FOUNTAINHEAD LEGAL

FOUNTAINHEAD LEGAL

TECHNOLOGY & DATA PRIVACY BULLETIN

Insights on Technology Law, Data Protection & Digital Governance

IN INDIA	US UNITED STATES	EU EUROPEAN UNION	OTHERS

MONTHLY EDITION **[OCTOBER 2026]**



FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

October's developments brought an interesting contrast in technology regulation. While Governments continued to develop frameworks for responsible AI and data sharing, incidents involving established financial and digital infrastructure raised a more immediate question: how prepared are organisations to manage the risks arising from technologies they already use?

In India, the Kerala High Court's observations regarding the operationalisation of the Data Protection Board marked an important development. With Consent Manager registration scheduled to commence in November, the focus is gradually shifting from legislation and rulemaking to the institutions responsible for administering the DPDP framework. The Board's ability to function will be significant in translating the law's provisions into an effective regulatory mechanism. At the same time, SBI's disclosure of suspected customer data exposure and eMudhra's certificate-security incident highlighted two different dimensions of digital risk. While the SBI incident raised concerns around the protection of customer information, the eMudhra incident demonstrated how weaknesses in digital trust infrastructure could affect businesses relying on it. Both developments underline the importance of identifying vulnerabilities, responding promptly and containing potential consequences before they escalate.

The discussion around AI governance is developing along similar lines. TRAI's proposed Guidelines on responsible AI use in telecommunications contemplate risk classification, board-level oversight, supplier accountability and incident management. MeitY's DEPA Handbook, meanwhile, explores how valuable datasets could be made available for AI training through contractual permissions and controlled technical environments, without necessarily transferring the underlying data. Together, these developments reflect an effort to enable AI innovation while introducing greater accountability over how data and technology are accessed and used.

International developments reinforce this direction. The European Commission's proceedings against Booking.com illustrate how platform accountability extends to fraudulent listings, phishing risks and advertising transparency. Enforcement actions concerning difficult privacy opt-outs, undisclosed tracking and subscription practices similarly demonstrate that regulators are looking beyond written policies to examine how digital services actually operate and how users experience them.

The common thread is accountability in practice. Whether an organisation is protecting customer information, relying on digital infrastructure, deploying AI or operating an online platform, regulatory attention is increasingly directed towards how safeguards function in real situations. Policies and contractual commitments remain important, but businesses must also ensure that the systems supporting them work as intended.

This edition explores these developments and the emerging expectations they create for businesses navigating an increasingly interconnected digital environment.

As we conclude this edition, we extend our warm wishes to you and your loved ones for a joyous and prosperous Diwali. May the festival of lights bring happiness, new opportunities and continued success.

Wishing you a Happy Diwali and an insightful read!



IN THIS ISSUE

TABLE OF CONTENTS

INDIA 05

- SBI reported Suspected Exposure of Customer Data on Dark Web
- ED searched Crypto Platforms over Suspected FEMA Violations involving Stablecoins
- TRAI proposed Guidelines on Responsible Use of AI in Telecommunications
- MeitY unveiled Handbook on Data Empowerment and Protection Architecture for AI Training
- eMudhra announced Exit from Global TLS Certificate Business following Weak-Key Incident
- Kerala High Court directed Data Protection Board to be Operational within Eight Weeks
- Supreme Court directed National CSEAM Database and Proportionate Online Child-Safety Safeguards
- Delhi High Court held Writ Jurisdiction cannot be invoked for Online Account Dispute against Private Platform

UNITED STATES OF AMERICA 09

- FTC launched Study of Personalised Consumer Pricing and Platform-Worker Pay
- California AG announced USD 1.8 million Lyft Settlement over Privacy Opt-outs
- FTC and States sued Restaurant Software and FinTech Firm over Alleged Hidden Fees and Cancellation Barriers
- FTC sued Sextortion-Relief Provider over Alleged Deceptive Practices
- US Copyright Office opened Consultation on Digital-Lock Exemptions

EUROPEAN UNION 12

- European Commission opened DSA Proceedings against Online Travel Booking Platform
- European Commission initiated First AI Act Information Requests to Model Providers
- EDPB issued Statement on Privacy Risks from Smart Glasses
- CNIL fined FNAC Companies over App Tracking without Consent

