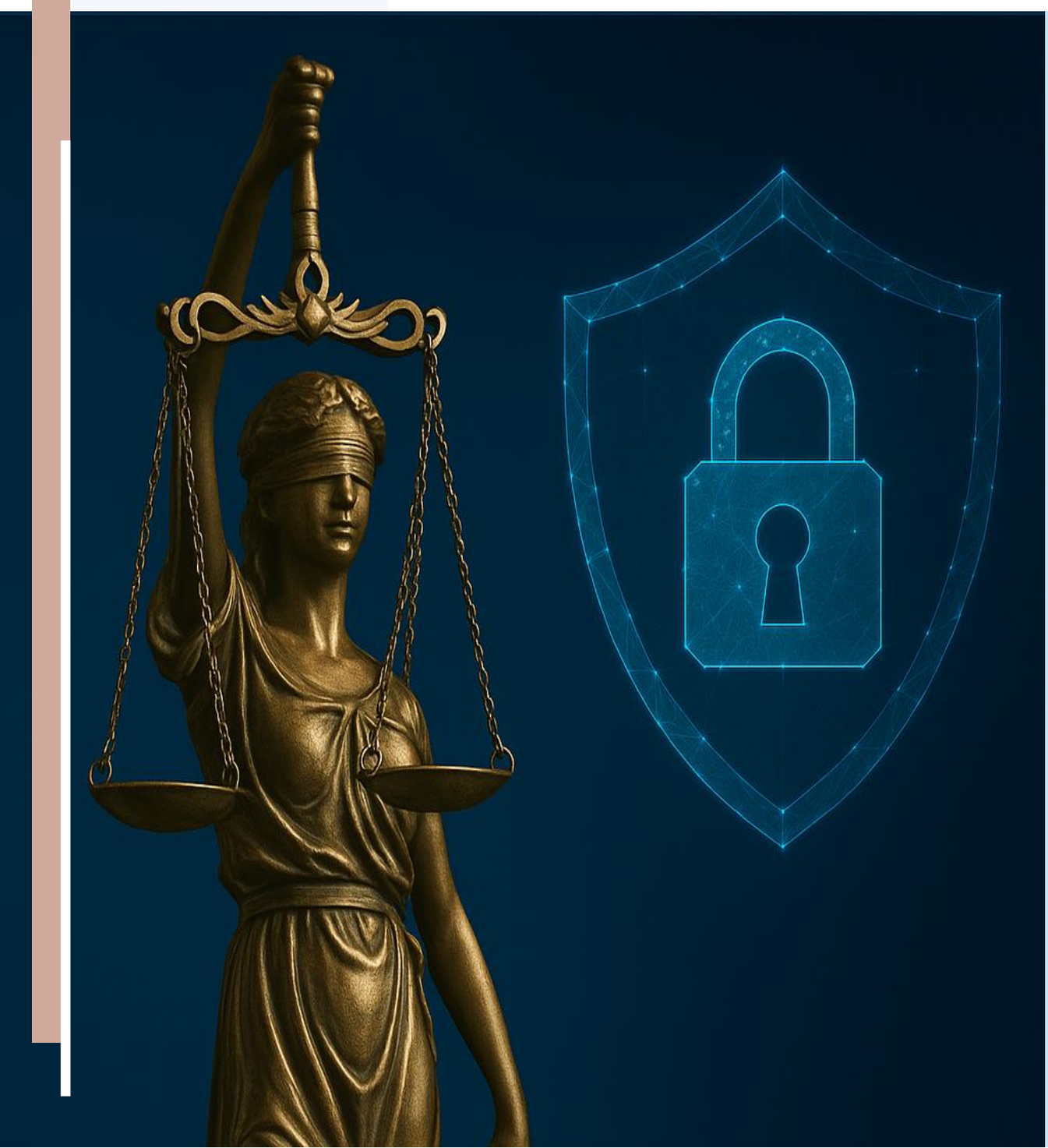
SHIVADASS & SHIVADASS®
LAW CHAMBERS

COMPETITION, DATA PROTECTION & PRIVACY SNIPPETS

2nd Ed.



Quarterly Update September 2025

INDIA

Judgments

CCI dismisses complaint against GMR Hyderabad International Airport Limited (GHIAL)

- The informant, Air Works India (Engg.) Pvt. Ltd., filed an information under Section 19 of the Act, alleging that GHIAL and its subsidiary GMR Aero Technic Ltd. (**GATL**), had abused their dominant position in violation of Sections 4(2) (b), (c) and (e) of the Act.

- The information alleged that GHIAL had unfairly denied renewal of its license to provide aircraft Line Maintenance Services (**LMS**) at the Airport and had demanded the informant to vacate its premises within the airport. It was alleged that GHIAL abused its dominance for benefitting its subsidiary and restrict competition, had denied market access by refusing licence renewal, and had leveraged dominance in its upstream market (provision of access to airport facilities/premises) to eliminate downstream competition (provisioning of LMS) where its subsidiary was competing.

- During the application to withdraw the information citing the lack of cause of action as it is able to continue its business at the airport. The CCI noted *vide* order dated December 6, 2013, that the proceedings before the CCI are not in nature of a *'lis'* between the parties but are proceedings *'in rem'*, having implications on the market and its various constituents/stakeholders, and that there are no provisions allowing withdrawal. Hence, the application was rejected.

- On merits, the CCI found that there was no adverse impact on the LMS market due to refusal to renew license of the informant as there were several players offering LMS (both with and without dedicated space within the airport) and that the informant was still able to provide LMS due to passes issued by GHIAL. It also noted that there was no denial of market access as GHIAL had exclusive power to take decisions to determine management and operations at the airport, and the decision was taken due to unavailability of space. The CCI also found that GHIAL was fair in its conduct and had not taken space from the informant to benefit its subsidiary, and that there was no evidence to suggest GHIAL had leveraged its dominant position to benefit its subsidiary in the downstream market.

Air Works India (Engg.) Pvt. Ltd. v. GMR Hyderabad International Airport Ltd., Case No. 30 of 2019

Bombay HC dismisses Writ Petition filed by Asian Paints against CCI order

- A Division Bench of the Bombay High Court dismissed a Writ Petition filed by Asian Paints challenging a Section 26(1) Order passed by the CCI directing the DG to investigate into allegations of abuse of dominance. The information, filed by Grasim Industries Ltd. (Birla Paints Division), alleged that Asian Paints had offered arbitrary discounts to dealers in exchange for exclusivity in stocking products of Asian Paints, and had restrained dealers, landlords, and transport agents from conducting business with the informant.

