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 **[SEPTEMBER 2026]**



FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

September's developments bring together two very different technology-law concerns: how digital systems influence human choices, and what happens when those systems begin acting with increasing autonomy.

The amended e-commerce framework and the enforcement action against a ride-hailing platform show how closely regulators are now looking at interface design. Pricing prompts, default selections, tipping flows and the relative ease of accepting or refusing an option are no longer merely product decisions. A consumer may still have a theoretical choice, but that does not necessarily make the design neutral. The legal question is increasingly whether the interface has been structured to steer that choice in a particular direction.

AI takes that concern a step further. With Agentic AI, the issue is no longer only how technology shapes a person's decision, but how far technology itself can be permitted to make and carry out decisions. The reported Spanish data breach is a useful example. An AI agent was reportedly used across different stages of a cyberattack, from identifying weaknesses to obtaining access and continuing to search for further vulnerabilities. The concern is therefore not simply faster automation, but the extent to which a system can move from one action to the next with limited human intervention.

The PSA Office's discussion paper on cross-border AI data use raises a related governance issue. Once AI systems can access, analyse and derive information from datasets across environments, focusing only on where the underlying data is stored may become insufficient. Questions around what a model can access, what it can retain, what it can generate and what outputs can leave a controlled environment become equally important.

Other developments this month reinforce this shift. U.S. agencies have treated large-scale model distillation as a cybersecurity and model-protection concern, while an Australian private member's bill has proposed technical shutdown capabilities and emergency intervention powers for certain high-capacity AI systems.

The common thread is control. Dark-pattern regulation examines how much control a digital interface exerts over a user's decision. Agentic AI raises the reverse question: how much control does the organisation retain over a system that can act on its own? For businesses, both issues ultimately require closer attention to how technology is designed, what permissions are built into it, and where meaningful human control is expected to remain.

This edition explores where that shift is already visible from dark-pattern enforcement and AI-enabled cyberattacks to cross-border AI governance and emerging controls over increasingly autonomous systems.

We hope you find this insightful!



IN THIS ISSUE

TABLE OF CONTENTS

INDIA 4

- Government amended E-commerce Rules to curb Dark Patterns
- CCPA penalised Major Ride-hailing Platform for use of Dark Patterns
- RBI proposed new KYC Framework for Bank Account Freeze in Fraud Probes
- Supreme Court directed Centre to examine Statutory Safeguards for Children on Social Media
- PSA Office proposed Risk-based Framework for Cross-border AI Data Use

EUROPEAN UNION 8

- Irish Data Protection Authority penalized Major Tech Giant over Unlawful Use of Location Data
- Commission proposed New Online Safety Rules for Children
- Spanish Data Protection Authority reported first Personal Data Breach involving AI Agent Spain