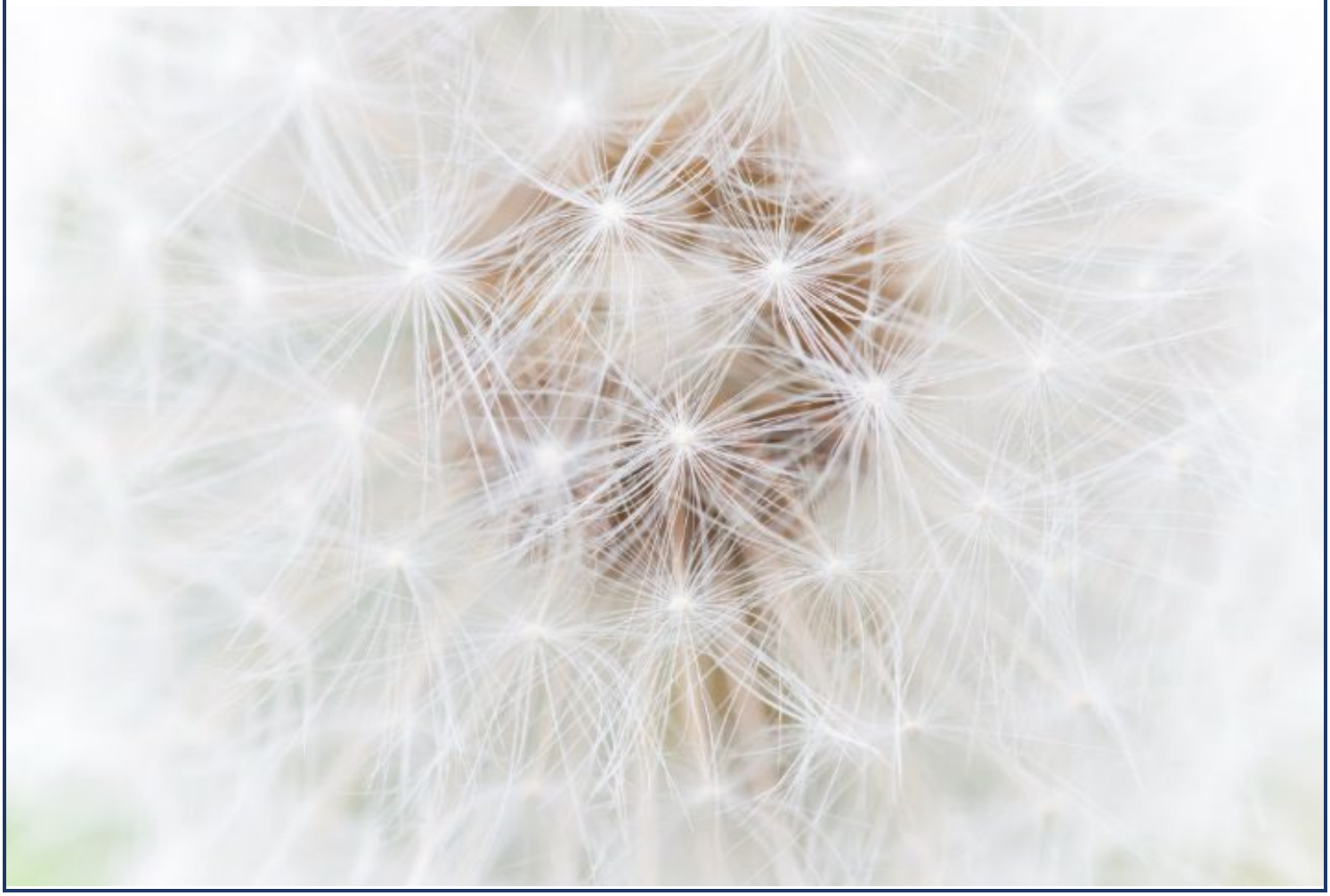
OTHER COUNTRIES 15

- UK ICO sought Evidence on Data-Protection Risks of Agentic AI
- Australia's Lower House passed Digital Duty of Care Bill
- Australia's Privacy Regulator investigated Smart-Glasses App Developer
- Canada proposed Children's Privacy Code for Online Services
- Canada updated Guidance on Recording Customer Telephone Calls
- OECD launched Repository on Privacy-Enhancing Technologies

ABBREVIATIONS **17**

ABOUT THE FIRM **19**

CONTACT US **20**



| INDIA



1	**SBI reported Suspected Exposure of Customer Data on Dark Web**[1] SBI disclosed to the stock exchanges on 21 October 2026 under the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 that it had been alerted to a suspected exposure of customer data on the dark web. Its preliminary examination of approximately 375,000 records identified 3,897 customer records containing personal data, including names, mobile numbers, dates of birth, addresses, branch and customer identifiers, and loan-related information. The nature and source of the exposure remained under investigation. SBI activated its incident-response procedures and appointed an independent CERT-In-empanelled agency to determine the authenticity, source and extent of the exposed data. It reported no material impact on operations or business continuity. Its disclosure did not establish how the incident occurred or whether affected customers had been individually informed. Nor did it confirm any compromise of account credentials or funds. *The business concern extends beyond financial loss: combined contact, identity and loan information can increase phishing and impersonation risks. Organisations should review access to customer and lead databases, third-party data sharing, monitoring of unusual exports, breach escalation and customer communication plans. This will help align with the obligations under DPDP Regulations as well.*
2	**ED searched Crypto Platforms over Suspected FEMA Violations involving Stablecoins**[2] ED conducted searches on 27 October 2026 under FEMA involving entities associated with Mudrex, Saber.money and Instadapp/Fluid, over suspected unauthorised cross-border payments using USDT and USDC stablecoins. It alleged that overseas entities and exchange accounts were used to facilitate transfers without the requisite RBI authorisation. ED estimated suspected contraventions exceeding INR 4,600 crore in one part of the investigation.

[1] https://nsearchives.nseindia.com/corporate/SBIN_21102026084938_BSE_NSE_21102026.pdf , last accessed on Nov 04, 2026
[2] https://enforcementdirectorate.gov.in/media/press-release-documents/fec4fc44-8df0-4d87-94cf-c43a3a856165_Press%20release%20%20_5.pdf , last accessed on Nov 04, 2026

ED also cited a preliminary figure of approximately USD 40 million in relation to Instadapp/Fluid. These remain allegations under investigation, not findings of liability. Mudrex has reportedly maintained that it is compliant and registered with FIU-India.

The key distinction for crypto and fintech platforms is that FIU-India registration for anti-money-laundering purposes is not, by itself, an authorisation for cross-border payments under FEMA. Businesses should examine who sends and receives value, the role of overseas entities, settlement flows and whether their services require separate regulatory approvals.

3 **TRAI proposed Guidelines on Responsible Use of AI in Telecommunications**[3]

TRAI released the *Draft Guidelines on Responsible Use of Artificial Intelligence (AI) in Telecommunication Networks and Provision of Telecommunication Services* (**"Draft Guidelines"**), inviting comments until 27 November 2026. The Draft Guidelines are intended for telecom licensees and authorisation holders that deploy or plan to deploy AI in networks and services, including outsourced AI solutions.