- The CCI identified the relevant product market as 'manufacture and sale of decorative paints in the organized sector' and the relevant geographic market as 'India'. Pursuant to the information being filed, Asian Paints submitted a letter making various submissions regarding the ease of entry in the decorative paints market and scale of expansion of the informant. The CCI formed a prima facie view that Asian Paints had engaged in abuse of its dominant position and directed the DG to commence investigation in Case No. 32 of 2024 vide order dated July 1, 2025.

- This order was challenged before the Bombay High Court by Asian Paints which contended inter alia that it should have been given an opportunity of being heard before the CCI passed its order. It also submitted that Section 26(2A) of the Act barred the CCI from re-inquiring into substantially similar complaints, as the matter was already investigated in a previous case, *i.e.*, ***JSW Paints Pvt. Ltd. v. Asian Paints Ltd. (Case Nos. 36 of 2019 and 17 of 2021)***

- The Court found that for Section 26(1) orders, the CCI exercises its administrative jurisdiction, and hence a hearing cannot be demanded as a matter of right. It further noted that at the 26(1) stage, the CCI's functions are preparatory and not adjudicatory in nature and the High Court is not competent to adjudicate the validity of such an order.

- On the second issue, the Court noted that Section 26(2A) was introduced in the interest of expediency and to avoid repetition of efforts already undertaken. The Court observed that the prior matter involved different issues and contraventions of different Sections of the Act. The prior proceedings were closed by the CCI due to inadequate evidence supporting the informant therein, and not on merits. The Court held that Section 26(2A) does not create a jurisdictional embargo on the CCI if the information is found distinct/different from the earlier representation. It also held that Section 26(2A) appears to be clarificatory and an enabling provision which only clarifies what was implicit in Section 26(2).

Asian Paints Ltd. v. CCI, Writ Petition No. 2887 of 2025

Supreme Court's observations in the Kerala Film Exhibitors Federation (KFEF) case

- An information was filed (in ***Case No. 16 of 2014***) by Crown Theatre alleging anti-competitive activities in violation by Sections 3(1) read with 3(3)(b) of the Competition Act, 2002, undertaken by KFEF and its office bearers. It alleged that film distributors were threated that their films would not be screened at cinema halls belonging to members of KFEF, if those distributors offered their films at Crown Theatre.

- The DG report found involvement and active participation of the President and General Secretary of KFEF in the alleged anti-competitive practices of KFEF. The CCI found that KFEF had violated Section 3(3)(b) of the Act, and its office bearers were liable under Section 48. The CCI imposed penalty of 10% of the average turnover and incomes of the KFEF and its President and General Secretary and directed them to cease and desist from engaging in anti-competitive conduct, and from associating with KFEF for a period of 2 years and vice versa.

- On appeal, the erstwhile COMPAT upheld the CCI's order on merits, but set aside penalty and directions qua the President and General Secretary as no specific opportunity was given to them to be heard on penalty.

- The Supreme Court held that in the present case, the CCI was in concurrence with the DG's Report, and hence a hearing notice constitutes sufficient compliance with the provisions of the Act for imposing penalty under Section 27 of the Act, especially since the original hearing notice was detailed. The Supreme Court set aside the order of the erstwhile COMPAT and restored the findings of the CCI.

- The Court also observed that imposing conditions to not associate with the KFEF is a part of behavioural and structural remedies contemplated by the Act, which are essential to ensure offenders comply with competition law in the future. It also noted that imposition of 10% average income as penalty was not disproportionate to achieving the objectives of the Act.

- Implications of the judgement are that there is no requirement for a separate penalty show cause notice for the pre-amendment period, especially when the hearing notice is detailed and identifies specific allegations and persons, as named in the DG report.

CCI v. Kerala Film Exhibitors Federation, Civil Appeal No. 9726 of 2016

NCLAT dismissed appeal against CCI order closing proceedings regarding export restrictions on beach sand minerals

- The information alleged violation of Section 4 on the grounds that DGFT and Indian Rare Earths Limited (IREL) restricted exports only through the IREL. The CCI found that the measure to channel exports through IREL is a matter of Government policy and pertained to the mineral's strategic importance in defence and nuclear applications.

- The NCLAT upheld the CCI's decision, emphasizing that the notification in question was a matter of government policy. The Tribunal noted that BSMs are classified as "atomic minerals" under the Mines and Minerals (Development and Regulation) Act, 1957, and as "prescribed substances" under the Atomic Energy Act, 1962. Due to their importance in defence and nuclear applications, the Tribunal concluded that the policy decision was outside the purview of competition law.

- NCLAT agreed with the CCI's reasoning that the measure related to Government policy and pertained to the minerals' strategic importance in defence and nuclear applications. It was further noted that the policy did not restrict business, but only channelled exports through IREL.

Beach Minerals Producers Association v. Government of India, Competition App. (AT) No. 48 of 2019

NCLAT concludes hearing in the WhatsApp/Meta case

- The National Company Law Appellate Tribunal (NCLAT) has concluded hearings and reserved its judgment on the appeals filed by Meta Platforms Inc. and WhatsApp LLC against the Competition Commission of India's (CCI) order dated November 18, 2024. The CCI had imposed a INR 213.14 crore penalty on Meta, ruling that the 2021 update to WhatsApp's privacy policy amounted to unfair business practices. Additionally, the CCI directed Meta to cease sharing user data collected on WhatsApp with other Meta companies for advertising purposes for a period of five years.

- In January 2025, NCLAT granted interim relief by staying the five-year ban on data sharing for advertising purposes. However, the NCLAT directed WhatsApp to disclose all purposes of data sharing, allow users to opt out of non-advertising data sharing, and deposit 50% of the penalty amount.

- NCLAT's forthcoming judgment will address significant regarding the intersection of competition law and data privacy, particularly concerning the jurisdiction of the CCI over data protection matters. WhatsApp has argued that data protection issues fall under the purview of specialized data protection authorities, not antitrust regulators like the CCI.

WhatsApp LLC v. CCI, Competition App. (AT) No. 1, 2 of 2025

Supreme Court admits appeals preferred by the CCI, Google, and Alliance Digital India Foundation (ADIF) against an order of the NCLAT

- The Supreme Court of India has admitted appeals filed by Google, the Competition Commission of India (CCI), and the Alliance of Digital India Foundation (ADIF) against a National Company Law Appellate Tribunal (NCLAT) order concerning Google's alleged abuse of dominance in the Android ecosystem.

