
K&L GATES
GLOBAL DATA PROTECTION INSIGHTS
AUGUST 2026

OVERVIEW

Staying ahead of data protection developments across multiple jurisdictions is one of the most demanding challenges facing businesses today. Our Global Data Protection Insights newsletter distills the most important regulatory, enforcement, and litigation developments from Australia, Europe, China, the United States, and beyond into one concise, practitioner-authored resource. Whether you are navigating new HIPAA cybersecurity requirements, children's privacy obligations, or cross-border data transfer rules, this newsletter gives you the clarity and context to act with confidence.

CONTENTS

Industry Focus **5**
Video Game Privacy at an Inflection Point: COPPA 2.0, the Amended COPPA Rule, and the Video Game Industry 5

Practice Pulse **9**
Sarah Pearce Joins K&L Gates in London 9
From the Floor: Privacy Themes at the Video Game Bar Association Summit 10

Enforcement Updates **12**
Court of Justice of the European Union—Data Protection Caselaw Update (April 2026–July 2026) 12
CIPA Update 13
An Australian Financial Services Licensee First: Receiving an Order to Pay AU$2.5 Million for Cybersecurity Failures 14

Regulatory Updates **16**
New Data Protection Rules for Consumer Credits Creditworthiness Assessments in the European Union 16
EU Regulatory Short News 17
Is America Finally Getting a National Data Privacy Law? 19
UK Data (Use and Access) Act—The First Year 21
EDPB June 2026 Plenary Session—Introduction of new Data Breach Template 23

US National Security **25**
Supreme Court's *Chatrie* Decision Has Broader Implications for Digital Privacy and Corporate Data Governance 25

Litigation Corner **28**
GDPR Litigation—Germany's Role in Private Enforcement 28
AI Listens, but Does It Print?: Voiceprint BIPA Claims in the Northern District of Illinois 31

Editors **35**

Authors **35**

INDUSTRY FOCUS

INDUSTRY FOCUS

VIDEO GAME PRIVACY AT AN INFLECTION POINT: COPPA 2.0, THE AMENDED COPPA RULE, AND THE VIDEO GAME INDUSTRY

By: Corey Bieber, William R. Bradley II, and Destinee S. Evers

Three overlapping regulatory developments in the first half of 2026 have materially changed what the law may require of video game companies serving players in the United States. The compliance date for the amended Children's Online Privacy Protection Act (COPPA) Rule arrived on 22 April 2026 (COPPA Rule). The US Senate passed the Children and Teens' Online Privacy Protection Act (COPPA 2.0), by unanimous consent on 5 March 2026 (S.836, 119th Congress, as passed by the Senate). The Federal Trade Commission (FTC) issued an enforcement policy statement on 25 February 2026 addressing the use of age-verification technologies under the COPPA Rule.

All three of these developments have an immediate impact on interactive entertainment. Games attract mixed audiences of children, teens, and adults; free-to-play titles depend on advertising and in-game monetization; and live-service games collect behavioral, device, account, and telemetry data on a persistent basis.

The Amended COPPA Rule Is Now Fully Operative

The FTC published the amended COPPA Rule in the *Federal Register* on 22 April 2025. The amendments took effect on 23 June 2025, and operators generally had until 22 April 2026 to come into compliance. Several of the changes bear on game operators.

First, the definition of personal information now includes biometric identifiers, such as voiceprints and facial templates, along with government-issued identifiers. Voice chat features, avatar creation tools, and identity checks at account creation can each bring a game within this expanded definition.

Second, operators must obtain a separate verifiable parental consent before disclosing a child's personal information to third parties for purposes that are not integral to the service, including targeted advertising. This requirement reaches the advertising and analytics software development kits (SDKs) embedded in free-to-play mobile games, where monetization depends on sharing persistent identifiers with ad networks. A single consent that bundles collection with third-party disclosure no longer suffices.

Third, the amended COPPA Rule adds a stand-alone definition of a “mixed audience website or online service,” confirming the two-step framework under which a game that is child-directed, but does not target children as its primary audience, may collect age information through a neutral age gate and apply COPPA protections to users who identify as under 13. For publishers of titles with substantial child and teen audiences alongside adult players, the mixed audience classification remains the pivot on which most compliance obligations turn.