The Draft Guidelines propose a board-approved AI policy, annual review, risk classification of AI systems, pre-deployment testing and documented human oversight. Operators would establish an AI governance and safety committee, classify and report significant AI incidents, maintain grievance mechanisms and records of AI-related harms, and secure audit and inspection rights in supplier contracts. Importantly, operators would remain accountable even where an AI system is supplied by a vendor.

This would move AI oversight from technology teams to board-level governance for telecom operators. Network optimisation, customer support, fraud detection and other AI use cases may require inventories, risk assessments, escalation procedures and stronger procurement terms. AI vendors serving operators would also be affected through contractual controls. The Draft Guidelines remain consultative; their binding status and certain reporting timelines require clarification.

4 **MeitY unveiled Handbook on Data Empowerment and Protection Architecture for AI Training**[4]

MeitY unveiled the Handbook on Data Empowerment and Protection Architecture (DEPA) for AI Training (**"DEPA"**). DEPA is a proposed techno-legal approach to making valuable datasets available for AI development while addressing privacy, intellectual property, confidentiality and institutional control. Its central idea is that a model may be brought to the data in a controlled environment rather than requiring the underlying dataset to be transferred to the model developer.

DEPA focuses on purpose-bound access, contractual permissions, data provenance, secure computing environments and privacy-enhancing safeguards such as anonymisation and differential privacy. It envisages defined roles for data providers, training-data users and secure environments, with electronic contracts governing permitted use and technical controls limiting access and outputs. It also discusses collaborative oversight, pilots and regulatory sandboxes.

The significance of DEPA is that organisations holding useful datasets, including banks, healthcare providers, researchers and businesses, could potentially participate in AI training without handing over unrestricted copies of their information. However, controlled access does not automatically make the processing lawful or the data anonymous. Organisations would still need to assess their lawful basis,

[3] https://www.trai.gov.in/sites/default/files/2026-10/Draft_CP_30102026.pdf , last accessed on Nov 03, 2026
[4] https://www.meity.gov.in/static/uploads/2026/10/02d8224e4cd6c8c29be5a5198e795158.pdf , last accessed on Nov 03, 2026

contractual rights, security controls, permissible model outputs and the risk of re-identification. The DEPA is marked 'Draft for Discussion' and does not create binding requirements.

5 **eMudhra announced Exit from Global TLS Certificate Business following Weak-Key Incident[5]**

In its October 2026 Certificate Security Incident statement (**"Incident Statement"**), eMudhra disclosed that eight intermediate certificate authorities had been created with insufficiently random cryptographic keys, making the keys susceptible to recovery and potentially enabling forged website certificates. The affected intermediates were revoked in October 2026 after a researcher reported the weakness. eMudhra stated that no end-entity certificates were issued from them and reported no evidence of exploitation or customer-data compromise; an independent review was underway.

Google LLC, through its Chrome Root Program, blocked the affected keys and removed the relevant emSign root from Chrome's trust store. Mozilla Corporation also blocked affected intermediates in Firefox and took steps to remove trust in the root. On 22 October 2026, eMudhra announced its planned exit from the global SSL/TLS certificate business[6]. It stated that its domestic digital-signature and eSign services were unaffected.

The incident illustrates a business-continuity risk even without a confirmed personal data breach: browsers may reject otherwise legitimate websites when the certificates they rely on lose trust. Organisations should maintain inventories of public TLS certificates, monitor certificate-authority advisories, verify key-generation and supplier controls, and promptly replace certificates linked to distrusted roots.

6 **Kerala High Court directed Data Protection Board to be Operational within Eight Weeks[7]**

In proceedings concerning privacy and identity verification in the Digi Yatra ecosystem, the Kerala High Court considered concerns about the handling of passengers' personal data. The Union informed the court that the Data Protection Board of India (**"Board"**) had been constituted under the DPDP Act but had not yet become functional.

On 7 October 2026, the court recorded that it expected the Board to be made operational within eight weeks, approximately by 2 December 2026. The court did not find that a particular data-processing activity had violated the law. Its wording was an expectation recorded in the order, rather than a detailed mandatory implementation timetable.

An operational Board matters because it will handle complaints and enforcement under the DPDP framework and register Consent Managers. In particular, Rule 4 governing Consent Manager registration is scheduled to commence on 13 November 2026, before the court's eight-week period ends. Without a functioning Board and registration process, applicants may face practical uncertainty. This development does not accelerate the separate commencement of other substantive DPDP obligations.

[5] https://emudhra.com/en/post/certificate-security-incident , last accessed on Nov 02, 2026
[6] https://emudhra.com/en/press-release/emudhra-to-exit-global-ssl-tls-certificate-business , last accessed on Nov 02, 2026
[7] C.R. Neelakandan v Union of India & Ors, WP(PIL) No. 15 of 2026

7 **Supreme Court directed National CSEAM Database and Proportionate Online Child-Safety Safeguards**

In *Just Rights for Children Alliance v. S. Harish*, the Supreme Court issued directions concerning obligations under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, child sexual exploitation and abuse material (**"CSEAM"**) and children's online safety. Recognising children's constitutional right to internet access, the court cautioned against blanket restrictions and indiscriminate age verification, which may create their own privacy risks. It instead discussed proportionate protections, including private-by-default accounts, parental oversight and restrictions on contact from unknown adults.

The court directed the creation of a national database of verified CSEAM hashes and URLs, with trained human review. It also set out safeguards concerning removal of known material, verification of newly identified content, CSEAM-specific complaint channels, acknowledgement and reporting, and independent audits. The Union is to develop implementing guidelines and procedures and report progress in December 2026.