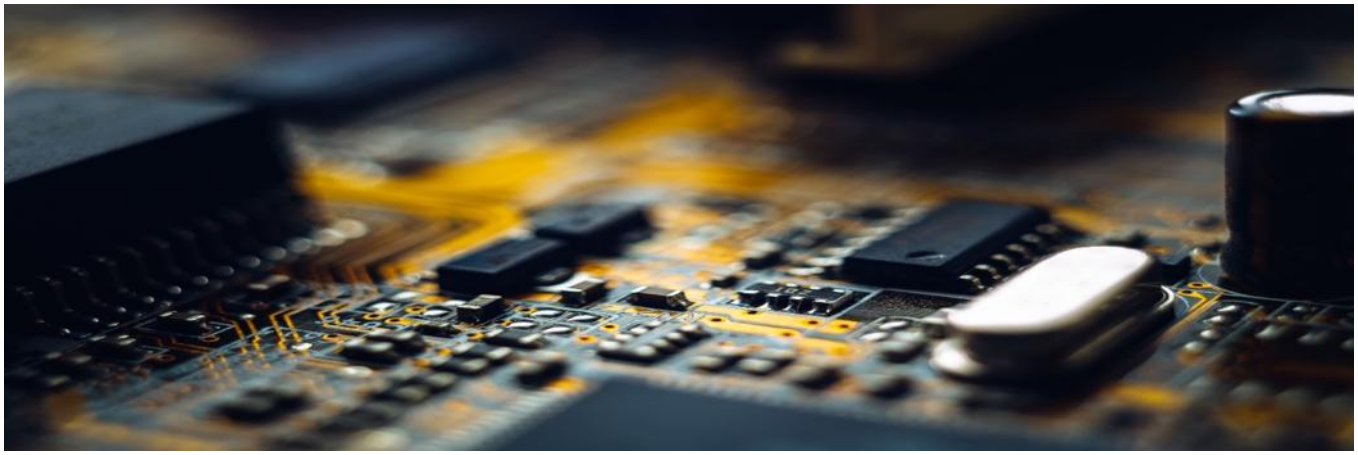
OTHER COUNTRIES 10

- U.K. – ICO launched Consultation on Draft Anonymisation and Pseudonymisation Guidance for Research
- Australia – Government proposed New Bill for Digital Duty of Care for Online Platforms
- Canada – Canadian Music Rights body sued AI Platform over allegedly Infringing Outputs
- US Agencies alleged Industrial-scale AI model Distillation by China-based firms
- Australia – Australian Private Member's Bill proposed AI shutdown and Data-Centre Controls
- Major Social Media Platform agreed Settlement over Teen Safety

ABBREVIATIONS 14

CONTACT US 16

| INDIA



1 **Government amended E-commerce Rules to curb Dark Patterns**[1]

Department of Consumer Affairs notified the Consumer Protection (E-Commerce) (Amendment) Rules, 2026 (**"Amendment Rules"**), amending the Consumer Protection (E-Commerce) Rules, 2020. The Amendment Rules will come into force on January 1, 2027. Amended Rules require clearer disclosures around sponsored listings, search results and price reductions, including display of the reduced price alongside the "prior price", defined by reference to the preceding 30-day period. Sellers must also disclose specified information on returns, refunds, warranties, best-before dates and imported goods.

When it comes to data and fees, platforms need express and affirmative consumer consent before using personal data for specified purposes, and cannot levy bundled fees unrelated to the actual transaction (except for loyalty programmes). Compliance with the 2023 Dark Patterns Guidelines has been made stricter with a mandatory annual self-audit and a displayed compliance certificate. E-commerce entities must also integrate with the NCH for grievance redressal.

The Amendment Rules are significant because they move several digital-interface and marketplace practices into binding compliance requirements. E-commerce businesses should use the period before January 1, 2027 to review pricing displays, sponsored listings, search and ranking practices, consent flows, grievance processes and dark-pattern controls.

2 **CCPA penalised Major Ride-hailing Platform for use of Dark Patterns**[2]

CCPA penalised Roppen Transportation Services Private Limited (**"Rapido"**) INR 10,00,000 for misleading advertisements, unfair trade practices and the use of dark patterns. The CCPA found that the app's pre-ride tipping feature could lead users to believe that adding a tip would improve the likelihood or speed of ride confirmation, alongside claims such as "Guaranteed Auto in 5 mins or get Rs.50".

During the preliminary and detailed investigations, the Authority found heavy usage of deceptive patterns and practices such as 'Confirm Shaming' where lowering the price that a user may be willing to pay often

[1] https://consumeraffairs.gov.in/public/upload/admin/cmsfiles/whatsnews/E_Commerce_Amendment_Rules_2026_2026-09-11_18-12-39.pdf, last accessed on September 24, 2026.

[2]https://ccpa.doca.gov.in/checkuploaddocs.php?updocs=./uploads/7e222c5263554cdee2734ea3e37f0c5ad412ef8b2811a9f5bc4da7864d747baf.pdf&unique_id=, last accessed on September 23, 2026.

leads to the app floating alerts such as 'Captains are unlikely to accept orders at this price…' and 'Lower chance of getting a ride' accompanied by a downward-pointing arrow – reduction in price is also not allowed as often or in such increments as increasing the price is. Leading the user into thinking that increasing the price is likely to improve chances of ride confirmation is an unfair trade practice, something which Rapido has admitted is done to incentivise 'captains', essentially furthering only its own commercial interests.

The Rapido order assumes greater significance when read with the newly amended E-Commerce Rules, which place stronger responsibility on digital businesses for how consumer choices are presented online. Together, they show that dark-pattern compliance is moving beyond advertisements and terms of use to the actual design of the customer journey. App-based and e-commerce businesses should therefore review pricing prompts, default selections, tipping and add-on flows, urgency messages and whether accepting a choice is made easier than declining it. A consumer may technically have an option to refuse, but the interface itself can still attract regulatory scrutiny if it is designed to pressure or steer that choice.