Fourth, operators must establish a written information security program and a written data retention policy, and they may not retain children's personal information indefinitely. Live-service games that accumulate engagement, matchmaking, and progression data over years of play will need retention schedules that tie each data category to a stated purpose and a defined period.

The amendments also impose transparency and reporting obligations on FTC-approved safe harbor programs. Certification through a program such as ESRB Privacy Certified remains available to game publishers, and participation now comes with public disclosure of membership and annual reporting to the FTC.

COPPA 2.0 Clears the Senate

S.836 would amend the COPPA statute itself, and its passage by unanimous consent signals bipartisan support for expanding federal children's privacy laws. The bill extends protections to teens aged 13 through 16; prohibits the collection, use, or disclosure of personal information of children and teens for individual-specific advertising; and grants teens rights to access, correct, and delete their information. The bill also revises the trigger for coverage: In place of the current actual knowledge standard, operators would be covered where knowledge that a user is a child or teen is fairly implied on the basis of objective circumstances. The definition of operator is updated to name mobile applications, online applications, and services delivered through connected devices.

Each of these changes would land with force in the game industry. Audience composition research, marketing plans, influencer campaigns, and content ratings could all supply the objective circumstances from which knowledge is implied, narrowing the room to treat a general audience designation as a shield. The prohibition on individual-specific advertising would apply to children and teens without a consent pathway, constraining the engagement-based advertising models common in free-to-play titles.

The House of Representatives (House) has not yet acted on the bill, and prior versions of COPPA 2.0 passed the Senate without reaching a House floor vote, so the bill's fate remains uncertain. Game companies should nonetheless treat expanded teen data protections as a future inevitability—a conclusion that current state laws support.

Enforcement Signals for Game Companies

The FTC has treated gaming as a priority enforcement area, and its recent matters reveal how privacy and monetization theories now travel together.
In its 2022 action against Epic Games, the FTC alleged that Fortnite was directed to children based on factors including its visual content, merchandising tie-ins, and audience data, and it also alleged that Epic collected children's personal information without notice or verifiable parental consent. Epic agreed to pay a US$275 million civil penalty (at the time, the largest penalty obtained for violation of an FTC rule), disable voice and text chat for children and teens by default absent affirmative consent, delete data collected in violation of COPPA, and maintain an audited privacy program. A companion order (at the time, the largest administrative order in the history of the FTC) required US$245 million in consumer redress for dark patterns in the game's purchase flows and alleged deceptive billing practices.

In January 2025, the FTC announced a settlement with Cognosphere, the operator of Genshin Impact, combining COPPA counts with FTC Act counts directed at loot box and virtual currency practices. The order requires a US$20 million payment, bars the sale of loot boxes to users under 16 without parental consent, requires deletion of data collected from children under 13 absent parental consent, and requires that loot boxes be available for direct purchase in fiat currency rather than through virtual currency bundles alone.

The FTC's US$20 million settlement with Microsoft over Xbox Live account creation completes the picture of the FTC's priorities because the account funnel, not just gameplay, was a primary focus. Among other items, the FTC alleged that Microsoft retained the personal data of children under 13 that it gained during the initial steps of the account creation process, even when the parent did not complete the process. The order required a US$20 million payment, parental consent for certain accounts created before May 2021, automatic deletion of personal data collected from children after two weeks if parental consent has not been obtained, and sharing with publishers that the user is a child when such child's personal information is disclosed.

The common thread across these matters is that regulators treat audience, data collection, social

features, and monetization design as a single, interconnected system—not separate compliance questions. An operator defending its age gate should expect its purchase flow, chat defaults, and SDK stack to be examined in the same matter.