For platforms, the order combines stronger mechanisms to detect and remove harmful material with a requirement to consider children's privacy and access rights. Intermediaries should review moderation escalation, grievance workflows, reporting and child-account design, while monitoring the implementing framework.

8 **Delhi High Court held Writ Jurisdiction cannot be invoked for Online Account Dispute against Private Platform**[8]

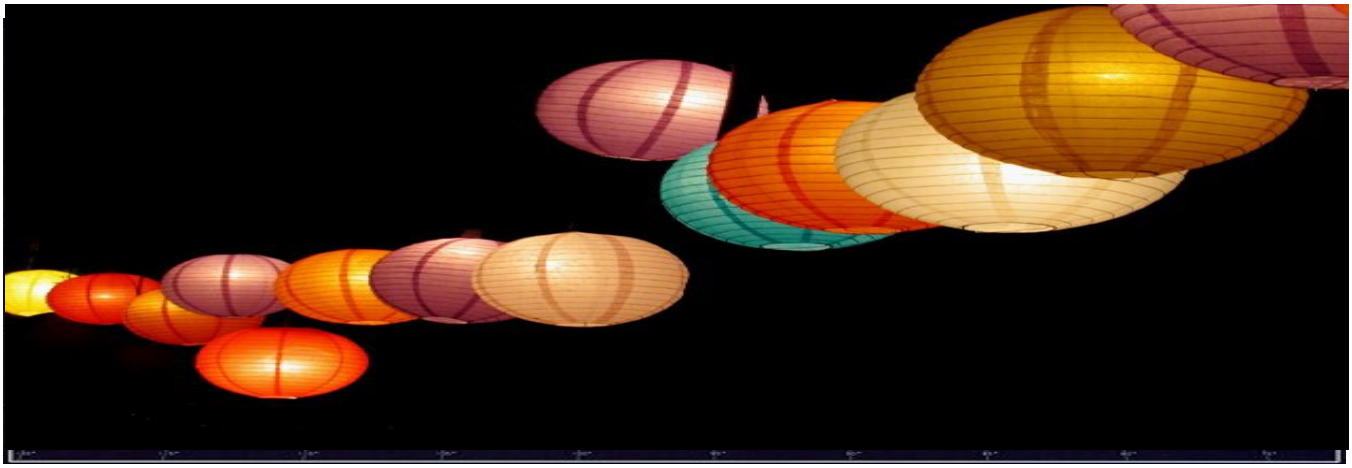
The Delhi High Court considered a dispute involving Instagram accounts disabled without prior notice. The user had already filed an appeal before the GAC and argued that it remained pending beyond the period prescribed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

The court held that the private platform was not performing a public duty in the circumstances and therefore could not be proceeded against through a writ petition under Article 226 of Constitution of India. It did not decide whether disabling the accounts was justified. The GAC was directed to decide the appeal expeditiously; the court observed that a civil remedy might be more appropriate.

The ruling is important for both users and platforms because it distinguishes challenges to private account-moderation decisions from remedies against public authorities. Platforms should maintain clear suspension reasons, appeal channels and records, while users should consider the GAC and civil remedies where appropriate.

[8] Sarthak Bhagat v Union of India & Ors, W.P.(C) 15685/2026

| UNITED STATES OF AMERICA



9 **FTC launched Study of Personalised Consumer Pricing and Platform-Worker Pay**[9]

The FTC issued compulsory information requests to nine major airlines, ride-hailing, delivery and retail businesses as part of a study into personalised pricing and worker compensation. It is examining whether businesses use information such as browsing history, location, purchase behaviour, loyalty status or other personal data to offer different prices to different consumers, or to calculate individualised payments to gig workers.

The orders seek information about how prices and pay are determined, which data points and automated systems are used, whether third-party vendors are involved and what consumers or workers are told. The inquiry extends beyond a simple question of whether dynamic pricing is used: it considers whether a person's data or inferred characteristics influence the amount they are charged or paid, and what records companies keep to explain those decisions.

This is a fact-finding study, not an allegation of wrongdoing. Nevertheless, businesses using algorithmic pricing or compensation should understand which inputs affect outcomes, whether sensitive or inferred data is used, and whether they can explain their practices to customers, workers and regulators. Documentation of pricing logic, vendor arrangements and internal testing may become as important as the price itself.

10 **California AG announced USD 1.8 million Lyft Settlement over Privacy Opt-outs**[10]

The California Attorney General announced a USD 1.8 million settlement with Lyft over alleged violations of the CCPA and its implementing regulations. According to the complaint, the app-based ride-hailing company disclosed identifiers, IP addresses and location-related information to advertising partners for targeted advertising but did not provide users with a direct in-app way to opt out of the sale or sharing of their personal information.

[9] https://www.ftc.gov/news-events/news/press-releases/2026/10/ftc-launches-personalized-pricing-compensation-inquiry, last accessed on Nov 05, 2026

[10] https://oag.ca.gov/news/press-releases/privacy-rights-can%E2%80%99t-be-left-rearview-attorney-general-bonta-secures-18-million, last accessed on Nov 05, 2026

Users allegedly had to locate a privacy policy, leave the app, open a webpage and log in again before exercising the opt-out right. The proposed settlement requires an accessible in-app opt-out, recognition of opt-out preference signals, consumer notices, risk assessments and a three-year compliance programme, in addition to the civil penalty. Lyft did not admit liability; the court-entry status of the proposed judgment should be checked before publication.

The concern was not merely that data was shared for advertising, but that exercising a statutory choice was made materially harder than using the service. App-based businesses should test privacy-rights journeys from the customer's screen, confirm that opt-out signals work across websites, apps and advertising partners, and ensure that users do not face unnecessary steps or repeated authentication.