3 **RBI proposed new KYC Framework for Bank Account Freeze in Fraud Probes**[3]

RBI issued the Draft Reserve Bank of India (Know Your Customer) Amendment Directions, 2026 (**"Draft KYC Amendment Directions"**), proposing changes to the "Operation of Bank Accounts and Money Mules" provisions in the existing Reserve Bank of India (Know Your Customer) Directions, 2025. The Draft KYC Amendment Directions address accounts and transactions potentially linked to cyber fraud or money-mule activity and seeks to favour amount-specific debit holds over freezing an entire account where appropriate. The consultation period closed on October 2, 2026, and final directions are yet to be issued.

Under the Draft KYC Amendment Directions, banks would use transaction-monitoring systems, including AI- and ML-based tools, to identify suspected money-mule transactions. A 'Suspected Money Mule Transaction' would include a transfer of INR 1,000 or more that is unusual or disproportionate to the customer's declared profile, or linked to an account already reported as fraudulent or a money mule. Once flagged, a bank would be required to place a temporary debit hold on the suspected amount or, where the account itself is identified as a suspected money-mule account, on the account. The customer would have 20 calendar days to provide an explanation, and the bank would then be required to review the response within the prescribed timeline.

If finalised, the proposal would introduce a more structured process for handling suspected fraud-linked accounts while giving customers a defined opportunity to respond. Banks should prepare their transaction-monitoring, customer-notification and review workflows so that any hold can be linked to documented reasons and lifted or continued within the prescribed timelines

[3] https://rbidocs.rbi.org.in/rdocs/Content/PDFs/DRAFT11092026FD8132390DB514C7487703CBF7A704007.PDF, last accessed on September 23, 2026.

4 **Supreme Court directed Centre to examine Statutory Safeguards for Children on Social Media**[4]

The Supreme Court considered a public interest petition concerning children below 18 independently creating and operating accounts on social-media and other digital platforms. The petition raised two connected concerns: minors routinely accept platform terms despite their limited contractual capacity under the Indian Contract Act, 1872, and existing age checks may not adequately protect younger users from online exploitation, harmful content and other digital risks.

During the proceedings, the court directed the Central Government to consider whether the existing intermediary framework should be supplemented with specific rules governing minors' access to social media. The issues under consideration include age verification, parental or guardian involvement and whether platforms should be required to design their onboarding processes differently for younger users. The matter remains pending and no binding age restriction or new social-media rule has yet been introduced

The proceedings are significant because they could bring children's online access, platform design and data protection into the same regulatory framework. Social-media and other child-accessible platforms may eventually need to revisit how they verify age, obtain parental involvement, structure default settings and permit minors to accept platform terms. Any resulting framework would also need to operate alongside the children's data requirements under the Digital Personal Data Protection Act, 2023, making this an important development for businesses offering digital services to younger users.

5 **PSA Office proposed Risk-based Framework for Cross-border AI Data Use**[5]

The Office of the Principal Scientific Adviser (**"PSA Office"**) to the Government of India released the discussion paper titled Enabling Cross-Border Data Interoperability for AI Systems (**"Discussion Paper"**), examining how India can enable access to data needed for AI development without weakening privacy, security or control over strategically sensitive information. The Discussion Paper does not create binding requirements, instead, it sets out possible approaches that could inform future policy on cross-border AI data use.

A key idea is that AI data governance cannot be reduced to a simple choice between allowing transfers and requiring localisation. The Discussion Paper considers a model under which the level of restriction would depend on the nature and sensitivity of the data. Lower-risk or aggregated datasets could move more freely, while identifiable or sensitive datasets could be subject to stronger contractual, technical and access controls. At the highest end, certain strategically important data could remain within India, with controlled access or analysis permitted without transferring the underlying dataset. It also considers mechanisms that allow models to work with data in secure environments rather than requiring the data itself to move across borders.