Age Assurance and the Mixed-Audience Problem

COPPA contains a structural tension for mixed-audience games: The COPPA Rule requires parental consent before collecting personal information from a child, yet several age-assurance methods require collecting personal information to determine whether the user is a child at all. The FTC examined this tension at its 28 January 2026 workshop on age-verification technologies and responded with its 25 February 2026 enforcement policy statement. Under the statement, the FTC will not bring a COPPA enforcement action against operators of general audience and mixed audience services that collect, use, or disclose personal information for the sole purpose of determining a user's age without first obtaining verifiable parental consent, provided the operator limits the data to that purpose, deletes it once the age determination is complete, obtains confidentiality and deletion commitments from vendors, provides notice, maintains safeguards, and uses methods that are reasonably accurate.

The statement has limits that matter to game companies. It does not extend to services directed to children as a primary audience; it does not bind state attorneys general, who retain independent COPPA enforcement authority; and it may be withdrawn. Within those limits, it meaningfully reduces the federal enforcement risk of deploying age estimation or verification at account creation in mixed-audience titles. It also signals something more pointed: The FTC expects operators of such titles to know the ages of their players. The FTC has stated its intent to initiate a review of the COPPA Rule to address age-verification mechanisms through amendment.

Practical Steps for Game Companies

For publishers, platforms, and developers assessing their position against this framework, several near-term actions follow:

- Reassess the audience classification of each title against the multifactor test, using current audience data, marketing plans, and content ratings, and documents the analysis and its refresh cadence.
- Inventory advertising and analytics SDKs, map each disclosure of persistent identifiers against the separate consent requirement, and confirm contractual limits on downstream use.
- Review monetization flows for younger users, including purchase consent mechanics, odds and pricing disclosures for randomized items, and the presentation of virtual currency.
- Confirm that protective defaults for chat, friend requests, matchmaking, and user-generated content activate for users identified as minors after the age gate.
- Adopt or refresh the written security program and retention schedule to cover telemetry and engagement data. Safe-harbor certification through a program such as ESRB Privacy Certified is worth evaluating now.
- Monitor House action on S.836 and the FTC's anticipated rulemaking on age verification; both could shift the compliance calculus materially.

PRACTICE PULSE

PRACTICE PULSE

SARAH PEARCE JOINS K&L GATES IN LONDON

Sarah Pearce has joined K&L Gates as a partner in the firm's London office, strengthening the firm's global bench with a practice she built at the intersection of data privacy, cybersecurity, and artificial intelligence (AI).

Sarah's path into the field has been international from the start. She earned an English law degree from King's College London and a French law degree from the University of Paris-Sorbonne, and she worked at the European Commission in Brussels before qualifying as a lawyer in both London and Paris. Now based in London, her practice spans data privacy, cybersecurity, and AI across all sectors. She advises clients on risk management and compliance across the United Kingdom, Europe, the Middle East, and Africa, covering policy preparation, cross-border data transfers, and transactional matters. Data breach and cyber-incident response, along with regulatory investigations, have become a growing part of her practice as the threat landscape intensifies.

Over the years, Sarah completed secondments to the privacy teams at Yahoo and UBS and served as an interim data protection officer for Richemont. Those front-row seats to the data, privacy, and security pressures facing major organizations across sectors shaped the pragmatic, commercial approach she brings to client work today.

The breadth of opportunity, collaborative culture, and extensive global footprint at K&L Gates all appealed to Sarah—but it was the people she met along the way who sealed the deal.

SARAH PEARCE
Partner
London
Sarah.Pearce@klgates.com

FROM THE FLOOR: PRIVACY THEMES AT THE VIDEO GAME BAR ASSOCIATION SUMMIT

By: Destinee S. Evers, Eric F. Vicente Flores

Destinee Evers (Seattle) attended this year's Video Game Bar Association (VGBA) Northwest Summit in Seattle in May. The two-day event featured panelists from around the world and across the interactive entertainment space. Notable topics included cross-border compliance, privacy developments like the Children and Teens' Online Privacy Protection Act, and new trends for child safety regulation.

A key theme was the tension between privacy regulation and child safety requirements. Complying with child safety protections may require companies to collect private information to comply with obligations, such as age verification, that users would expect to be private or out of scope for relevant data collection. In some countries, data privacy regulations that minimize collection may even conflict with child safety regulations that require more data gathering. Panelists emphasized the practical importance of clear user-facing messaging to explain why such data is being collected, helping address concerns that companies are overreaching in their data practices.