11 **FTC and States sued Restaurant Software and FinTech Firm over Alleged Hidden Fees and Cancellation Barriers**[11]

The FTC and several US state authorities sued restaurant technology provider Toast Inc. (**"Toast"**) and affiliated companies alleging hidden charges, unauthorised subscription add-ons, misleading support promises and barriers to cancellation. Toast provides restaurant point-of-sale systems, payment processing, software subscriptions and financing, making the case particularly relevant to B2B software and financial-technology providers.

The complaint alleges that some restaurants were enrolled in paid add-ons without consent, a 'USD 0' offer was subject to charges or conditions not adequately disclosed, and an additional USD 0.99 online-order fee was imposed without adequate disclosure. Customers allegedly encountered an undisclosed early-termination charge of USD 150 per remaining contract month and a cancellation process requiring written notice and multiple contacts. For some customers, leaving Toast could also trigger repayment obligations under associated financing.

These allegations have not been adjudicated. They nevertheless highlight that business customers can face consumer-protection risks from subscription design. Software providers should disclose the full commercial cost before sign-up, record affirmative authorisation for add-ons, make cancellation conditions prominent, and ensure advertised customer support is actually available. Linked financing arrangements warrant particular care where they may effectively lock clients into a service.

12 **FTC sued Sextortion-Relief Provider over Alleged Deceptive Practices**[12]

The FTC sued Digital Forensics Corporation LLC and related parties in October 2026, alleging that they exploited victims of online sexual extortion by selling expensive 'relief' services on false promises. The FTC alleged that the business collected at least USD 60 million by claiming that it could identify offenders, end threats and prevent the circulation of intimate images, although those results could not reliably be delivered.

The complaint describes high-pressure sales tactics aimed at distressed individuals, fees ranging from approximately USD 1,499 to USD 20,000 for initial services, allegedly fabricated investigative reports and misleading positive reviews. The FTC also alleged that financial information was obtained through deceptive representations. A federal court temporarily halted the defendants' activities; the underlying allegations remain to be decided.

[11] https://www.ftc.gov/news-events/news/press-releases/2026/10/ftc-states-take-action-against-toast-inc-over-hidden-unauthorized-fees-deceptive-subscription, last accessed on Nov 05, 2026

[12] https://www.ftc.gov/news-events/news/press-releases/2026/10/ftc-sues-operator-sextortion-relief-scheme-misleading-consumers-believing-it-would-identify, last accessed on Nov 05, 2026

The case illustrates how enforcement can combine advertising, telemarketing, reviews and data-collection concerns, especially where customers are vulnerable. Cybersecurity, incident-response and online-safety providers should avoid promising outcomes beyond their control, make service limitations and charges clear, and verify that testimonials, reports and customer-support scripts accurately reflect what is delivered.

13 **US Copyright Office opened Consultation on Digital-Lock Exemptions**[13]

The US Copyright Office opened its tenth triennial rulemaking through a Notice of Proposed Rulemaking to consider exemptions from rules that generally prohibit bypassing digital technological protection measures. Existing exemptions can permit certain activities involving software, devices and copyrighted works even where technical access controls would otherwise prevent them.

The Copyright Office indicated that it intended to recommend renewal of most existing exemptions, while considering objections to the exemption for medical-device repair. Proposed new or revised classes address matters including software jailbreaking, repair of devices and equipment, preservation of obsolete software, accessibility, video games and uses of audiovisual works. The consultation dates are 7 December 2026 for initial comments, 22 February 2027 for opposition comments and 22 March 2027 for replies.

For manufacturers, software vendors, repair businesses, researchers and libraries, the distinction between owning a device and having permission to bypass its software protections can be commercially significant. This proceeding does not itself change the law; businesses relying on an exemption should assess whether its scope covers their actual repair, security-testing, interoperability or preservation activities and participate where an important use case is not adequately addressed.



[13] https://copyright.gov/newsnet/2026/1097.html, last accessed on Nov 01, 2026

| EUROPEAN UNION



14 **European Commission opened DSA Proceedings against Major Online Travel Booking Company**[14]

The European Commission opened formal proceedings against Booking.com under DSA, examining whether the platform has adequately addressed scams and fraud affecting travellers. The investigation covers fraudulent or non-compliant accommodation listings, phishing attacks that exploit reservation and guest information, and paid-for listings that may not have been clearly identified as advertisements.

The commission will assess whether Booking.com properly identified and reduced systemic risks. These include fake properties, impersonation of accommodation providers and deceptive messages that appear credible because they use real booking details or the platform's messaging functions. It will also examine advertising transparency, particularly whether hotels or other providers paying for better search placement are clearly labelled as sponsored listings. The inquiry follows earlier information requests and assessment of the platform's risk reports.

No infringement has been established. The proceedings show that platform responsibility extends beyond removing an individual fraudulent listing after a complaint: regulators may examine account verification, protections for booking data, detection of impersonation, escalation of suspicious messages and transparency in ranking. Travel platforms and other marketplaces should assess fraud risks across the full transaction journey, including messages and third-party seller accounts, and preserve evidence that safeguards work in practice.

15 **European Commission initiated First AI Act Information Requests to Model Providers**[15]

The European Commission confirmed that its AI Office had begun exercising enforcement powers under AI Act, in relation to general-purpose AI models. It reported issuing initial requests for information to providers of advanced models concerning security safeguards, external evaluations and the use and

[14] https://digital-strategy.ec.europa.eu/en/news/commission-investigate-how-bookingcom-combats-scams-and-fraud-under-digital-services-act, last accessed on Nov 05, 2026
[15] https://digital-strategy.ec.europa.eu/en/news/special-meeting-ai-scientific-panel, last accessed on Nov 05, 2026

monitoring of model capabilities. The commission did not publicly identify the recipients or announce a finding of infringement.