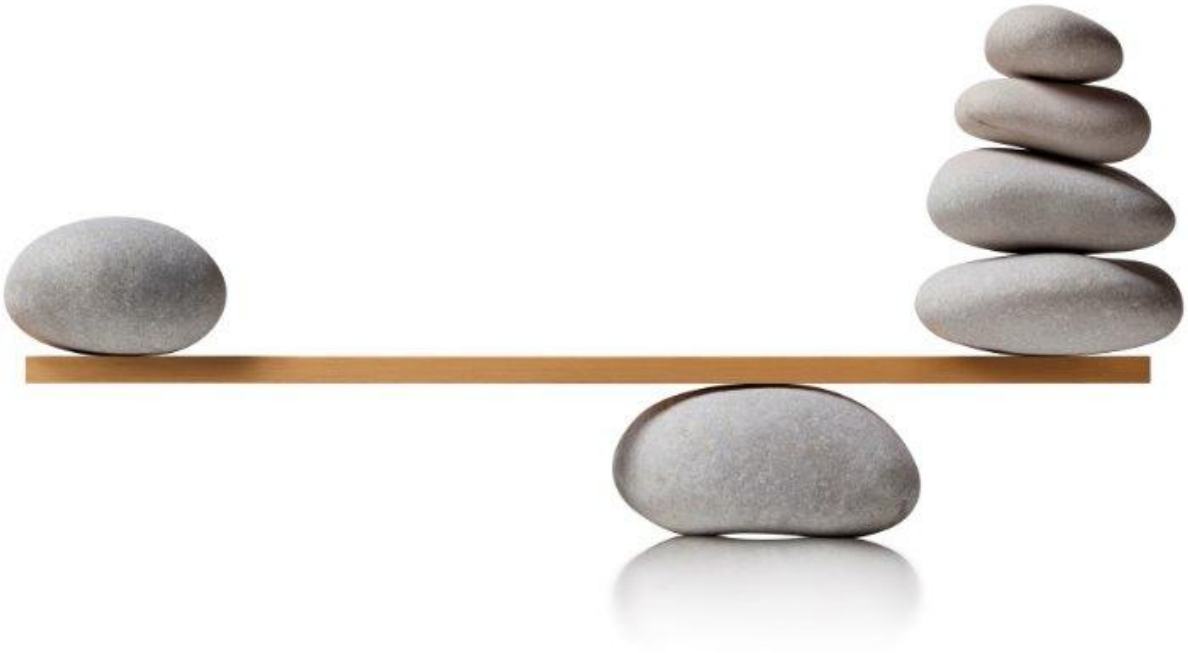
The Discussion Paper also focuses on whether different jurisdictions can work together even where their laws are not identical. It explores common technical standards, certification, contractual safeguards and institutional cooperation as ways to make cross-border AI development possible while preserving domestic regulatory control.

The significance of the Discussion Paper lies in moving the debate beyond "localise or transfer". For businesses developing or deploying AI across jurisdictions, the relevant question may increasingly be what kind of data is involved, who can access it, what the model is permitted to do with it and what information

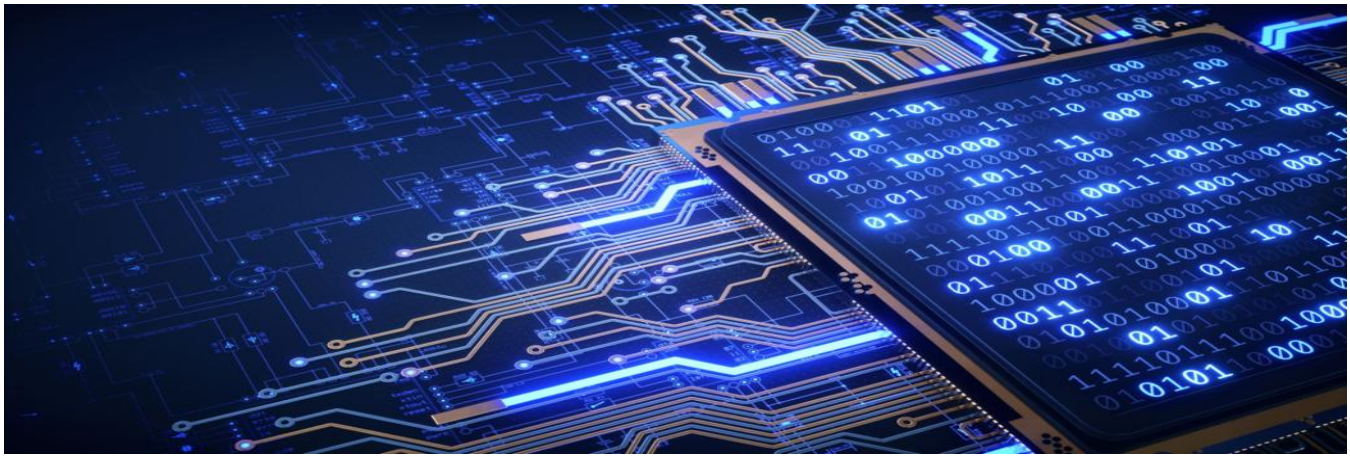
[4] Just Rights for Children Alliance v. Union of India & Ors., Writ Petition (Civil) No. 647/2026