One of the key child safety issues that is coming up this year is age verification in app stores. In 2025 and 2026, Texas, Utah, Louisiana, and California each enacted laws requiring app stores and related platforms to verify users' ages and, in most cases, obtain parental consent before minors can download or purchase apps.

These laws target app store providers and app developers. Texas (SB 2420), Utah (SB 142), and Louisiana (HB 570) impose obligations on those who own, operate, or control app stores, as well as developers who distribute apps through those platforms. California (AB 1043) takes a broader approach, extending obligations to operating system providers who must transmit age verification signals to developers through a real-time application programming interface.

All four states require age verification at account creation, using four age brackets: under 13, 13 to 15, 16 to 17, and 18 and older. Texas, Utah, and Louisiana require minors' accounts to be linked to a parent account, with verifiable parental consent needed before any download or purchase. California's signal-based model requires operating system providers to collect age data at device setup and share age-bracket signals with developers upon request.

Each law includes a form of safe harbor. Texas, Utah, and Louisiana shield developers who rely in good faith on app store age data and apply widely adopted industry standards consistently. California protects operating system providers and app stores that make a good-faith compliance effort, accounting for available technology and reasonable technical limitations.

The major app stores are already responding. Leading mobile application marketplaces have begun implementing age assurance, age verification, and parental consent requirements for new users in Texas and have indicated that these measures will be expanded to other jurisdictions as comparable laws take effect.

Organizations operating in these states should take note: Enforcement timelines range from January 2026 (Texas) to January 2027 (California).

ENFORCEMENT UPDATES

ENFORCEMENT UPDATES

COURT OF JUSTICE OF THE EUROPEAN UNION—DATA PROTECTION CASELAW UPDATE (APRIL 2026–JULY 2026)

By: Dr. Thomas Nietsch, Lorenz Strub

Case C-312/24—4 June 2026 | GDPR/Law Enforcement Data in Personnel Files

Topic: Personal data from a criminal investigation (without conviction) stored in a police officer's personnel file, allegedly impeding his promotion.

Key Findings:

- The General Data Protection Regulation (GDPR) (not Directive 2016/680) governs where data obtained during a criminal investigation is subsequently processed for *human resources management purposes*, regardless of whether the data originated within the same public authority.
- Processing may be lawful under Article 6(1)(c) GDPR if based on a clear, precise, and foreseeable national legal obligation—but must be *proportionate* and time limited.
- Article 10 GDPR conditions apply even where no offense was established. If retention is no longer justified, the *right to erasure* under Article 17 GDPR revives.

Case C-414/24—18 June 2026 | GDPR/Parallel Complaint and Civil Proceedings

Topic: The Austrian Data Protection Authority dismissed a GDPR complaint solely because a parallel civil court action on the same matter was pending.

Key Findings:

- Article 77 and Article 79 GDPR remedies are *independent and may run in parallel*. A supervisory authority cannot refuse to act solely because civil proceedings are ongoing.
- Member states may, however, provide for a *suspension mechanism* allowing the authority to stay its proceedings pending a final civil judgment.

Case C-484/24—18 June 2026 | GDPR/Unlawfully Obtained Evidence

Topic: Employer accessed a dismissed employee's private eBay account using retained login credentials and sought to rely on the resulting data as evidence in labor court proceedings.

Key Findings:

- The GDPR and the Charter of Fundamental Rights of the European Union do *not automatically prohibit* the use of unlawfully obtained personal data as evidence. The right to data protection must be balanced against the right to a fair trial; a breach of Article 13 GDPR does not by itself exclude the evidence.
- The data minimization principle does not require a separate proportionality assessment where its requirements are already satisfied.
- Before disclosing data to parties or third parties, courts must *limit disclosure to what is necessary* and adopt protective measures where appropriate.

