# Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

April 2025

Your Privacy Digest is filled with the latest developments in the field of privacy and data protection across the globe

# PRIVACY DIGEST

Welcome to this edition of our Privacy & AI Digest, where we bring you the latest developments shaping the intersection of artificial intelligence, data privacy, and digital governance. In the U.S., a federal judge has denied Elon Musk's attempt to halt OpenAI's for-profit transition, while the courts also reaffirmed that AI-generated content without human authorship is ineligible for copyright protection. Across the Atlantic, French publishers are taking Meta to court over alleged AI training violations, highlighting growing tensions around intellectual property. In Asia, Alibaba has introduced a new open-source AI model to challenge global rivals, India is pushing forward with a light-touch regulatory approach to foster innovation, and China has unveiled stringent AI transparency laws that surpass even the EU's AI Act. Meanwhile, a massive X/Twitter data breach underscores the rising threat of insider risks and the urgent need for robust data governance. Stay tuned as we unpack these key updates and their global implications.

# PRIVACY DIGEST

## ASIA PRIVACY UPDATES

### Alibaba Unveils Open-Source AI Model to Rival OpenAI & DeepSeek

Alibaba has launched Qianwen QwQ-32B, a new open-source AI model that it claims achieves a major leap in mathematics, coding, and general reasoning, outperforming OpenAI's o1-mini and competing closely with DeepSeek-R1. According to benchmark tests, QwQ-32B excelled in mathematical ability (AIME24), coding proficiency (LiveCodeBench), and instruction-following (IFEval), surpassing even DeepSeek-R1 in key evaluations. This release signals China's aggressive push to lead the global AI race and reinforces the growing trend toward open-source AI. Stay tuned for more updates on AI governance and innovation.

### China Enacts Strict AI Transparency Law; More Detailed Than EU AI Act

China has introduced new AI transparency regulations, requiring clear labeling of AI-generated content across text, audio, images, video, and virtual scenes—stricter and more detailed than the EU AI Act's provisions. The law mandates prominent warnings in interactive interfaces and embedded metadata for downloadable content. Online platforms must verify AI-generated content disclosures before approving applications for release. Service providers are also required to outline labeling methods and compliance in user agreements. Set to take effect in September 2025, this regulation underscores China's focus on AI governance.

### Proposed Income Tax Bill 2025 Raises Alarms Over Digital Privacy Rights

The newly proposed Income Tax Bill, 2025, aims to modernize and streamline tax procedures but has sparked privacy concerns by granting tax authorities expanded powers to access individuals' digital spaces, including emails and social media, during investigations. While intended to enhance enforcement and curb evasion, critics warn that such access risks infringing on citizens' digital privacy and opens the door to potential misuse. As the bill moves through legislative processes, it's vital to strike a careful balance between effective tax regulation and the protection of fundamental privacy rights, ensuring accountability does not come at the cost of civil liberties.

# PRIVACY DIGEST

### Reliance Launches Jio Coin, a New Step in India's Digital Economy


Reliance Industries has introduced Jio Coin, a blockchain-based reward token integrated into the Jio digital ecosystem. Although the official launch is pending, users can already earn Jio Coins by engaging with platforms such as JioSphere, JioMart, JioCinema, and MyJio. The token currently holds a value of ₹21.99 and can be used for services like mobile recharges and shopping discounts. Developed in partnership with Polygon Labs, Jio Coin aims to promote Web3 adoption in India. Its future impact will depend on user participation, regulatory developments, and the expansion of use cases within the Jio ecosystem.

## EU PRIVACY UPDATES

### French Publishers & Authors Sue Meta Over AI Copyright Infringement

In a first-of-its-kind lawsuit in France, major French publishing and author organizations, SGDL, SNAC, and SNE, are suing Meta for allegedly using copyrighted works without permission to train its AI models. Calling Meta's actions "parasitic," the plaintiffs argue that AI companies must respect copyright laws, ensure transparency, and compensate creators for their work. This legal battle aligns with the EU's AI Act and global efforts to defend intellectual property against unauthorized AI training. The lawsuit seeks the removal of unauthorized datasets and aims to set a precedent for future copyright actions against AI companies. Expect more legal challenges ahead as the AI copyright debate intensifies.

# PRIVACY DIGEST

## US PRIVACY UPDATES

### Judge Denies Elon Musk's Bid to Halt OpenAI's For-Profit Shift, But Case Moves Forward

A federal judge has rejected Elon Musk's request for a preliminary injunction to stop OpenAI's transition into a for-profit company. Musk, alongside Shivon Zilis and xAI Corp., argued that OpenAI's shift violated antitrust and state laws, even submitting email exchanges to support his claims. However, the court ruled that the plaintiffs failed to meet the high burden of proof required for such extraordinary relief. While the injunction was denied, the judge offered to fast-track the case's core claims, prioritizing public interest concerns. This legal battle is far from over—expect more developments soon.


### U.S. Appeals Court Rejects Copyright for AI-Generated Work Without Human Author

The U.S. Court of Appeals has ruled that AI-generated works cannot be copyrighted unless a human is involved. The case involved Dr. Stephen Thaler, who sought copyright for an artwork created by his AI, the "Creativity Machine," listing the AI as the sole author. The Copyright Office denied the application, citing its human authorship requirement, and the court upheld this decision. This ruling sets a major precedent in the ongoing legal battle over AI-generated content, reinforcing that copyright law still centers on human creativity.