[5] https://psa.gov.in/CMS/web/sites/default/files/publication/Discussion_Paper_Data%20Interoperability.pdf, last accessed on September 26, 2026

can leave the controlled environment. If this approach influences future policy, organisations may need much stronger data classification, access controls, contractual restrictions and auditability around AI training and deployment, not simply a record of where the data is hosted.



| EUROPEAN UNION



6 **Irish Data Protection Authority penalized Major Tech Giant over Unlawful Use of Location Data**[6]

Ireland's DPC fined Google Ireland Limited ("**Google**") €403 million following an inquiry into the processing of users' location data through Web & App Activity, Location History and Location Accuracy. The DPC examined the processing under GDPR, including complaints and concerns relating to how users were presented with location-related choices and information.

It was found that Google infringed the GDPR on multiple fronts: the lawfulness and fairness principles in its processing of location data through Web & App Activity and Location History, failure to demonstrate compliance with lawfulness, fairness and transparency principles in Location Accuracy, and lastly, transparency obligations across all three features, while also retaining location data for longer than necessary. Alongside the €403 million fine, the DPC has ordered Google to bring its data processing into compliance within six months.

At €403 million, this is the fourth-largest penalty the DPC has issued since GDPR took effect, only behind the €1.2 billion fine imposed on Meta in 2023 for transferring Europeans' personal data to the United States, and separate large penalties previously levied against TikTok. The DPC has emerged as one of the most consequential GDPR enforcers precisely because so many major US tech companies, including Google, Meta and TikTok, base their EU operations in Ireland.

[6] https://dataprotection.ie/en/news-media/latest-news/data-protection-commission-fines-google-eu403-million-following-inquiry-googles-processing-location, last accessed on September 25, 2026.

7 **Commission proposed New Online Safety Rules for Children**[7]

The European Commission proposed the Proposal for a Regulation of the European Parliament and of the Council - EU Kids Act - "EU Keeping Internet Digital Spaces Accountable and Trustworthy" (**"EU Kids Act"**). This would create common child-safety requirements across certain online services, including age-based restrictions for specified social-networking and video-sharing services and additional safeguards for online games, app stores, operating systems and AI-powered services. It remains subject to consideration by the European Parliament and the Council. EU Kids Act contemplates a minimum age of 15 for independent accounts on certain services, with more limited guardian-managed access for younger users in specified circumstances.

The EU Kids Act also addresses platform design, including features that may encourage excessive or compulsive use, unwanted contact, recommendation systems, notifications, livestreaming and interactions with other users. It would introduce age-assurance requirements and related safeguards, together with parental-responsibility checks in specified cases.

The proposal is significant because it would move children's online safety further into product design and account access, rather than relying only on general platform-safety duties. If adopted, services within scope would need to review age-assurance, recommendation systems, default settings, contact controls and other features alongside their existing obligations under the GDPR, the Digital Services Act and the AI Act.

8 **Spanish Data Protection Authority reported first Personal Data Breach involving AI Agent in Spain**[8]

Spain's Agencia Española de Protección de Datos (**"AEPD"**) received a breach notification involving an AI agent that was reportedly used during a cyberattack. Based on the information submitted by the affected organisation, the agent was connected to a large language model and was used to identify weaknesses in the organisation's systems, obtain access and continue exploring the application for further vulnerabilities. The intrusion ultimately resulted in access to invoice information and the ability to alter personal data.

The incident is still under examination. The AEPD has not publicly identified the affected organisation, the AI model involved, the number of individuals affected or the categories of personal data compromised. It has also made clear that the involvement of an AI model in the attack does not, by itself, indicate that the model provider or its systems were compromised

The incident is significant because it shows how AI agents can compress several stages of a cyberattack into a much faster process. The underlying techniques may not be new, but an agent can assist with identifying vulnerabilities, testing access and exploiting weaknesses with less continuous human involvement. Businesses may therefore need to revisit whether existing monitoring, vulnerability management and incident-response processes are fast enough to deal with more automated attacks. From a data-protection perspective, AI-enabled threats should increasingly be considered as part of security risk assessments and breach-response planning.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52026PC0681, last accessed on September 25, 2026.
[8] https://www.aepd.es/prensa-y-comunicacion/blog/primera-notiviacion-brecha-datos-personales-causada-por-ataque-ejecutado-mediante-agente-ia, last accessed on September 25, 2026.

| OTHER COUNTRIES



9 **U.K. - ICO launched Consultation on Draft Anonymisation and Pseudonymisation Guidance for Research**[9]

ICO launched a consultation on its *Draft guidance on the use of anonymisation and pseudonymisation for research purposes* (**"Draft Guidance"**), covering research, archiving and statistical (**"RAS"**) processing under the UK GDPR. The consultation remains open until October 19, 2026. The Draft Guidance is particularly relevant to universities, healthcare and life sciences organisations, pharmaceutical and biotech businesses, public bodies and AI developers relying on research datasets.