CIPA UPDATE

By: Katy M. Ramos and Michael J. Stortz

Relief may be on the horizon for businesses inundated with pre-suit notice letters, lawsuits, and arbitration demands under the California Invasion of Privacy Act (CIPA), challenging the use of common third-party technologies on consumer-facing websites. The flood of CIPA claims is due in part to conflicting trial court interpretations of this decades-old statute, enacted decades before the modern Internet. State and federal trial court judges in California have reached diametrically opposite conclusions as to CIPA's scope. An ongoing appeal, as well as pending legislation, may provide some long-overdue clarity for businesses confronted with these claims.

The appellate matter, currently pending before California's Second District Court of Appeal under *Variety Media LLC v. Superior Court*, presents the question of whether the trap-and-trace and pen register provisions of CIPA even apply to online data. The lawsuit began with defendant Variety Media unsuccessfully filing a demurrer to plaintiffs' complaint in the trial court on the grounds that the CIPA trap-and-trace and pen register provisions are limited to telephonic data and do not apply to online data (such as IP addresses and routing information). While this argument had been accepted in prior nonprecedential decisions, the trial court overruled the demurrer, leading Variety Media to petition for interlocutory appellate review. Although such review is exceedingly rare, the Second District Court of Appeal issued a show-cause order and permitted further briefing on the issue. Amicus briefs filed on behalf of numerous interested third parties and supplemental briefs filed by Variety Media have made a compelling case that the California Consumer Privacy Act, rather than CIPA, is the appropriate vehicle for regulating online privacy and that the CIPA provisions by their terms do not extend to online data sharing. Oral argument is scheduled for 25 August 2026, with a decision expected before the end of the year.

As for legislative reform, earlier this year a business coalition and other interested parties encouraged efforts to reform the CIPA statute. As recently amended, SB 690 would preclude private enforcement of claims for alleged violation of CIPA's trap-and-trace and pen register provisions, to the extent such claims arise from conduct on an Internet website or online or mobile application. The amendment would apply retroactively to claims commenced two years before the bill's proposed operative date. Further action is expected before end of the legislative session on 31 August 2026.

Together, *Variety Media* and pending legislative reform offer two promising paths to clarify the scope of the CIPA statute and perhaps provide significant relief to businesses confronted with claims invoking the statute. In the meantime, businesses should continue to evaluate the use of cookies, analytics, and similar technologies, and make appropriate disclosures as to the same.

AN AUSTRALIAN FINANCIAL SERVICES LICENSEE FIRST: RECEIVING AN ORDER TO PAY AU$2.5 MILLION FOR CYBERSECURITY FAILURES

By:Cameron Abbott, Emre Cakmakcioglu, Annaliese Filippis, Madison Jeffreys, Daniel Knight, Alex Parker, Rob Pulham

In a key decision against an Australian financial services license (AFSL) holder, the Federal Court of Australia has ordered the AFSL holder to pay AU$2.5 million in penalties for inadequate cybersecurity measures. The Australian Securities and Investments Commission (ASIC) took action following a cyberattack on the AFSL holder's information technology (IT) systems, resulting in approximately 385 gigabytes of data being downloaded from its servers.

This is the first time civil penalties have been imposed for cybersecurity failures pursuant to general AFSL obligations. The court found the AFSL holder failed to comply with the following obligations under the Corporations Act 2001 (Cth):