# PRIVACY DIGEST

## FINES AND PENALTIES

### Massive X/Twitter Data Leak Exposes 2.87 Billion Profiles Amid Insider Threat Allegations

A massive data leak exposing 2.87 billion X/Twitter profiles—far exceeding the platform's current user base—has surfaced on Breach Forums, with speculation pointing to a disgruntled former employee as the source. The leaked 34GB file, posted by user ThinkingOne, includes detailed metadata such as exact account creation dates, time zones, and app usage data, and merges information from a 2023 scraping breach that also included email addresses. While the insider theory remains unconfirmed, experts highlight the breach as a serious reminder of the risks posed by insider threats and inadequate data governance. Despite attempts to notify the company, X has yet to respond publicly. Security professionals urge users to enable multi-factor authentication and call for stronger access controls and breach detection systems to prevent future incidents.

### HDFC Securities Pays ₹65 Lakh to Settle SEBI Case

HDFC Securities has paid ₹65 lakh to SEBI to settle regulatory violations related to IT system failures, inadequate disaster recovery (DR) drills, and weak cybersecurity measures. The violations included lack of capacity alerts, incomplete server monitoring, and insufficient categorization of critical assets. Though the settlement closes this case, SEBI reserves the right to take further action if any terms are breached or disclosures are found incomplete.

### Oracle Confirms Cloud Breach, Downplays Impact

Oracle has confirmed a cloud data breach after a hacker claimed to have stolen data from over 140,000 tenants. While the company denies any major impact, leaked credentials, customer records, and internal videos suggest otherwise. The breach reportedly involved older systems, but experts say recent data may also be affected. The FBI and CrowdStrike are investigating the incident.

# PRIVACY DIGEST

## $10M Ransomware Attack Disrupts Kuala Lumpur Airport Operations


Kuala Lumpur International Airport (KLIA) suffered a major ransomware attack on March 23, causing widespread disruptions to flight info systems and check-in services. The attackers demanded $10 million, but Malaysian PM Anwar Ibrahim firmly refused to pay, calling the impact "quite heavy." While airport operator MAHB claimed operations continued as normal, experts warn the incident highlights critical infrastructure vulnerabilities in the region. Investigations are ongoing, with cybersecurity firms urging faster recovery plans and stronger defenses against future threats.

## Hackers Hit Polish Space Agency POLSA in Cybersecurity Incident


The Polish Space Agency (POLSA) took its network offline on March 4 following a cyberattack, possibly linked to an internal email compromise. Officials confirmed unauthorized access but said affected systems have been secured with help from national cybersecurity teams. The agency, part of the European Space Agency, has shifted to phone communications as investigations continue. While the source remains unknown, Poland's digital authorities suggest pro-Russian hackers may be involved due to Poland's support for Ukraine.

## CaixaBank Fined €3.5M for GDPR Breach

Spain's data protection authority (AEPD) has fined CaixaBank €3.5 million for GDPR violations after a complaint revealed unauthorized access to customer data via its online platform. The AEPD found that CaixaBank failed to implement adequate security measures, violating Articles 5(1)(f) and 25 of the GDPR, which mandate data protection by design and default.

# PRIVACY DIGEST

## Romania Fines NTT DATA RON 124K for GDPR Breach

Romania's data watchdog (ANSPDCP) fined NTT DATA Romania RON 124,430 after a cyberattack exposed sensitive personal data, including IDs, financial info, and employment details. The company failed to notify authorities within the mandatory 72-hour window and lacked sufficient security measures. The fine has been paid.

## Apple Fined €150M by France for Antitrust Violation

France's antitrust watchdog has fined Apple €150 million ($162.4M) over its App Tracking Transparency (ATT) tool, citing abuse of market dominance from 2021 to 2023. Regulators say the tool unfairly hindered advertisers and smaller publishers by restricting data access. While Apple expressed disappointment, it's not required to modify ATT yet. Investigations in other EU nations are still ongoing.

## $500,000 Stolen in Australian Super Fund Cyberattack


A cyberattack on multiple Australian superannuation funds led to the theft of $500,000 from four accounts, with data from thousands of members potentially compromised. While most hacking attempts were thwarted, funds like AustralianSuper, Rest, and Hostplus were affected. The breach was linked to reused leaked passwords and involved credential stuffing techniques. Authorities and funds are urging members to update passwords, enable multi-factor authentication, and remain vigilant. A coordinated government response is underway to bolster defences across the superannuation sector.

# PRIVACY DIGEST

## AI UPDATES

### ChatGPT Can Now Create Fake Aadhaar & PAN Cards


OpenAI's ChatGPT (GPT-4) has sparked serious privacy concerns after users demonstrated its ability to generate highly realistic fake Aadhaar and PAN cards using minimal input like name, date of birth, and address. While these documents lack official security features, their near-perfect appearance has raised alarms about potential misuse in cybercrimes and identity fraud. Social media users are questioning how the AI knows the exact formats and whether sensitive datasets were involved in training, prompting renewed calls for stricter AI regulation to prevent malicious exploitation.

### Ghibli Filter Sparks Privacy Fears Among Social Media Users

A viral post has stirred panic among social media users, claiming that AI-generated Ghibli-style portraits could be reverse-engineered to reveal the original photos—sparking concern among those using the trend for "soft launching" relationships. While experts argue this is technically unlikely, the controversy highlights broader privacy concerns. By uploading images to use such filters, users may unknowingly allow platforms to process and store personal data, raising questions about consent and data usage in the age of AI-powered fun.

### Amazon to Store All Alexa Voice Commands in the Cloud from March 28

Amazon will begin automatically uploading all Alexa voice recordings to the cloud starting March 28, eliminating the option to process requests locally. This move supports the rollout of Alexa+, its new AI-powered assistant, but raises privacy concerns as users must now allow cloud storage to maintain features like Voice ID. Those opting out will lose access to key functionalities. While Amazon claims recordings are encrypted and privacy controls remain available, critics highlight past incidents involving misuse of voice data and lack of transparent consent.

# Azure Data Protection Consultants LLP

## Contact us for any queries:


https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com


## DISCLAIMER