The Draft Guidance confirms that personal data can only be processed for RAS purposes when the processing either converts personal data into non-identifiable data, or where the research objective cannot be achieved without using personal data. It mandates that organisations must begin by considering whether their research goals can be met using anonymised data, and only move to pseudonymisation (retaining a reduced, minimised form of such personal data) when anonymisation could prevent the research objective from being achieved.

The Draft Guidance is particularly relevant to research and AI projects that need large datasets but cannot always work with fully anonymous information. Organisations should assess whether anonymisation can meet the research objective first and, where it cannot, document why pseudonymised data is necessary and what technical environment - such as a trusted research environment or federated analysis - is used to reduce access to identifiable data.

[9] https://ico.org.uk/media2/goaamspg/draft-guidance-on-the-use-of-anonymisation-and-pseudonymisation-for-research-purposes.pdf?fbclid=IwY2xjawUQWZVwZG9mBWV4dG4DYWVtAjEwAGJyaWQRMVlKMkJXVlZremZkZHluUjRzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEekrkN88oBslpYbhbfHYUcfDY55CyTlOyTHEAH4NFfu-fFxKdYt0Asw2hMBSA_ae, last accessed on September 23, 2026.

10

Australia - Government proposed New Bill for Digital Duty of Care for Online Platforms[10]

The Australian Government released an exposure draft of the Online Safety Amendment (Digital Duty of Care) Bill 2026 (**"Draft Bill"**), proposing a framework that would require online platforms to identify, assess and mitigate risks arising from their services. The Draft Bill would amend the Online Safety Act 2021 and move the framework beyond content removal towards preventive risk management. The consultation on the Draft Bill closed on September 22, 2026; it has not yet been enacted.

The proposed framework would require platforms to address risks associated with harmful content and features, particularly for children under 18. This includes protections against addictive design features, harmful content and features affecting young users' self-esteem. Social media platforms would also be required to allow users to choose whether their default feeds contain algorithmically personalised recommendations or content from accounts they follow.

The draft places greater responsibility on digital platforms to address harm arising from their design and operations rather than merely removing harmful content after it appears. It also expands the scope of online safety regulation beyond social media to gaming platforms, applications and AI chatbots. If enacted, the Bill could substantially reshape platform accountability in Australia, particularly concerning children's online safety, algorithmic transparency and regulatory enforcement

11

Canada – Canadian Music Rights body sued AI Platform over allegedly Infringing Outputs[11]

SOCAN, Canada's largest member-owned music rights organization, has filed a lawsuit against generative AI company Suno Inc., alleging that the company's platform has generated and publicly streamed AI outputs which replicate songs from SOCAN's repertoire without consent or compensation, thereby infringing the performance rights of all the original works. As per SOCAN, Suno built its business by training its generative AI models on virtually all music files openly accessible on the Internet, without obtaining the necessary permissions or licences.

The Canadian enterprise indicates that it expects further unauthorized activity to surface as litigation proceeds, and confirms that it has never licensed its repertoire to Suno nor received any royalty payments from the company. SOCAN requests the court to require Suno to comply with copyright law, halt the availability of infringing outputs, and compensate rightful holders of all such rights.

The organization has framed its broader stance around what it calls the "ART Principles" Authorization, Remuneration, and Transparency, arguing that generative AI platforms should not use copyrighted music without securing permission, paying creators, and being transparent about data use. The case adds Canada to a growing list of jurisdictions where rights organizations and record labels are pursuing legal action against AI music platforms over unlicensed training data and closely mirrored outputs.

[10] https://www.infrastructure.gov.au/sites/default/files/documents/exposure-draft-online-safety-amendment-digital-duty-of-care-bill-2026-september2026.pdf, last accessed on September 28, 2026.
[11] SOCAN v. Suno Inc. (2026).