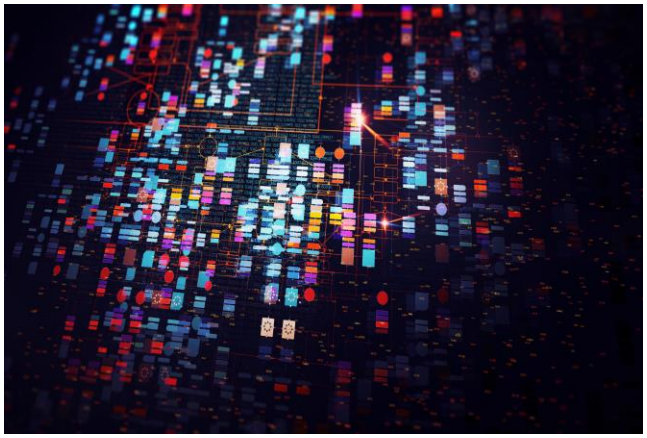
- *Efficient, honest, and fair financial services* (s 912A(1)(a)): The AFSL holder lacked an adequate incident response plan, such as monitoring threat alerts or providing mandatory cybersecurity awareness training.
- *Adequate resources* (s 912A(1)(d)): The AFSL holder delegated responsibility for its IT security measures to staff without adequate skills or knowledge and did not dedicate sufficient financial resources toward adequate cybersecurity measures.
- *Adequate risk management systems* (s 912A(1)(h)): The AFSL holder failed to implement, maintain, and monitor controls outlined in its risk management system, including under its IT Information Security Policy, Cyber and Information Security Policy, and its annual audits of custodial services.

In addition to the AU$2.5 million penalty and AU$500,000 in costs awarded to ASIC, the AFSL holder must undertake a compliance program that involves engaging an independent expert to ensure its cybersecurity and cyber resilience systems are reasonably managed. Importantly, the court found the penalties and remediation costs far exceeded what it would have cost the AFSL holder to implement adequate controls in the first place.

Key takeaways are as follows:

- Australian financial services licensees must fully implement controls in their risk management systems and maintain adequate resources, systems, and training.
- ASIC will penalize underinvestment in cybersecurity, with penalties likely to exceed the costs of initially implementing adequate controls.

You can read more from ASIC's media release here.



REGULATORY UPDATES

REGULATORY UPDATES

NEW DATA PROTECTION RULES FOR CONSUMER CREDITS CREDITWORTHINESS ASSESSMENTS IN THE EUROPEAN UNION

By: Dr. Ulrike Elteste

By 20 November 2026, the rules of the revised Consumer Credit Directive (Directive (EU) 2023/2225) (the Directive) will take effect, as the period set for its transposition into the national laws of the EU member states ends. In addition to further regulation of creditors for consumer credits, the Directive also provides for data processing rules in context of creditworthiness checks.

Scope

The Directive regulates credit agreements with consumers. Contrary to the previous version of the Directive, it applies to credit involving amounts below €200 and even most cases of credit granted free of interest and without any other charges.

The Directive does not apply to loans of more than €100,000. It also does not apply to credit agreements covering the granting of credit secured by immovable property and credit agreements the purpose of which is to finance the acquisition or retention of property rights in land or in an existing or projected building.

The Directive includes rules on pre-contractual transparency, advertising, the content of credit agreements, and creditworthiness assessments.

Registration Obligations for Creditors and Intermediaries

Creditors and credit intermediaries must register with the financial services supervisory authorities. Due to the extended scope of the Directive, this will be a new requirement for some companies. Holders of licenses for banking and payment services are exempt, and further exceptions for small and medium-sized companies apply.

Disclosure of Personalized Pricing Based on Automated Processing

Where a consumer is presented with a personalized offer based on automated processing of personal data, the creditor or credit intermediary must inform the consumer of this. This aligns broadly with already existing obligations under Article 22 of the General Data Protection Regulation (GDPR) governing automated decision-making with legal effect for data subjects.

Creditworthiness Assessments

Creditors may only grant credit to consumers if they conclude that it is likely that the consumers can meet their obligations. This must be based on an assessment of their creditworthiness, including relevant and accurate information on a consumer's income, expenses, and other financial and economic circumstances. In general, the assessment must be necessary and proportionate to the nature, duration, value, and risks of the credit. The Directive provides specific rules for processing of consumer data in the context of creditworthiness assessments, specifying and in part overruling the generic provisions of the GDPR as follows:

- Special categories of personal data (Art. 9(1) GDPR), including data revealing racial or ethnic origin, political opinions, religious beliefs, health data, biometric data, and data concerning sex life or sexual orientation must not be used in the creditworthiness assessment.
- Publicly available personal data obtained from social networks must not be used for creditworthiness assessments.
- Any information obtained for the assessment must be appropriately verified, where necessary,

through reference to independently verifiable documentation.

