data protection authorities (DPAs) when cases involve companies operating across multiple EU member states. Such cases have often been slowed by procedural disagreements, inconsistent standards, and lengthy back-and-forth between national regulators earlier.

- The law introduces harmonized criteria for assessing whether complaints are admissible, ensuring that all DPAs follow the same standards when deciding to open an investigation. It also sets common rules for complainant participation and clarifies companies' rights, including the right to be heard and to receive preliminary findings. To ease administrative load, the regulation creates a "simple cooperation procedure" for straightforward cases, avoiding the lengthy full cooperation mechanism. It also imposes strict deadlines like standard investigations must be completed within 15 months (with a possible 12-month extension for complex cases), while simple cases must finish within 12 months. With the Council's approval, the regulation will enter into force 20 days after publication and will apply 15 months later.

United States of America

Regulatory

Seven things to know before 2026 CCPA updates take effect

The California Privacy Protection Agency (CPPA) has recently issued a new guidance document titled "7 Things to Know Before 2026 CCPA Updates Take Effect", outlining key compliance obligations businesses should know and prepare for before the updated California Consumer Privacy Act regulations become effective on 01.01.2026:

- Conducting risk assessments for certain types of new data processing;
- Providing consumers with a means to confirm status of opt-out requests;
- Allowing access to personal information collected as far back as 21.01.2022;
- Providing consumers with the name of the source from which they received inaccurate information or inform the source themselves that the data must be corrected,;
- Maintaining accurate data;
- Accepting and making available consumer statements contesting the accuracy of health information; and
- Personal information of consumers under 16 years of age is now considered sensitive personal information.

California's Data Broker Enforcement Strike Force

On 18.11.2025, the CPPA announced a new Data Broker Enforcement Strike Force within its Enforcement Division to investigate potential violations of the CCPA and the Delete Act's data broker registration rules. The unit will also support rollout of the Delete Request and Opt-Out Platform, which will let consumers submit a single deletion request to all registered data brokers starting January 2026. This move follows the CPPA's 2024 enforcement sweep of data brokers, which has already led to numerous ongoing actions. The Strike Force will strengthen oversight and expand enforcement of both the CCPA and Delete Act requirements.

California Approves Delete Act Regulations (13.11.2025)

California's Office of Administrative Law has approved new regulations to implement the Delete Act, enabling a major expansion of consumer privacy rights. Beginning 01.01.2026, Californians will be able to use the CPPA's new Delete Request and Opt-out Platform (DROP) (a state-run website allowing users to request deletion of their personal data from hundreds of data brokers with a single click). Under the regulations:

- Starting 01.08.2026, data brokers must check the DROP at least every 45 days for new deletion requests.
- When a match is found, data brokers must delete all related personal information, including inferences, unless an exemption applies.
- Data brokers must update the DROP within 45 days to report the status of each request.
- They must also maintain a record of all deletion requests to ensure ongoing compliance.

India

Court Room Updates

Akshay Hari Om Bhatia v. John Doe (25.10.2025)

The plaintiff, actor Akshay Kumar, alleged large-scale misuse of his personality rights through AI-generated deepfake videos, morphed images, unauthorized voice cloning, impersonation and sale of merchandise bearing his likeness. A recent deepfake video falsely depicted him making communally inflammatory remarks about Rishi Valmiki, which went viral and threatened his reputation, dignity and family's safety. He sought urgent injunctive relief against unknown entities, websites and social media platforms to curb the unlawful commercial exploitation and dissemination of such fabricated content.

Key Violations Found	Decision
Unlawful exploitation of personality rights, including name, image, likeness, voice and mannerisms. Creation and dissemination of AI-generated deepfakes causing reputational and personal harm. Unauthorized commercial use through impersonation and counterfeit merchandise. Threat to safety, dignity and public image arising from fabricated inflammatory content.	The Bombay High Court granted ex parte ad-interim relief, recognizing the plaintiff's exclusive proprietary rights over all identifiable personality attributes and restraining unknown entities and platforms from exploiting or disseminating such content. It directed immediate takedown and disabling of all infringing listings, pages, and materials.

Suniel V Shetty v. John Doe S Ashok Kumar (10.10.2025)

Suniel Shetty, a well-known actor and public figure, alleged widespread misuse of his personality attributes like his name, image, likeness, voice, signature and mannerisms across multiple online platforms. Numerous unidentified and identified entities created and circulated AI-generated deepfake images and videos depicting him and his family in obscene, false or misleading contexts. Others falsely used his persona for various media. Several impersonator accounts were also created on Meta and X. The plaintiff argued that these acts infringed his personality rights, privacy, dignity, commercial interests and misled the public.