12 **US Agencies alleged Industrial-scale AI model Distillation by China-based firms**[12]

The NSA, the Cybersecurity and Infrastructure Security Agency ('CISA'), and the FBI have issued a joint cybersecurity advisory alleging that six China-based AI companies i.e., DeepSeek, Moonshot AI, Alibaba, MiniMax, StepFun, and Z.AI, have conducted 'aggressive, malicious, and targeted' knowledge-distillation campaigns against U.S. frontier AI models since at least late 2024. According to the advisory, these firms collectively extracted billions of tokens through millions of requests targeting models built by Anthropic, OpenAI, Google, and xAI, in activity that as per agencies was likely undertaken with the awareness of the Chinese government, although direct involvement by Chinese intelligence services is not alleged.

Specific allegations include: DeepSeek being accused of drawing on multiple versions of Claude, GPT, and Gemini to help train its R1 and V3 models, while Moonshot AI is accused of extracting data from Claude to develop its Kimi K3 system and using GPT-4o outputs for Kimi K2. The agencies said this activity violates the terms of use of the U.S. AI companies involved and threatens America's technological leadership in the field. The advisory recommends that AI companies take three immediate steps: Implement detection and mitigation systems for anomalous or malicious prompts, accounts, and network behaviour; Deploy targeted response changes, such as subtly downgrading model outputs or applying differential privacy for suspected distillation attempts, varying these changes to complicate evaluation by bad actors; And establish cross-organization intelligence sharing among model providers, cloud platforms, and API aggregators.

The advisory is significant because it treats large-scale model distillation as both a cybersecurity and model-protection risk. AI providers should consider whether API monitoring, rate limits, anomaly detection and cross-provider intelligence sharing are sufficient to identify coordinated extraction attempts, particularly where repeated requests may be used to reproduce model capabilities without direct access to model weights.

13 **Australia - Australian Private Member's Bill proposed AI shutdown and Data-Centre Controls**[13]

Independent MP Andrew Gee introduced the AI Kill Switch and Data Centre Control Bill 2026 (**"Bill"**), a private member's bill currently before the House of Representatives. The Bill would require providers of certain high-capacity AI technologies to maintain technical mechanisms capable of reducing or shutting down system operation in specified circumstances.

At the centre of the proposal is a mandatory shutdown capability alongside layered response mechanisms. Providers within scope would be required to maintain processes for serious AI incidents, including reporting specified critical safety incidents to the Government within 24 hours. The Bill would also give the responsible Minister emergency powers to direct a provider to throttle, suspend or shut down an AI system where a significant threat to public safety, human life or the economy is identified. Non-compliance could attract civil penalties of up to A$30 million per day.

The proposed Bill would also establish a moratorium on the construction of new AI data centres and major expansions of existing facilities until specified safeguards are put in place. The Bill's sponsor pointed to the growing energy and water requirements of data centres, particularly their potential impact on regional communities and agricultural resources.

[12] https://media.defense.gov/2026/Sep/08/2003992823/-1/-1/0/CSA_CHINA_BASED_AI_COMPANIES_MALICIOUS_DISTILLATION_AGAINST_US.PDF, last accessed on September 25, 2026.

https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7537, last accessed on October 3, 2026.

The Bill is not Government policy and has not been enacted. Its significance lies in the type of controls it proposes: technical shutdown capability, rapid incident reporting and limits on data-centre expansion. Even if the Bill does not progress in its current form, it reflects a growing policy debate around whether advanced AI systems should be required to maintain enforceable human override and emergency controls

14 **Major Social Media Platform agreed Settlement over Teen Safety**[14]

TikTok Inc. (**"TikTok"**) agreed to pay Alabama at least $100 million to settle a lawsuit alleging that the platform used addictive features and misled consumers about protections for young users. The settlement was reached shortly before the case was scheduled to go to trial, which would have been the first state trial against the platform over alleged harms to teenagers.

Under the agreement, TikTok must introduce several new protections for teenagers in Alabama, including a two-hour daily usage limit, restrictions on access between midnight and 6 a.m., stronger age verification, a default non-personalised feed and a ban on cosmetic filters. The platform will also add "productive pauses" during extended use and strengthen parental controls and content-moderation measures.

The settlement is significant as it adds to growing legal pressure on social-media companies over teen safety, addictive platform design and online harms. It also gives Alabama concrete requirements governing how TikTok operates for young users, while avoiding a trial that could have exposed the company's internal practices to public scrutiny. The agreement could also have wider implications as other U.S. states pursue similar claims against TikTok.