- Where the creditworthiness assessment involves the use of automated processing of personal data (e.g., the calculation of a scoring value), the Directive grants consumers the right to request (i) a clear and comprehensible explanation of the assessment, including the logic and risks involved in the automated processing and its significance and effects on the decision; (ii) the right to express the consumer's own point of view; and (iii) the right to request a review of the assessment and the decision on the granting of credit by a human.
- Databases offering creditworthiness assessments of consumers in the European Union must only provide their services to creditors who are properly registered in an EU member state and comply with the GDPR.

EU REGULATORY SHORT NEWS

By: Dr. Ulrike Elteste

Stakeholders Seek Clarity on EU Political Advertising Rules

Regulation (EU) 2024/900 on the transparency and targeting of political advertising has been applicable since October 2025. Among other things, the law limits the sale of personal data for targeted political advertising, requires the data subject's explicit consent, and sets out comprehensive transparency obligations. The law prohibits "profiling" and the targeting of young people who are one year or more under voting age. The European Data Protection Board (EDPB) has recently published a report on a stakeholder event where first experiences with the law were discussed. Most participants of the stakeholder event said that the relevant provisions were not workable and that, in particular, the distinction between permitted "targeting" and prohibited "profiling" was unclear. The EDPB is now working on respective guidelines.

Cyber Resilience Act Reminder

The obligation to report known vulnerabilities and security incidents to the European Union Agency for Cybersecurity under the Cyber Resilience Act (Regulation (EU) 2024/2847) starts to apply on 11 September 2026. While the other provisions of the Cyber Resilience Act start to apply only on 11 December 2027, major players have already started their supply chain due diligence and are passing on Cyber Resilience Act requirements to their suppliers through contractual means. The European Commission has published a draft guidance to assist companies in applying the Cyber Resilience Act. General information on the Cyber Resilience Act can be found on dedicated web pages of the European Commission and of the German Federal Office for Information Security.

AI Omnibus Bill Adopted

Critical deadlines under the EU Artificial Intelligence Act (EU AI Act) (Regulation (EU) 2024/1689) are being postponed by the Digital Omnibus on AI (Regulation (EU) 2026/1744), which entered into force on 27 July 2026. The law amends the existing EU AI Act and is part of an effort to accommodate industry stakeholder concerns and to harmonize the EU AI Act and other EU digital laws. In particular, the Digital Omnibus on AI regulation does the following:

- Postpones the application of the EU AI Act's rules for high-risk artificial intelligence (AI) systems until 2 December 2027 for stand-alone high-risk AI systems and until 2 August 2028 for high-risk AI systems embedded in products.
- Postpones the date of applicability of the transparency rules for providers of AI systems generating synthetic audio, image, video, or text content under Article 50(2) of the EU AI Act until 2

December 2026 for systems that have been placed on the market prior to 2 August 2026.

- Adds a new provision (Article 4a) allowing the processing of special category personal data for the purpose of bias detection and correction in AI systems and models, which functions as a legal basis under the General Data Protection Regulation (GDPR).
- Expressly prohibits AI systems that generate fake nude and sexually explicit images and videos without specific consent, as well as child pornography, if such use is reasonably foreseeable.
- Partly narrows the definition of "high-risk AI systems" and limits the responsibility of providers whose systems are modified by others after their introduction to the market.

Commission Publishes Draft Guidelines for the Classification of AI Systems

The European Commission has published draft guidelines for the classification of high-risk AI systems under the EU AI Act. They are designed to assist stakeholders in determining which rules apply to their AI systems and contain useful illustrative examples.

Commission Publishes Draft Code of Practice for Marking and Labeling AI-Generated Content

The European Commission has also published a draft of a nonbinding Code of Practice on marking and labeling of AI-generated content. It complements the transparency rules pursuant to Article 50 of the EU AI Act (Regulation (EU) 2024/1689), which will become applicable on 2 December 2026 per the Digital Omnibus on AI.