Key Violations Found	Decision
Unauthorized creation and circulation of AI-generated deepfake videos and morphed images of the plaintiff. Misuse of his personality attributes Impersonation through fake social-media accounts and misleading advertisements/endorsements. Unlawful sale of merchandise using the plaintiff's identity. Violation of personality/publicity rights, right to privacy, and passing off through false association.	The Bombay High Court granted ex-parte ad-interim relief, restraining unknown entities, websites and social-media platforms from using or exploiting any of the plaintiff's personality attributes in any manner. It directed immediate takedown/removal/disablement of all infringing content and prohibited further misuse, acknowledging the severe reputational and personal harm caused by realistic AI-generated deepfakes.

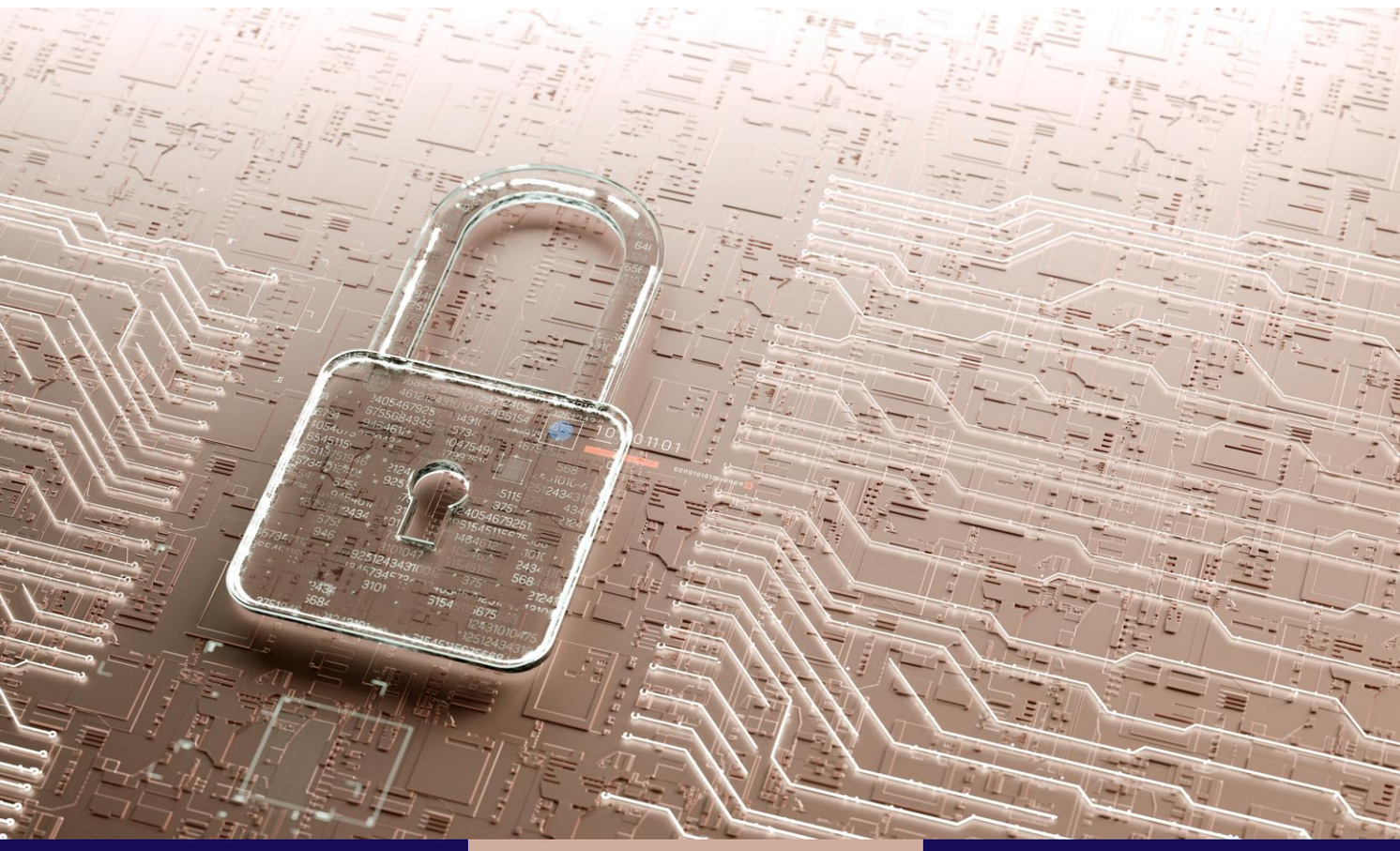
India

Court Room Updates

Dr. Ilaiyaraaja v. John Doe Ashok Kumar (20.11.2025)

Ilaiyaraaja, a legendary Indian music composer, filed a suit before the Madras High Court seeking protection of his personality rights after various media platforms and YouTube channels began using his name, images, photographs and AI-generated depictions without authorization. These included fabricated videos, memes and animated content portraying him in ways he never approved. His counsel argued that such misuse was being done for commercial gain, to attract viewers and earn revenue, thereby exploiting his identity and tarnishing his reputation. The Court examined screenshots and examples showing unauthorized and exploitative use of his persona.