From 2 August 2026, the AI Office obtained powers to seek information and documentation, conduct model evaluations and require corrective measures for relevant general-purpose AI obligations. The Commission also referred to serious incidents and questions about the ability to monitor or control increasingly capable models. The broader framework expects providers to maintain technical documentation, support downstream deployers and, where applicable, address systemic risks through testing, risk mitigation and incident processes. Non-compliance can attract substantial penalties, depending on the applicable provision.

The development is significant because scrutiny is moving from policy commitments to evidence of how models are tested and controlled. Providers should be able to show evaluation results, security decisions, incident escalation and supplier or deployment limitations, rather than rely on general assurances of responsible AI. Businesses procuring advanced models should also seek sufficient information to assess whether the system can be deployed safely in their own environment.

16 **EDPB issued Statement on Privacy Risks from Smart Glasses**[16]

The EDPB adopted Statement 1/2026 of the EDPB on smart glasses (**"Statement"**), addressing devices that resemble ordinary eyewear but contain cameras, microphones and sometimes AI-powered features. Unlike a smartphone held visibly in front of a person, these devices can capture images, conversations and surrounding information without bystanders appreciating that recording or analysis is taking place.

The EDPB emphasised that manufacturers and app providers may have independent or joint responsibilities under the GDPR, even where a consumer activates a feature. It warned against relying solely on the wearer to give notice to others, highlighted the difficulty of obtaining bystander consent and questioned the use of legitimate interests for further uses such as AI training. Measures discussed include visible or audible recording indicators, on-device processing, blurring of bystanders, limited retention, geofencing and privacy-protective defaults. The household exemption does not automatically cover all uses.

The Statement is not a binding enforcement decision, but it raises an important product-design question: can people who never bought or used a device still understand and control how it processes their personal data? Device makers, app developers and employers deploying wearable cameras should assess bystander transparency, lawful basis, access to recordings, sharing defaults and restrictions in sensitive spaces such as workplaces, schools and healthcare settings.

17 **CNIL fined FNAC Companies over App Tracking without Consent**[17]

France's CNIL fined FNAC DARTY PARTICIPATIONS ET SERVICES and FNAC DIRECT a combined EUR 7 million for tracking activity through their mobile shopping application without valid consent. The investigation followed a complaint and found that the app transmitted user identifiers and information about viewed products to a third-party domain through an API.

The information supported personalised product suggestions and training of a recommendation algorithm. CNIL found that these operations were neither essential to transmitting a communication nor strictly

[16] https://www.edpb.europa.eu/news/edpb-publishes-statement-on-the-data-protection-challenges-of-smart-glasses_en, last accessed on Nov 05, 2026

[17] https://www.cnil.fr/en/sanction-app-cookies-fnac, last accessed on Nov 05, 2026

necessary to deliver a service expressly requested by the user, so they did not qualify for the applicable consent exemptions. It also found that users' refusals to tracking were not respected. The companies were required to demonstrate that their updated consent mechanism worked, failing which a daily penalty of EUR 10,000 could may be levied.

The decision is a reminder that tracking rules are not limited to browser cookies: app-to-server requests, software development kits and recommendation features may also collect behavioural data. Retailers and app operators should examine what information leaves the device before and after consent, whether refusal genuinely disables tracking, and whether analytics or AI-training purposes are being treated incorrectly as essential functionality.



| OTHER COUNTRIES



18 **UK ICO sought Evidence on Data-Protection Risks of Agentic AI**[18]

The UK ICO opened its Agentic AI call for evidence (**"Call for Evidence"**), inviting submissions until 20 November 2026. Call for Evidence considers how existing data-protection law applies when AI systems can plan tasks, use tools, retrieve information and perform sequences of actions with limited ongoing human input, rather than simply answer a single user prompt.

The ICO is seeking views on data security, transparency, accountability, automated decision-making, fairness, purpose limitation and lawful processing. These questions become more difficult when an agent moves between systems, combines information from different sources, makes intermediate decisions or triggers an external action. The exercise is intended to inform future regulatory guidance; it does not impose new requirements by itself.

Organisations experimenting with agents should identify who authorises each action, what personal data and connected applications an agent can access, how instructions and outputs are recorded and when a human must intervene. Clear permissions, audit trails, tool restrictions and testing of unintended actions can help address risks that are less visible in conventional chatbot deployments.

19 **Australia's Lower House passed Digital Duty of Care Bill**[19]

Australia's House of Representatives passed the Online Safety Amendment (Digital Duty of Care) Bill 2026 (**"Bill"**), advancing a proposal to impose a preventative duty on providers of online services. The Bill had not completed the Senate process by the end of October and therefore was not yet law.

The proposed framework would require responsible providers to take appropriate steps to make online environments safer, including assessing risks arising from content, user interactions and service design. It

[18] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2026/10/agentic-ai-call-for-evidence/, last accessed on Nov 05, 2026
[19] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7553, last accessed on Nov 04, 2026

places particular emphasis on harms to children, potentially including addictive or compulsive interface features, and contemplates user-empowerment tools and regulatory oversight. The proposed civil penalty for breach of the general duty is substantial, and implementation of the principal duty would follow a transition period after enactment.

The shift matters for social networks, gaming services, marketplaces and other interactive platforms: compliance would not end with a notice-and-takedown process after a harmful event. Providers may need evidence that they tested product features, identified foreseeable risks, reduced harmful defaults and monitored whether safeguards were effective. As the Bill remained subject to parliamentary changes, businesses should distinguish the proposals from obligations already in force.