- In 2022, the CCI imposed a ₹936.44 crore penalty on Google for mandating the use of its Google Play Billing System for app purchases and in-app transactions, while exempting its own applications like YouTube from similar commission structures. The CCI found that Google leveraged its dominance in the markets for licensable operating systems for smartphones and app stores for Android OS to unfairly promote its own services, such as Google Pay, thereby violating Section 4 of the Competition Act.

- The NCLAT, in March 2025, upheld the CCI's findings regarding Google's abuse of dominance but reduced the penalty to ₹216.69 crore, noting that the original fine was based on Google's global turnover rather than revenues from the Play Store. The tribunal also set aside certain findings of the CCI such as denial of market access, restriction of innovation, and certain preventative directions.

Alphabet Inc. v. CCI, C.A. No. 9644 of 2025)

Supreme Court dismisses SLP from Delhi High Court's (DHC) order in LPA No. 150 of 2020 and others

- The CCI had initiated investigations against Ericsson and Monsanto, alleging that their patent licensing practices violated Sections 3 and 4 of the Competition Act, 2002. The informants alleged that the companies were charging excessive royalties and imposing unfair licensing terms for their Standard Essential Patents (SEPs). However, both companies challenged the CCI's jurisdiction, asserting that such matters fell under the purview of the Patents Act, 1970.

- The DHC, in its 2023 judgment, ruled in favor of Ericsson and Monsanto. The court held that once a settlement had been reached between the informant and the opposite party, the very substratum of the CCI's proceedings was lost. Consequently, the DHC quashed the CCI's investigations, emphasizing that the Patents Act takes precedence over the Competition Act concerning patent rights.

- The Supreme Court upheld the DHC's decision. The apex court observed that since the original informants had settled their disputes with the companies and had "nothing further to say," the CCI's proceedings lacked a foundation to continue. However, questions of law in the case were left open to be agitated in some other appropriate case

CCI v. Monsanto Holdings Pvt. Ltd., S.L.P. (C.) No. 25026 of 2023

China

Regulatory

Updates to provisions on Prohibition of Monopoly Agreements, 2023

- Draft provisions have been introduced for public feedback to amend the safe-harbour rules for vertical agreements in the Prohibition of Monopoly Agreements, 2023.
- The 2023 provisions supplement the Anti-Monopoly Law which saw significant overhauls in 2022. They permit companies to enter into vertical resale pricing agreements under certain market share conditions. However, market share and turnover requirements were left undefined.
- The new amendments provide market share and turnover parameters under which a company is allowed to enter into vertical agreements to fix prices of resold goods. It also provides an application process to be exempted from antitrust investigations in respect of such transactions.
- **Impact**: Safe harbour regulations, reduce uncertainty for smaller entities in the supply chain engaged in resale or agency arrangements. Regulators gain a more explicit toolkit to assess vertical restraints

Updated Anti-Unfair Competition Law is set to be implemented in October

- In June, China introduced revisions to its Anti-Unfair Competition Law (AUCL) which will come into effect in October.
- The major updates include:
  - Dedicated abuse of dominance provisions, including platforms forcing vendors to sell below cost.
  - Platforms to define fair competition rules in agreements and policies.
  - Data scrapping and unauthorized data usage identified as unfair competitive behavior.
  - Fake orders, reviews and malicious returns included within the scope of unfair competitive behavior.
  - Clarifications on existing unfair competitive activities such as defamation, bribery, etc.
- The amendment also brought around extraterritorial jurisdiction clauses allowing enforcement for competitive actions taken abroad if they disrupt domestic markets or harm the rights of Chinese customers

United Kingdom

Regulatory

CMA advises Government to replace EU derived exemptions for technology licensing agreements

- The CMA submitted proposals to the UK Government to replace the EU-era Assimilated Technology Transfer Block Exemption Regulation (TTBER), which is due to expire in April 2026, and replace it with UK-specific regulations.
- The TTBER is a block exemption regulation that permits companies to share and license technology (including patents and software) without breaching competition law if conditions are fulfilled.
- The proposals form part of the UK's vision to streamline regulations to boost its economy. Technology transfer agreements generally benefit competition, but restrictive clauses may be harmful.
- Under the proposed regulations, agreements may qualify for exemption either by meeting market share thresholds, or by demonstrating the existence of competing technologies

Google provisionally designated as holding Strategic Market Status (SMS) in general search and search advertising services

- After an investigation initiated in January 2025, the CMA published its proposed decision in June 2025 on designation finding (provisionally) that Google holds SMS in general search and search advertising services.
- SMS designated entities are subject to conduct requirements imposed by the CMA. The CMA may also launch pro-competition interventions. Along with the proposed decision to designate Google, CMA also released potential conduct requirements and interventions it may impose if Google is designated.
- Notably, Google's Gemini AI has been excluded from the scope of the proposed designation as it is branded, accessed, and monetized separately. Standalone search services like Google Flights are also excluded.
- The provisional conduct requirements/interventions include category 1 measures such as: data portability while switching services, fair ranking of results, choice screens for default search engines, and publisher controls. There are also category 2 and 3 measures that may be consulted upon and implemented down the line.

Judgments

Visa and Mastercard's default multilateral interchange fees violate competition law

- The Competition Appeal Tribunal ruled that the global payment processors default multilateral interchange fees (**MIF**) which are charged to retailers when cardholders make a transaction, violate competition law.
- Various merchants who brought the action against Visa and Mastercard, argued that the MIFs are non-negotiable charges that are part of service fees paid by retailers to accept card transactions, and are a restriction under law.
- Visa and Mastercard argued that the MIFs supported secure payments and promoted competition. Negotiated fees may cause higher costs to be borne by retailers.
- The Tribunal relied on an earlier ruling in ***Sainsbury*** to hold that MIFs being collectively agreed upon and non-negotiable, and inherently anti-competitive.

Umbrella Interchange Fee Claimants v. Umbrella Interchange Fee Defendants, Case Nos: 1517/11/7/22 (UM), [2025] CAT 37

Brazil

Regulatory

Brazil submits Bill No. 4675/2025 to regulate antitrust concerns in digital markets

- In September 2025, Brazil's President submitted a bill to regulate antirust concerns in digital markets. It empowers the CADE to oversee and intervene in the operations "systematically significant" digital platforms.
- It targets identified anticompetitive practices such as self-preferencing and price abuse. It also requires:
  - data portability, interoperability, and integration of third-party applications
  - bans exclusivity clauses
  - provides mechanisms to examine acquisitions of start-ups, even if below thresholds
- Unlike the DMA, the bill emphasizes flexibility and proposes a quasi-regulatory model inspired from regulations in Japan, Germany, and the U.K., and empowers CADE to look into concerns on a case-by-case basis.