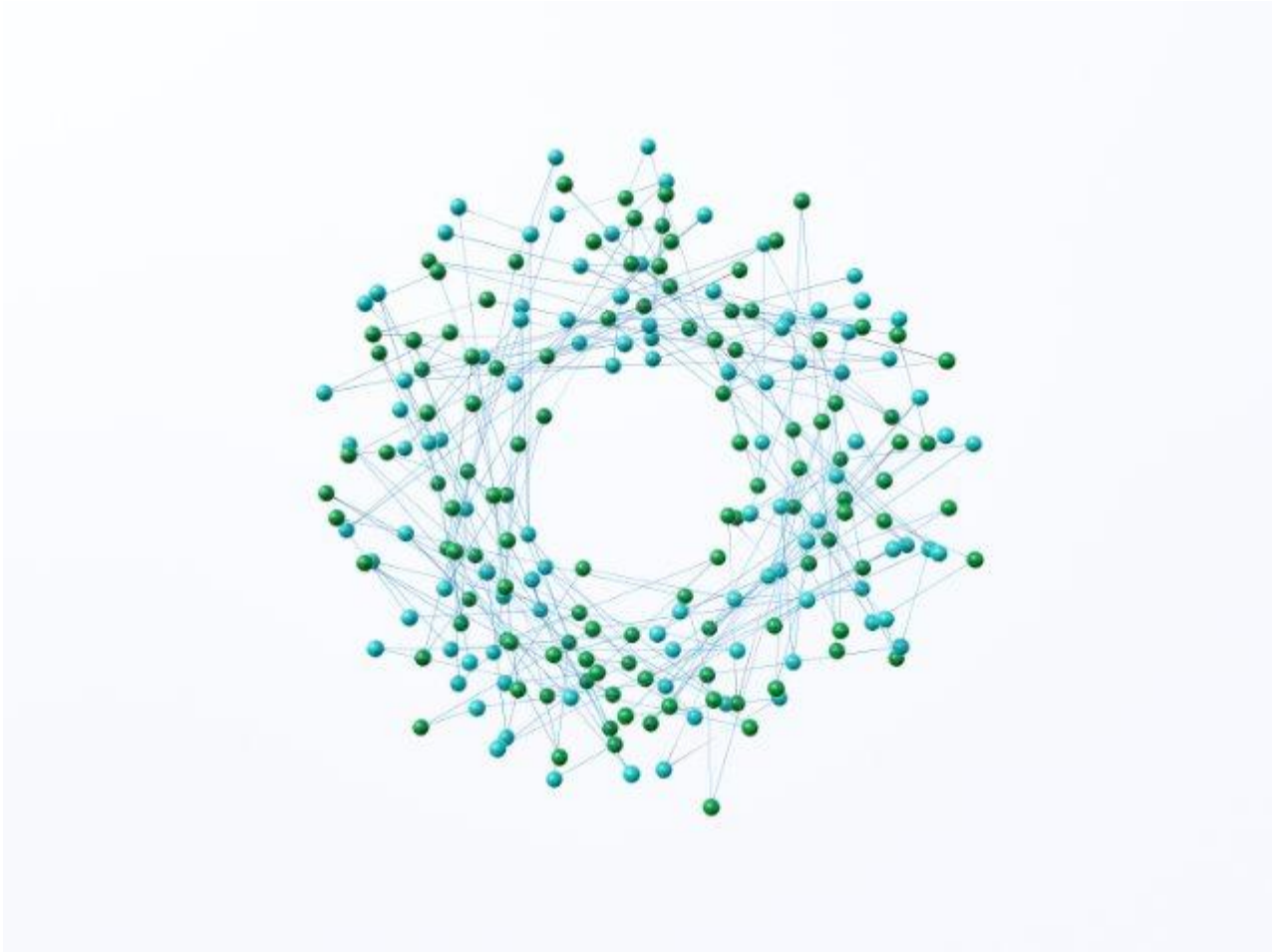


[14] State of Alabama v. TikTok Inc. et al.

ABBREVIATIONS

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

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
CCPA	Central Consumer Protection Authority
CCTV	Closed-Circuit Television
DPC	Data Protection Commission
DPDP Act	Digital Personal Data Protection Act, 2023
GDPR	General Data Protection Regulation
NCH	National Consumer Helpline
RBI	Reserve Bank of India
RTI	Right to Information Act, 2005



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 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.

Shirin Patel, partner, is a seasoned professional with over 25 years of leadership experience in legal, compliance and governance roles within the insurance sector. Her expertise spans regulatory compliance, corporate advisory, risk and contract management, data privacy implementation and governance frameworks. She is also a qualified Company Secretary and holds a Post Graduate Diploma in Cyber Law & Cyber Forensics from the National Law School of India University.

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.