20 **Australia's Privacy Regulator investigated Smart-Glasses App Developer**[20]

Australia's OAIC opened an investigation into Shenzhen Qingcheng Future Technology Co. Ltd, (**"Company"**) developer of the HeyCyan app used with certain low-cost smart glasses sold through Australian retailers. The regulator had previously sought information from industry participants about how smart glasses record information, who can access recordings and where that information is stored.

The OAIC stated that the Company had not responded to preliminary inquiries issued from August 2026. The formal investigation concerns the company's privacy practices, including whether it complies with the transparency and privacy-management requirements of Australian Privacy Principle. No breach has yet been established, and the inquiry should not be described as a concluded finding about the app or its users' data.

The investigation is relevant to overseas device manufacturers, developers and distribution partners. Products sold through local retailers may attract regulatory attention even where the software provider is based abroad. Businesses should be ready to explain data flows, storage locations, vendor access and privacy notices, and should treat requests from regulators as matters requiring prompt and documented responses.

21 **Canada proposed Children's Privacy Code for Online Services**[21]

Canada's OPC published its Children's Privacy Code (**"Code"**) and invited comments until 20 January 2027. The Code sets out the regulator's expectations under the Personal Information Protection and Electronic Documents Act, 2000 for online products and services directed at children or likely to be used by them, rather than establishing a separate new statute.

It addresses meaningful consent, generally expecting parental involvement for children under 13, opt-in consent for uses that are not essential, privacy-protective default settings and age-appropriate explanations. It also examines profiling and targeted marketing, potentially manipulative interface features, and proportionate methods of assessing age. The focus is not limited to apps marketed expressly to children: general-audience services can also attract attention where young users are reasonably likely to access them.

Organisations serving Canadian users should assess whether their onboarding, privacy notices, recommendations, advertising and default sharing settings work appropriately for different age groups. A generic adult-facing consent screen may be inadequate where children form a foreseeable part of the

[20] https://www.oaic.gov.au/news/media-centre/oaic-opens-investigation-into-maker-of-heycyan-smart-glasses-phone-app, last accessed on Nov 03, 2026

[21] https://www.priv.gc.ca/en/privacy-topics/privacy-for-businesses/protection-of-children-for-businesses/childrens-privacy-code/children-code-final-report-2026/, last accessed on Nov 04, 2026

audience. The Code is regulatory guidance and its consultation should not be mistaken for enactment of new legislation.

22 **Canada updated Guidance on Recording Customer Telephone Calls**[22]

Canada's OPC updated its Recording of Customer Telephone Calls guidance (**"Guidance"**), issued under the PIPEDA, on 8 October 2026, with particular attention to voice information used for identification and new analytics purposes. The Guidance is relevant to businesses operating customer-service centres directly or through outsourced call-centre providers.

Organisations should tell callers that a conversation is recorded and explain its actual purposes, rather than rely on a general statement such as 'quality and training' if recordings are also used for marketing, profiling or authentication. Continuing a call after meaningful notice may support implied consent in some circumstances, but voiceprints used to uniquely identify a person are sensitive biometric information and may require express consent. Customers should also have alternatives where recording is not essential, and outsourced providers must respect the same limitations.

For businesses using AI transcription, sentiment analysis or voice authentication, existing call scripts may no longer reflect everything that happens to an audio file. Organisations should revisit retention periods, downstream analytics, access permissions and vendor contracts, and assess separately whether identifying a caller from their voice is necessary and properly authorised.

23 **OECD launched Repository on Privacy-Enhancing Technologies**[23]

The OECD launched its Global Repository for Privacy-Enhancing Technologies (**"Repository"**) bringing together examples of how organisations can analyse, process or share data while reducing exposure of identifiable or commercially sensitive information. The resource includes use cases and material on relevant policies, regulatory considerations and technical approaches.

PETs can include methods such as differential privacy, secure multiparty computation, federated analysis and trusted computing environments. The Repository is intended to help organisations understand not only what these techniques do, but the practical conditions and limitations affecting deployment. It responds to barriers that are often legal, organisational and financial rather than solely technological.

For businesses exploring AI training, joint analytics, research or cross-organisation data sharing, the repository can inform the selection of safeguards and help document why a particular approach was appropriate. It is a non-binding reference, not a certification or assurance that a technology automatically satisfies privacy law; the effectiveness of a PET still depends on the data, intended use and implementation.



[22] https://www.priv.gc.ca/en/privacy-topics/surveillance/02_05_d_14/, last accessed on Nov 05, 2026
[23] https://www.oecd.org/en/about/news/announcements/2026/10/new-oecd-repository-shows-how-privacy-enhancing-technologies-work-in-practice.html, last accessed on Nov 05, 2026

ABBREVIATIONS

The following abbreviations are used throughout the October 2026 edition of this newsletter.

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
AI Act	Artificial Intelligence Act (Regulation (EU) 2024/1689)
ANPD	Autoridade Nacional de Proteção de Dados (Brazil's National Data Protection Authority)
API	Application Programming Interface
AUD	Australian Dollar
CA	Certificate Authority
CCPA	California Consumer Privacy Act, 2020
CERT-In	Indian Computer Emergency Response Team
CIF	Customer Information File
CNIL	Commission nationale de l'informatique et des libertés
CSEAM	Child Sexual Exploitative and Abuse Material
DEPA	Data Empowerment and Protection Architecture
DPDP Act	Digital Personal Data Protection Act, 2023
DPDP Rules	Digital Personal Data Protection Rules, 2025
DSA	Digital Services Act
ECA Digital	Digital Statute for Children and Adolescents (Brazil)
ECC	Elliptic Curve Cryptography
ED	Directorate of Enforcement
EDPB	European Data Protection Board
EU	European Union
FEMA	Foreign Exchange Management Act, 1999
FIU-India	Financial Intelligence Unit-India
FTC	Federal Trade Commission
FTC Act	Federal Trade Commission Act