Europe

Judgments

Clarity on limitation period to claim damages for victims of cartels

- In September 2025, the CJEU rendered a judgment in ***Case C-21/24*** providing clarity on the limitation period for claiming damages. In 2015, the Spanish regulator CNMC, found various entities in the car manufacturing sector in violation of the Spanish Competition Act and Article 101 of the TFEU for exchanging commercially sensitive information.
- An applicant filed a follow-on action seeking damages caused due to one of the participants in the cartel – Nissan. Nissan resisted the challenge on the grounds that the right to claim damages had already expired under the Spanish Civil Code, and the claim must have been filed latest by September 2015, when the injured party became aware of the unlawful conduct.
- The question was referred to the CJEU by a Commercial Court to clarify at what point does the limitation period start in follow-on actions for damages, and whether the present claims are time-barred?

- The CJEU held that the limitation period for follow-on actions does not begin with publication of the decision by national authorities, but rather, when it becomes final in Court, i.e., in 2021 in the present case, when the Supreme Court dismissed the car manufacturers' appeals.

Cp v. Nissan Iberia SA, Case C-21/24)

United States

Judgments

Remedies imposed on Google after being found in violation of the Sherman Act

- The US District Court for the District of Columbia, in a landmark ruling in September 2025, imposed remedies to address Google's monopoly in search and advertising in search markets.
- Google was found in violation of Section 2 of the Sherman Act in 2024. Recently, the District Court imposed remedies to address its monopoly, which will be in place for the next 6 years.
- Remedies include:
  - Ban exclusivity contracts and practices to ensure Google's search engine is chosen as the default choice in desktops and mobile devices.
  - Ban on tying Play Store licenses and revenue sharing agreements to placement of search tools.
  - Google must provide competitors with access to search index and user-interaction data. This does not apply to ads data.
  - Offer search and search text ads syndication services to competitors on parity with current commercial practices.
  - Disclose any material changes to its ad auction process.
- The Court also ordered the establishment of a technical committee to assist implementation and enforcement of the judgment.

United States v. Google LLC, Case No. 20-cv-3010 (APM), Case No. 20-cv-3715 (APM0029)

INDIA

Regulatory

MeitY signals readiness to operationalise India's Data Protection & Cybersecurity Framework

- On 28 July 2025, Ministry of Electronics & Information Technology (hereinafter referred to as the "***MeitY***") confirmed that the public consultation on the *Draft Digital Personal Data Protection Rules, 2025* (under the Digital Personal Data Protection Act, 2023) has concluded, after receiving 6,915 responses from a diverse set of stakeholders.

- In parallel, MeitY is developing India's National Cybersecurity Strategy, focusing on strengthening institutional frameworks such as CERT-In, NCIIPC, etc., along with awareness & capacity building.

- Some key supporting programs: the ISEA programme (thousands of workshops, reaching 8+ lakh individuals), CyberShakti (women in cybersecurity), Cyber Swachhta Kendra, multilingual outreach, etc.

- Also relevant to note is that the DPDP Rules are still in draft stage. MeitY has only signalled the conclusion of consultation and is now reviewing responses. There is as yet no notification making the rules final.

- Until the rules are notified and the commencement date is fixed, the DPDP Act's provisions remain on hold in terms of enforceability.

- In August 2025, MeitY and the Competition Commission of India (CCI) held a meeting to deliberate the interface between data protection (DPDP) and competition law.

- The objective was to harmonise regulatory overlap in the digital economy, specifically, how data governance obligations under DPDP might intersect with market power / antitrust concerns under the Competition Act.

- The CCI, in its press statements, noted its willingness to align data governance with competition principles in light of technological trends.

- It may be pertinent to keep in mind in December 2024, in its Statement on Developmental & Regulatory Policies, the Reserve Bank of India (RBI) announced the formation of a committee to draft a Framework for Responsible and Ethical Enablement of AI (FREE-AI) in the financial sector.

The key features of the framework include:

- Setting up AI innovation sandboxes in the financial sector.
- Building shared data infrastructure and enabling indigenous AI models for the financial sector.
- Embedding governance, audit, explainability, transparency, consumer safeguards, and incident reporting in the AI lifecycle.
- Recommending adaptive / enabling policies and graded liability so that experimentation is not unduly hampered at early stages.
- Aligning with digital public infrastructure (e.g. integration with UPI / existing platforms) and designing audit frameworks.

Why does it matter?

Once the rules are notified, all entities handling digital personal data will face definite, enforceable obligations: consent, breach reporting, data fiduciary responsibilities, etc. Businesses should start internal reviews now: privacy notices, consent mechanisms, security practices, cross-border data flow policies, data mapping and audits. Watch for the final rules on "standard formats" (notices, breach reports, etc.), and when the Data Protection Board of India gets constituted.

INDIA

Regulatory

Pushback by Digital Payment players on consent clauses enshrined under the Digital Personal Data Protection Act, 2023 (DPDP Act)

- Leading digital payment firms including Google Pay, PhonePe, Amazon Pay and NPCI, have requested exemptions or relief from the compliance mandates under DPDP Act, specifically, that consent must be obtained for each individual transaction. An argument has been made by these entities that clause, as drafted, is operationally burdensome. ***[The Economic Times]***

- The concern is around scalability and user experience: requiring a separate explicit consent for every transaction, could slow down and complicate payments, possibly undermining digital payments adoption.

- It may be pertinent to note that this has parallels with the consent overload phenomena of the EU. Some examples are as follows:

    a) Under GDPR Article 7, consent must be freely given, specific, informed, and unambiguous. Recitals and guidance make clear that bundled consent or presenting many consent prompts can reduce the meaningfulness of consent. Consent for different purposes must be separate, and consent cannot be a precondition for accessing a service if that data processing is not necessary.
    b) More recently, there have been discussions by the European Data Protection Board (EDPB) about "consent-or-pay" models (e.g. services where users must accept tracking or pay a fee) and whether those models give a "real choice" or when they force consent due to lack of alternatives. This ties into questions of free consent (implied pressure, imbalance of power) and whether the model leads to consent becoming a formality without meaningful control.
    c) Also, there is concern (in EU practice and scholarly literature) about "consent fatigue" or "consent overload" where users are bombarded with frequent consent requests, notifications, pop ups etc., so they stop reading or distinguishing what they are consenting to. This reduces the efficacy of consent as a protection.

- Also, RBI's Authentication Mechanisms for Digital Payment Transactions, 2025 come into force from April 1, 2026, requiring two-factor authentication for all digital payments, with at least one factor being dynamic (transaction-specific) for non card-present transactions.

- For cross-border card-not-present (CNP) transactions, card issuers must implement validation mechanisms for non-recurring transactions from October 1, 2026.