Key Violations Found	Decision
Unauthorized commercial use of Ilaiyaraaja's name, photograph, likeness and identity. Creation and circulation of AI-generated images and animations depicting him without consent. Use of his persona to create memes and content that could tarnish his dignity and reputation. Misappropriation of personality attributes for revenue generation and public deception.	The Madras High Court held that Ilaiyaraaja established a prima facie case and granted an interim injunction restraining all defendants from using his name, image, photographs, comical or animated depictions, voice or any identifiable attributes without authorization. The Court directed the defendants to file their counter and recognized the risk of reputation damage and unauthorized commercial exploitation of his personality rights.



EUROPE

Court Room Updates

OC v. Commission (01.10.2025)

The case concerned a claim for non-contractual liability against the Commission arising from a European Anti-fraud Office (hereinafter referred to as "OLAF") press release issued on 5 May 2020. OC alleged that OLAF unlawfully processed her personal data, breached the presumption of innocence, and failed to respect principles of good administration and confidentiality during an ongoing investigation. The General Court found that OLAF's press release disclosed personal data and conveyed misleading information capable of harming OC's reputation, amounting to a sufficiently serious breach of EU law. The Court established causation and awarded OC EUR 50,000 in damages.

Key Violations Found	Decision
Unlawful processing and disclosure of personal data in an OLAF press release, breach of the presumption of innocence, failure to respect confidentiality and the duty of diligent, good administration.	Ordered for the European Commission to pay OC EUR 50,000 in compensation and bear all costs.

Inteligo Media SA v. ANSPDCP (13.11.2025)

In an important decision, the CJEU's First Chamber ruled that email newsletters qualify as direct marketing under Articles 13(1) and 13(2) of the e-Privacy Directive (2002/58/EC). Publishers obtaining user emails via free account creation, granting limited free articles, a daily legislative summary newsletter with hyperlinks, and optional paid access, do so "in the context of the sale of a service", even if indirectly remunerated through subscriptions.

Key Violations Found	Decision
Processing customers' personal data without consent. Sending newsletters as direct marketing without explicit consent	Administrative fine imposed for incompatibility with original purpose. The Court held such newsletters promote similar paid content, bypassing GDPR Article 6 consent requirements per Article 95 GDPR and e-Privacy specificity. Opt-out options at collection and per email suffice. Questions on "commercial communication" equivalence and fines were deemed inadmissible. It essentially ruled that the e-Privacy Directive takes precedence over the GDPR for direct marketing purposes.

X v. Russmedia Digital SRL and Inform Media Press SRL (02.12.2025)

In this case, the CJEU (Grand Chamber) ruled that the operator of an online marketplace that allows user-posted advertisements is a (joint) controller under the GDPR for the personal data published in those ads. It must therefore, before publication, implement measures to (i) detect sensitive data (ii) verify the advertiser's identity and whether they are the data subject, and (iii) refuse publication without explicit consent or another Art. 9(2) exception.

Key Violations Found	Decision
Whether an online marketplace operator violates GDPR by failing to act as a data controller for ads containing personal and sensitive data posted by users, and whether it can rely on the E-commerce Directive liability exemption.	The operator is a data controller, jointly responsible with advertisers, must ensure GDPR compliance (including identifying sensitive-data ads and preventing unlawful publication), and cannot invoke the E-commerce Directive liability exemption when acting as a controller.

United States of America

Court Room Updates

Holmes v. Elephant Insurance Co., (14.10.2025)

The case arose from a data breach at Elephant Insurance in which hackers accessed nearly 3 million driver's license numbers by exploiting the company's auto-populate quoting tool. Four named plaintiffs filed a consolidated class action alleging several injuries:

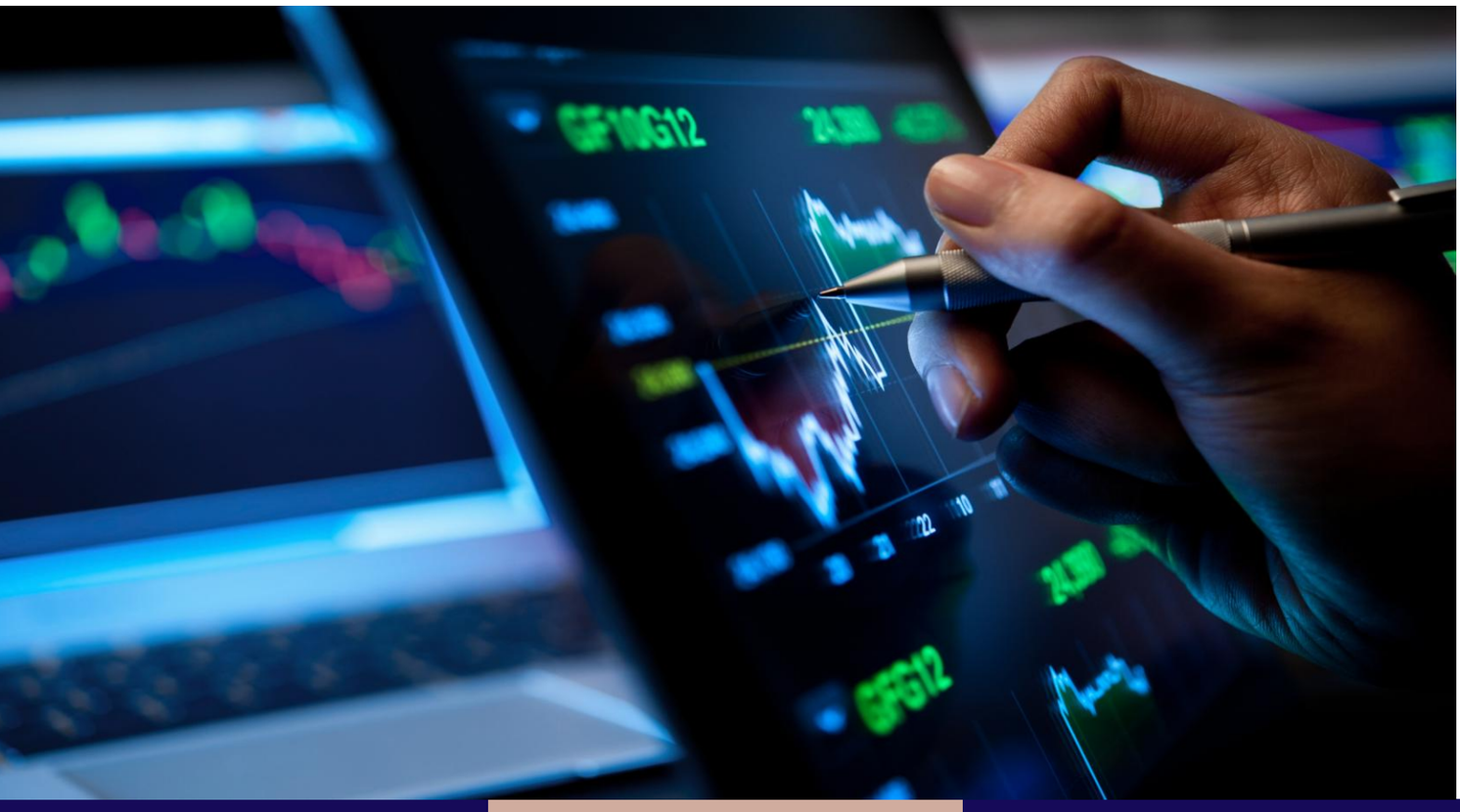
- Public exposure of sensitive data
- Increased risk of identity theft
- Emotional distress and time spent monitoring accounts

Key Violations Found	Decision
Exposure of driver's license numbers and related privacy harms.	Only plaintiffs whose data appeared on the dark web had standing, all others' claims were dismissed for lack of concrete injury.

Cole v. Quest Diagnostics, Inc. (13.11.2025)

The plaintiffs alleged Quest violated California's California Invasion of Privacy Act ("CIPA") and Confidentiality of Medical Information Act ("CMIA") by sending Facebook Pixel data from its websites, including the patient portal. The Third Circuit affirmed dismissal, holding that data sent directly by users' browsers did not constitute "interception" under CIPA, and merely revealing that a patient accessed test results was not "substantive medical information" under CMIA. Thus, no privacy violations were found, and the claims were properly dismissed.

Key Violations Found	Decision
Unauthorized interception of communications (CIPA) and disclosure of medical information (CMIA) via Facebook Pixel.	Affirmed dismissal. Browser-to-Facebook transmissions not "interception" and accessing results page not "medical information".



THANK YOU

For further queries/information please get in touch with us

Level 3,
No. 4/2, Millers Road,
Bangalore – 560052
admin@sdlaw.co.in | +91 8043779955