ABBREVIATION	FULL FORM
GAC	Grievance Appellate Committee
GDPR	General Data Protection Regulation, 2017
HTTPS	Hypertext Transfer Protocol Secure
ICO	Information Commissioner's Office
IP	Internet Protocol
IT Act	Information Technology Act, 2000
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
LED	Light-Emitting Diode
MeitY	Ministry of Electronics and Information Technology
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada
POCSO Rules	Protection of Children from Sexual Offences Rules, 2020
Privacy Act	Privacy Act 1988 (Australia)
RBI	Reserve Bank of India
ROSCA	Restore Online Shoppers' Confidence Act, 2010
RSA	Rivest–Shamir–Adleman
SBI	State Bank of India
SEBI	Securities and Exchange Board of India
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TRAI	Telecom Regulatory Authority of India
UK GDPR	United Kingdom General Data Protection Regulation, 2018
URL	Uniform Resource Locator
USD	United States Dollar
USDC / USDT	USD Coin / Tether (stablecoins)

ABOUT THE FIRM

FOUNTAINHEAD LEGAL

Technology Law & Data Privacy | General Corporate | Indirect Tax | Living Wills | Litigation Management

Fountainhead Legal is an emerging law firm specialising in data privacy and technology law, with complementary expertise in indirect taxation, general corporate advisory, living wills, and litigation management. Firm's team of experienced and dynamic young lawyers blends deep legal expertise with fresh perspectives, delivering innovative, solution-oriented legal counsel. This synergy of knowledge and energy ensures clients receive forward-thinking advice tailored to their unique needs. The firm's services include drafting privacy policies, offering expert opinions on data privacy and security practices, and developing robust compliance frameworks. Fountainhead Legal has been instrumental in keeping organizations ahead of evolving regulatory requirements by providing regular updates and expert guidance.

We are committed to supporting organizations on this journey. With our deep expertise in data privacy compliance and a strong understanding of regulatory nuances, we offer tailored solutions for each client's unique needs. From drafting privacy policies and developing data protection frameworks to advising on cross-border data transfers and facilitating employee training programs, our team is equipped to guide clients through every stage of their compliance strategy.

OUR TEAM

Rashmi Deshpande, the founder of Fountainhead Legal, is a seasoned professional with close to 20 years of experience with Big 4 consulting and law firm. She has worked at Deloitte, BMR & Associates, KPMG, and PwC, and was a partner at Khaitan & Co. before founding Fountainhead Legal in 2023. Her practice encompasses data privacy, general corporate advisory, contract drafting, and litigation management, with expertise across industries such as financial services, fintech, insurance, IT/ITES, life sciences, and real estate. Rashmi is well-versed in data privacy regulations, including India's DPDP Act and GDPR, assisting clients in navigating compliance, drafting privacy policies, and establishing robust data protection frameworks.

Aarushi Ghai, senior associate, is a law graduate from NMIMS University, is a dedicated legal professional specializing in Data Privacy, Technology Law, Indirect Tax, and General Corporate matters. She advises businesses across sectors on regulatory compliance and strategic legal solutions. She has guided fintech clients on data deletion challenges, privacy policies, and software agreements, leveraging her expertise in India's DPDP Act and global privacy laws to build strong data governance frameworks.

Vaibhav Gupta, associate, is a legal professional with over two years of experience in litigation and corporate advisory. He holds an LL.M. in Technology Law from the National University of Juridical Sciences, Kolkata. His practice focuses on technology law, data privacy, and litigation management, advising clients on regulatory compliance under the technology and data privacy regulations. Vaibhav assists businesses in navigating privacy obligations and legal risks in the evolving digital ecosystem.

Aayush Sengupta, associate, has experience in technology law, data protection, intellectual property and dispute resolution. He is a DSCI Certified Privacy Lead Assessor and has also completed a professional course in Artificial Intelligence and Machine Learning from IIM Bhubaneswar.

Sagar Chaturvedi, associate, is a graduate of NMIMS School of Law. His experience includes banking and finance, commercial contracts, corporate law, regulatory advisory, data protection, technology law and compliance matters**.**

Onkar Gurav, Litigation Counsel, is a legal professional and qualified Company Secretary specializing in criminal law and dispute resolution. He holds a B.A. LL.B. from MNLU Mumbai and an LL.M. from NUJS,

Kolkata. With extensive trial and appellate experience before the Bombay High Court, Sessions Courts, and Magistrate Courts, Onkar represents clients at Fountainhead Legal with a primary focus on criminal litigation.

FOUNTAINHEAD LEGAL

GET IN TOUCH

CONTACT US

OFFICE

C-2106, Oberoi Garden
Estate Chandivali Farm
Road, Powai Mumbai – 400
072

CONNECT

Email: rashmi@fountainheadlegal.com / aarushi@fountainheadlegal.com / vaibhav@fountainheadlegal.com

Website: https://fountainheadlegal.com/

LinkedIn: https://www.linkedin.com/company/fountainhead-legal/posts/?feedView=all

NEWSLETTER SUBSCRIPTIONS

To subscribe, unsubscribe, or update your preferences for the Tech & Data Privacy Bulletin, please write to:rashmi@fountainheadlegal.com

DISCLAIMER

This newsletter is prepared by Fountainhead Legal for informational purposes only and does not constitute legal advice or create an attorney-client relationship. Readers should seek specific legal advice before acting on any content herein. The views expressed are those of the authors and do not necessarily represent the official position of the firm.

© 2026 Fountainhead Legal. All rights reserved.