- Payment service providers must reconcile RBI/PPI/NBFC compliance requirements with DPDP obligations, including consent, audit, and security mandates.

- RBI's Account Aggregator regime already uses a consent dashboard to record who is authorised and for which purpose, which may serve as a reference for DPDP "Consent Managers."

Implications

How MeitY responds to these comments, will determine whether digital payment companies must redesign their flows or seek alternative legal methods (if available), for processing transactional personal data.

Payment aggregators already face obligations such as information security, board-approved policies, audits, transaction limits, and grievance redress, creating potential overlap or conflict with DPDP Rules if RBI and MeitY mandates diverge.

Regulators will need to balance consumer protection (ensuring transparency and control) with practicality and efficiency for services, that rely on frequent micro-transactions.

INDIA

Regulatory

Concerns over journalistic freedom, RTI & 'Journalistic Purpose' exemption

Journalists, civil society and RTI activists, have raised two major concerns with the DPDP Act:

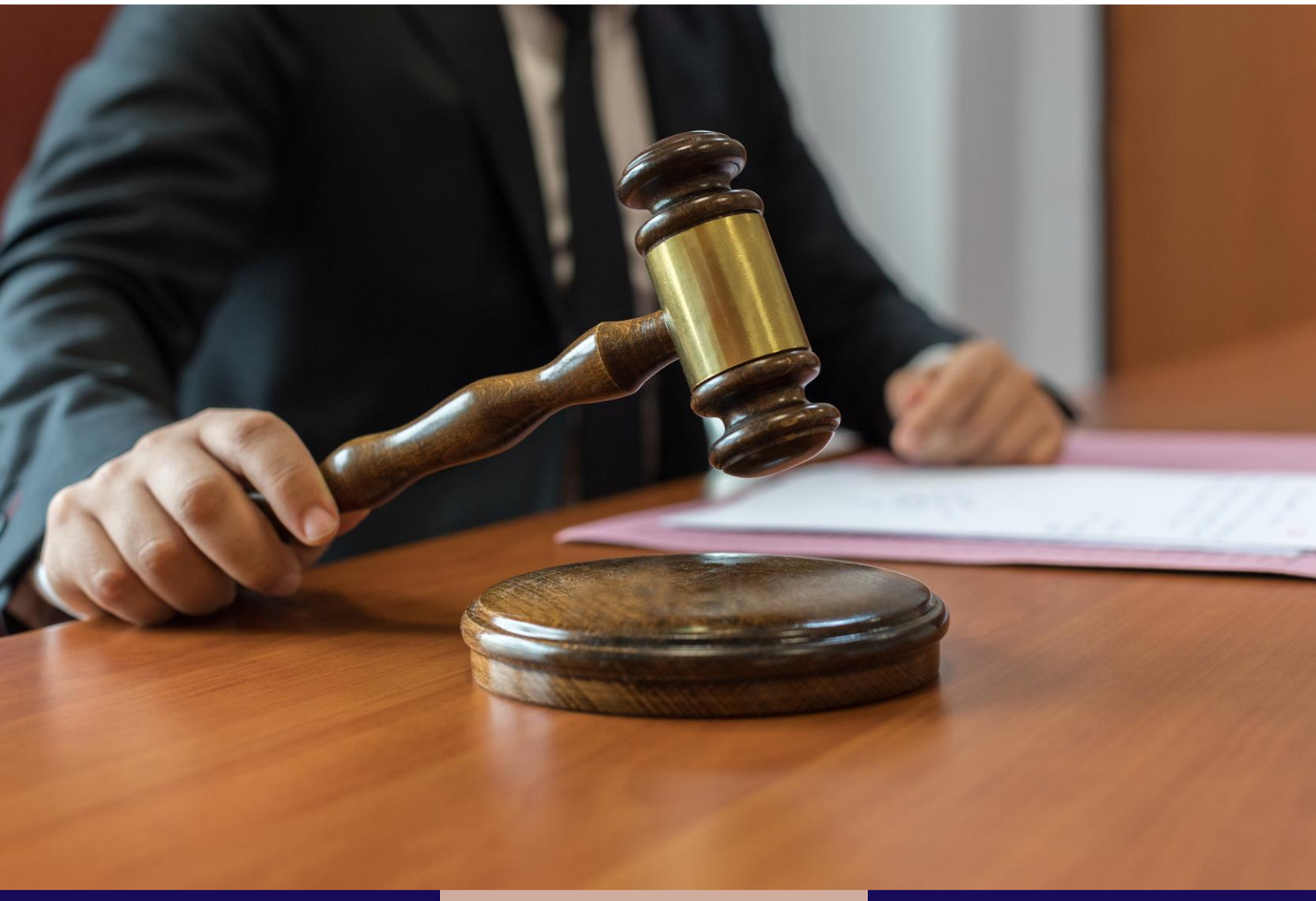
- The absence of a "journalistic purpose" exemption: Earlier versions of data protection bills had such provisions, allowing journalistic work to process personal data under certain conditions; the current DPDP Act does not.

- An amendment to Section 8(1)(j) of the Right to Information (RTI) Act via the DPDP Act, which broadly exempts "personal information" from disclosure. Critics argue that this undermines transparency and removes safeguards and public interest overrides.

MeitY's response: rather than seeking to amend the statute, it has proposed to issue FAQs to clarify how the law should be interpreted concerning journalistic freedom.

Why is this contentious?

FAQs / explanatory notes are not law; they do not override or change statutory text. For journalists and activists, the lack of formal exemption and removal of the RTI override, raises risks of chilling effects suppressing investigative reporting, whistleblowing, transparency, etc.



INDIA

Judgments

Karnataka High Court on caste survey and privacy concerns (WP 28665/2025)

Aadhaar concerns:

- Petitioners argued that use of Aadhaar for verification in the survey, violates the Aadhaar Act, especially since Section 57 was deleted in 2019.
- Court noted Commission's stand that Aadhaar is only for identity confirmation to avoid duplication, and disclosure is optional.

Right to Privacy under Article 21:

- Petitioners stressed that collecting detailed personal data (religion, caste, income, property, indebtedness, marital status, disabilities, etc.), infringes citizens' privacy as recognised in *Justice K.S. Puttaswamy v. Union of India*.
- Court acknowledged the sensitivity of information and emphasized the need for strong safeguards.

Court's protective directions on privacy:

- Data collected shall not be disclosed to anyone, including the Government and only the Commission may access it.
- No one is obliged to provide Aadhaar details or respond to survey questions and participation is voluntary.
- Enumerators must inform participants upfront that the survey is optional.
- If a participant refuses, enumerators cannot pressurize them further.
- Commission must file an affidavit within one working day confirming measures for confidentiality and data security.
- Court directed the Commission to issue public notices making the voluntary nature of the survey clear.
- Data collected cannot be repurposed or used beyond the survey's stated
- objective.

EUROPE

Regulatory

EU AI Act

The European Parliament passed the EU AI Act and the same has been enforced with effect from August 1, 2024. Since its inception, the Regulations were set to be implemented in stages. A significant milestone in 2025 was reached on August 2, 2025, when governance rules and obligations for providers of general-purpose AI (GPAI) models became applicable. However, the Act will not be fully applicable until August 2, 2026, with high-risk AI systems in products having until August 2, 2027, for full compliance.

Interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR): European Data Protection Board (EDPB) adopts Guidelines

On September 12, 2025, EDPB adopted Guidelines 3/2025, clarifying how the DSA and GDPR interact. These are the first Guidelines tackling how both the digital regulatory regimes overlap.

The Guidelines address provisions of the DSA that involve processing personal data, especially by "intermediary service providers" such as platforms and search engines. Key areas of overlap include:

- Notice-and-action systems for reporting illegal content
- Recommender systems (how content is surfaced, profiling involved, the user choice)
- Protection of minors (profiling-based ads especially, privacy & safety obligations)
- Transparency of advertising; and
- Prohibition of profiling-based advertising using special categories of data

The Guidelines also underscore the need for cross-regulatory cooperation: between data protection authorities (GDPR regime), Digital Services Coordinators (DSA regime), and the European Commission, to ensure consistent interpretations and avoid regulatory gaps or conflicting obligations.

These Guidelines are open for public consultation until October 31, 2025. Stakeholders are invited to comment.

Why does it matter?

For EU-based platforms, online services, and intermediaries, these Guidelines will shape compliance strategy: how to design systems (recommendation engines, ad targeting, notice-action mechanisms), so that one may satisfy both GDPR and DSA requirements.

Crucial is how minors are treated, and how to ensure transparency in ads.

There may be operational challenges: e.g., how to provide alternatives when recommender systems profiling is involved; how to document / justify profiling or use of sensitive categories; what constitutes legal basis under GDPR when DSA obligations impose processing.

EDPB & EDPS Opinion on Targeted GDPR Amendments

The EDPB and European Data Protection Supervisor (EDPS), issued a joint opinion on the European Commission's proposals to simplify certain GDPR obligations, for example, reducing / easing record-keeping burdens for SMEs.

They welcome simplification in general, but stress that any changes must be accompanied by clear safeguards, so privacy protections are not weakened. For instance, simplifications must still ensure accountability, auditability, transparency, rights of data subjects (access, objection, etc.) remain robust.

EUROPE

Regulatory

Italy enacts AI Law covering Privacy, Oversight and Child Access

Italy's parliament approved a sweeping AI law aligned with the EU AI Act, setting national rules for transparency, traceability and human oversight of AI, across healthcare, work, education, justice and public administration.

The law requires parental consent for users under 14, limiting minors' direct access to certain AI services.

The Agency for Digital Italy and the National Cybersecurity Agency are given central roles, while sector regulators (e.g., Bank of Italy, Consob) keep their powers. Misuse (e.g., harmful deepfakes, AI-enabled fraud/identity theft) carries criminal penalties.

The law backs a state-linked fund (reported ~€1 billion) to invest in AI, cybersecurity and related tech, though some critics say funds are modest versus global competitors.

EU Court Upholds Europe-U.S. Data Transfer Accord

A court in the EU has upheld the current data transfer framework / accord between Europe and the U.S., reaffirming its validity. This helps maintain legal certainty for cross-border transfers from EU to U.S., but oversight and adequacy mechanisms will continue to be watched closely.

EU CHAT CONTROL LAW

EU's proposal for a Regulation to Prevent and Combat Child Sexual Abuse mandates service providers including end-to-end encrypted communication and storage services to scan all communications and files to detect child sexual abuse material.
The proposal details duties related to assessing risks, applying mitigation strategies, and, if required by competent authorities, identifying, reporting, and removing child sexual abuse material (CSAM) and possibly grooming activities.
The proposal contradicts GDPR principles such as data minimization and lawful processing, as it involves scanning vast amounts of sensitive data without specific suspicion.
The proposal undermines EU's efforts to promote privacy and interoperability in the digital market.
On October 14th, the European Council is likely to vote on the proposed Regulation.

EUROPE

Judgments

XYZ v. Online Platform **(September 15, 2025)**

The platform blocked access to essential services unless users consented to tracking cookies. The CJEU emphasized that consent must be freely given, informed, and revocable, striking down coercive practices.

Key Violations Found	Decision
Users were forced to accept cookies to access content, with no genuine alternative.	Such "consent walls" are **unlawful** unless users have a genuine opt-out option.

ABC v. Data Exporter **(September 3, 2025)**

The High Court of Ireland examined whether SCCs adequately protected EU personal data in third countries. It confirmed that risk assessment and additional safeguards are mandatory to prevent unlawful exposure.

Key Violations Found	Decision
Reliance solely on Standard Contractual Clauses (SCCs) to transfer personal data to a country with extensive government surveillance.	SCCs alone are insufficient; controllers must implement supplementary measures.

DEF v. Credit Platform **(August 28, 2025)**

AI was used to automatically reject job candidates and deny loans. The Tribunal de Grande Instance de Paris (France) reinforced that data subjects have the right to human review and explanation.

Key Violations Found	Decision
Fully automated recruitment and credit scoring without meaningful human intervention.	GDPR Article 22 prohibits such decisions without human oversight; individuals must be able to contest outcomes.

GHI v. Social Media Platform **(July 12, 2025)**

Pre-checked boxes and confusing UI were used to obtain consent for behavioural advertising. Higher Regional Court of Munich, Germany invalidated such consent, emphasizing users' free choice cannot be undermined by design.

Key Violations Found	Decision
Use of pre-checked boxes and interface tricks to obtain consent.	Consent must be active, explicit, and freely given; manipulative designs are prohibited.

EUROPE

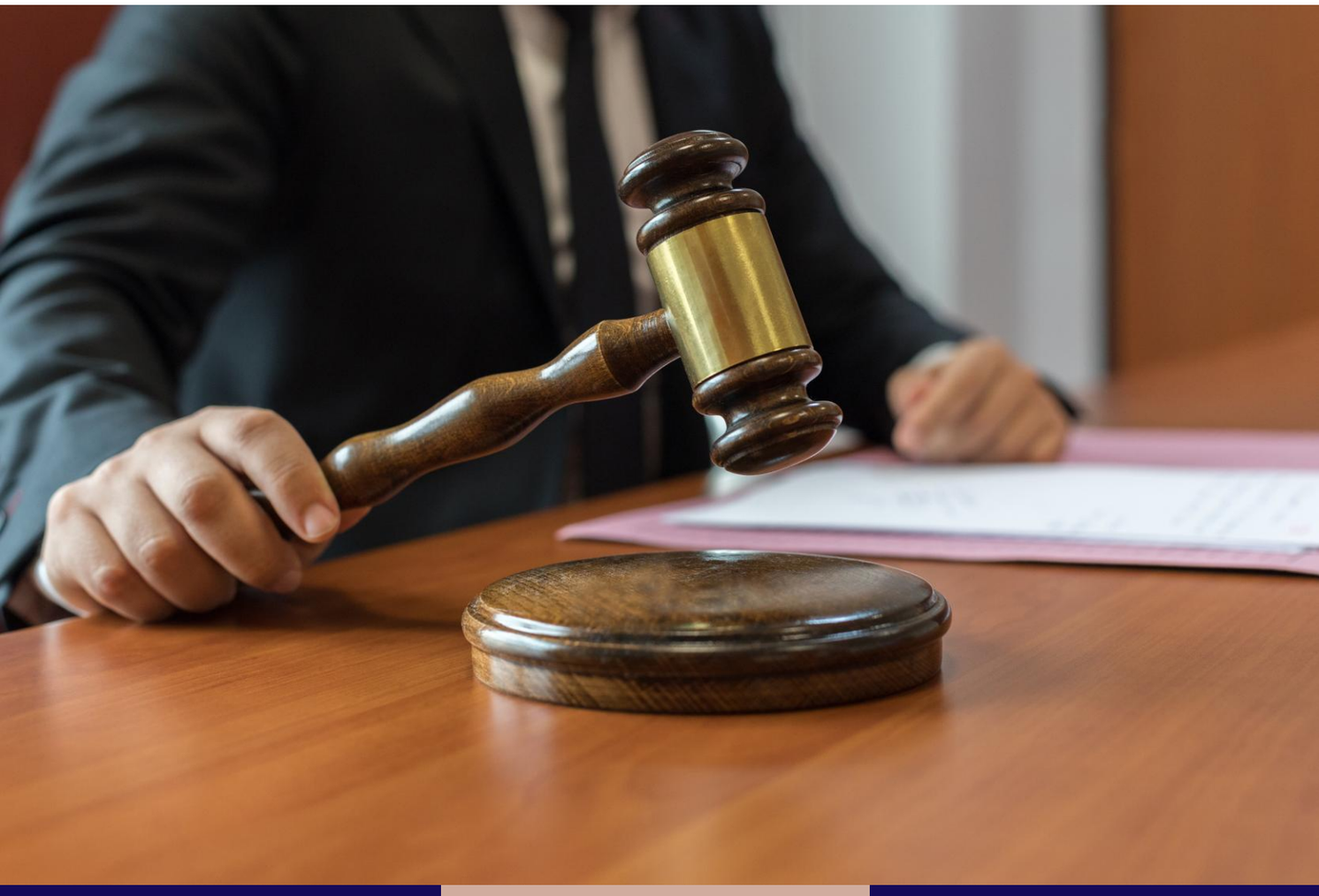
Judgments

JKL v. Online Education Platform **(August 6, 2025)**
The platform collected data from children without parental involvement. Audiencia Nacional (Spain) emphasized heightened protection for minors and mandatory consent mechanisms.

Key Violations Found	Decision
Collection of children's data without age verification or parental consent.	GDPR requires verifiable parental consent for minors under 16 and clear privacy notices.

Latombe v. Commission **(September 4, 2025)**
French MEP Philippe Latombe challenged the European Commission's **2023 adequacy decision** on the EU-US Data Privacy Framework, arguing U.S. surveillance laws still failed to meet GDPR standards for equivalent protection.

Key Violations Found	Decision
U.S. intelligence practices allegedly lacked sufficient safeguards, undermining EU citizens' rights under GDPR.	The General Court **dismissed the challenge**, holding that the U.S. ensures an **adequate level of protection**, with oversight via the new **Data Protection Review Court (DPRC)**. The framework therefore remains valid.



USA

Regulatory

Increase in State Privacy Laws effective 2025

Several States within the USA, have passed new consumer privacy / data protection laws that came into effect in 2025 (e.g. Tennessee Information Protection Act, Minnesota Consumer Data Privacy Act, etc.). These impose obligations around consumer rights (access, deletion), opt-out of targeted advertising, data minimization, etc.

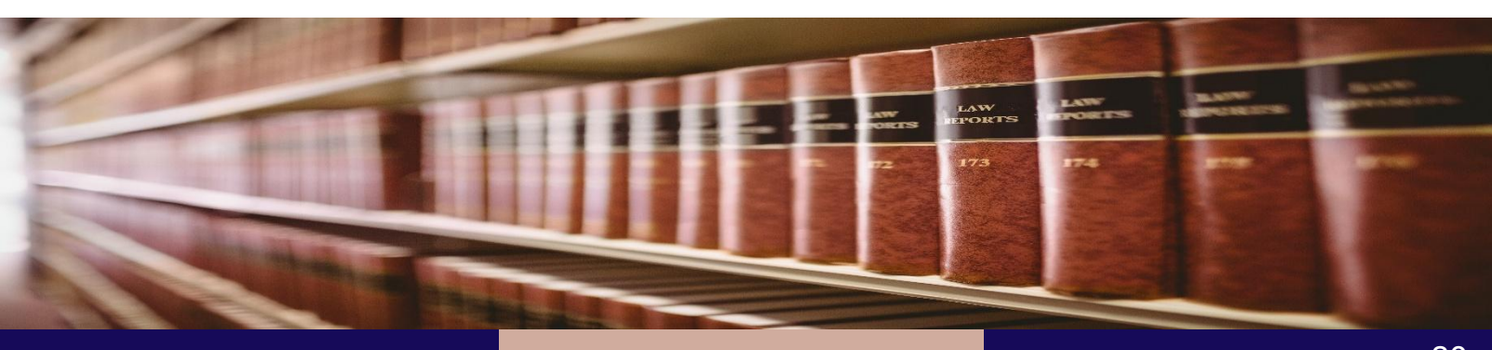
This means businesses operating across multiple States, now face increasingly complex compliance landscapes.

CCPA finalizes regulations governing use of Automated Decision-Making Technologies (ADMT)

Regulation of Automated Decision-Making Technology (ADMT):
"ADMT" is now broadly defined to include systems that replace or substantially replace human decision-making.
Businesses must disclose to consumers when ADMT is used, including the logic, significance, consequences, and consumer rights.
Consumers will have the right to opt out of ADMT being used for "significant decisions" (e.g. decisions about employment, healthcare, credit).
At least two methods must be offered to consumers for submitting opt-out requests.
Businesses using ADMT before January 1, 2027 must bring themselves into compliance by that date.

Risk Assessments
Employers must conduct a risk assessment before deploying ADMT for significant decisions.
The assessment must evaluate whether privacy risks outweigh benefits, and consider factors such as logic, safeguards, negative impacts, and mitigation.
It must be documented, approved by an executive, and updated every 3 years or sooner upon material change.
Employers are required to submit summary information of risk assessments to the authority, and provide full assessments on request.

Pre-Use Notice & Transparency
Prior to collecting data for ADMT, employers must provide a pre-use notice explaining:
The purpose of the ADMT
- How it makes decisions
- Categories of personal information used
- Types of outputs
- How outputs are used in decisions
- The rights to access, opt out, appeal, and non-retaliation



USA

Regulatory

OpenAI tightens rules on sensitive queries amid teen concerns

Amid growing concern about teens accessing sensitive content via AI systems, OpenAI has introduced stricter rules / controls on what kinds of sensitive queries are allowed / how they are handled.

OpenAI is rolling out new protections for users it believes are under 18. It's building an age-prediction system to estimate whether someone is a teen, and if there is doubt, the system will default to the under-18 user experience.

For users identified (or assumed) to be minors, graphic sexual content and flirtatious exchanges will be blocked and discussions of suicide or self-harm will not be allowed, even in a creative or fictional setting.

Parental controls are being added wherein parents (for users 13+), will be able to link their accounts, disable features like memory or chat history, set usage limits or "blackout" times, and receive alerts if the system thinks a teen is in acute distress.

Adults may need to verify their age (via ID in some regions) to access full/unrestricted features if the system thinks they are underage or if age is uncertain.

These changes are largely being driven by concerns over teen mental health and safety, including a high-profile lawsuit by the family of a 16-year-old who took his own life, alleging problematic interactions with ChatGPT.

Proposal for an AI "Sandbox" by Sen. Cruz

U.S. Senator Ted Cruz has proposed an "AI sandbox" model for essentially providing regulatory relief / controlled experimentation framework for tech companies intended to ease regulatory burdens while still maintaining oversight.

Judgments

Google Class Action – $425 Million Jury Award (August 2025)

US District Court found that Google continued collecting user data even when users disabled "Web & App Activity."

Key Violations Found	Decision
Privacy controls misleading; unauthorized collection of personal data.	Jury awarded **$425 million** to a class covering ~98 million users and 174 million devices. No punitive damages imposed (no finding of malice). Google plans to appeal.

State of Texas v. Google **(September 2025)**

Texas alleged Google misled users by:

- Collecting location data when tracking was "off"
- Collecting biometric identifiers (voiceprints, facial geometry) without consent
- Misleading users about privacy of **Incognito Mode**

Key Violations Found	Decision
Violations of Texas consumer protection & privacy statutes.	Settlement of **$1.375 billion** reached (pending final approval). Google denies wrongdoing; no product changes required.

USA

Judgments

Google Class Action – Pre-Trial Ruling on "Surveillance" (July 2025)
In a class action alleging misuse of Android data, plaintiffs sought to argue Google's practices amounted to "surveillance."

Key Violations Found	Decision
Framing user data transfers as unlawful surveillance.	Judge barred plaintiffs from using "surveillance" framing or arguing the case was "lawyer-driven." Trial limited to concrete statutory/contractual violations.

California Courts – Divergence on Personal Jurisdiction Ongoing (July–Sept 2025)
Courts split on whether out-of-state defendants can be sued in California for privacy violations.

Key Violations Found	Decision
Applicability of California jurisdiction over nationwide websites engaging in geolocation targeting or privacy disclosures.	One court: Nationwide website + geolocation targeting = sufficient for jurisdiction. Another court: Reached opposite result. Uncertainty persists until further Ninth Circuit or Supreme Court guidance.

Facebook (Meta) Privacy Settlement – Cambridge Analytica (September 2025 (Payouts Begin)
$725 million settlement approved in 2023 for Cambridge Analytica data-sharing scandal.

Key Violations Found	Decision
Improper sharing of Facebook user data with third parties.	Settlement fund distribution to eligible U.S. Facebook users began in September 2025. Meta denied wrongdoing.

California AG v. Healthline Media LLC – CCPA Settlement (September 2025 -Settlement pending court approval)
Healthline shared sensitive user data (article titles revealing diagnoses) with advertisers despite opt-outs.

Key Violations Found	Decision
Failure to implement opt-out mechanisms under **CCPA** Inadequate third-party contracts	**Penalty:** $1,550,000 **Injunctive Relief:** Ban on sharing article titles revealing medical conditions. Mandatory consumer notices & opt-out options. Full CCPA compliance on data sales/sharing **Compliance Program:** 3 years, with annual AG reporting.

VIETNAM

Regulatory

Vietnam's National Assembly has passed Personal Data Protection Law (PDP Law), which becomes effective on 1 January 2026, replacing the earlier Decree 13/2023. PDP Law imposes stricter penalties, including revenue-based fines for illegal data use and cross-border transfers, along with tougher rules for sensitive data and consent. It also introduces sector-specific regulations and offers temporary exemptions and transitional arrangements for startups, SMEs, and microenterprises.

ISRAEL

Regulatory

Israel's Amendment 13 to the Privacy Protection Law which came into effect on August 14, 2025 gives the Privacy Protection Authority (PPA) stronger enforcement powers, including monetary penalties, administrative orders, sectoral audits, and even criminal liability, marking a shift toward a more robust regulatory regime.

UAE

Regulatory

In July 2025, the Dubai International Financial Centre (DIFC) updated its Data Protection Law to align more closely with global standards like the GDPR. The amendments expand the law's extraterritorial scope, introduce a private right of action allowing individuals to sue for damages, and increase penalties for non-compliance such as fines for failing Data Protection Impact Assessments or omitting annual assessments. These changes aim to strengthen enforcement and accountability within and beyond DIFC.

QATAR

Regulatory

Privacy violations via technology (sharing/taking photos, audio, videos without consent) now carry up to 3 years jail and/or fine up to QR 100,000 (approximately INR 23,00,000), as outlined in Article 8-bis added to the Anti-Cybercrime Law.

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