Digital Omnibus Proposal Remains Contentious

The legislative bodies of the European Union continue discussing a draft "Digital Omnibus Act." If adopted, the law would consolidate and simplify several digital laws of the European Union. It would significantly modify the GDPR. First, it would narrow the scope of applicability of the GDPR by limiting the definition of "personal data" and enabling the European Commission to determine when pseudonymized data is deemed to be anonymous. Second, the law would create a lighter regime for small and medium-sized organizations under the GDPR. Third, the rules for Internet tracking would be softened and consolidated in the GDPR. However, the bill remains controversial, and it is not clear if and when it will be adopted.

IS AMERICA FINALLY GETTING A NATIONAL DATA PRIVACY LAW?

By: Vivian K. Bridges, Lauren M. Flynn, Scott J. Gelbman, Marne Marotta

A sweeping new federal legislative proposal could reshape how US companies collect, use, and profit from consumer data. Here is what you need to know.

Your compliance team is already toggling between 20+ state privacy laws—one spreadsheet for California, another for Texas, and a third for Colorado. Meanwhile, every smartphone app is quietly sharing location data, health metrics, and browsing history with dozens of third parties. For businesses, it is an operational nightmare. For consumers, it is an invisible free-for-all. That may be about to change.

On 21 April 2026, House Republicans released the SECURE Data Act (H.R. 8413) (the Act), the most comprehensive attempt yet to create a national data privacy standard. Paired with the GUARD Financial Data Act (H.R. 8398), which covers financial institutions under the Gramm-Leach-Bliley Act, the two bills aim to eliminate gaps and overlaps in consumer data protection across the entire economy.

What Rights Would Consumers Get?

The Act would codify enforceable privacy rights against data controllers—persons that determine the purpose and means of processing personal data (financial institutions subject to the Gramm-Leach-Bliley Act are separately exempt). Consumers would gain the right to access, correct, delete, and port their data, as well as the ability to opt out of targeted advertising, data sales, and profiling decisions with significant effects.

Controllers would need to respond to verified requests within 45 days. Consumers may submit two free requests per right per year. Controllers would also need to establish an appeals process for denied requests. These are not aspirational principles; they would be enforceable, uniform, nationwide rights.

Data Minimization: No More "Collect Everything, Figure It Out Later"

Perhaps the most operationally significant provision is data minimization. The Act would limit collection to what is "adequate, relevant, and reasonably necessary in relation to each purpose for which the data is processed as disclosed to the consumer," curbing excessive collection and unanticipated secondary uses.

The Act would also require affirmative opt-in consent before processing sensitive data—a category that includes data disclosing racial or ethnic origin, religious belief, health diagnosis, sexual orientation, or immigration status; genetic or biometric identifiers; data collected from children or teens; and precise geolocation data. For companies accustomed to opt-out defaults, this would require rethinking consent architecture from the ground up.

Consider a fitness app that collects geolocation and health data: Under the Act, it would need opt-in consent before processing, and it could not quietly repurpose that data to train an artificial intelligence (AI) model or sell it to a data broker (defined as a controller that derives 50% or more of its revenue from selling data about noncustomers, excluding persons acting solely as processors).

Automated Decision-Making: When Algorithms Make Life-Altering Decisions

One of the most significant provisions targets automated decision-making. Where a controller relies on profiling to make a decision with a legal or similarly significant effect on a consumer—and that decision is made with no human review, involvement, oversight, or intervention—the Act would require disclosure and give consumers the right to opt out.

The covered categories include decisions to deny a consumer a healthcare service, a rental or lease of housing, or an employment opportunity. An employer using AI to screen out applicants, a landlord using

algorithmic tenant scoring to deny a lease, or a health insurer using automated claims adjudication to refuse coverage could all be caught. For companies that have quietly integrated AI into high-stakes decisions, this provision may demand the most immediate attention.

One Standard to Rule Them All

For many businesses, the most appealing aspect of the bill is federal preemption. The Act would bar any state or political subdivision from prescribing or enforcing any law that "relates to the provisions of" the Act—replacing the current patchwork with a single national standard. A broad coalition of industry groups, including the US Chamber of Commerce and more than 50 other business associations, have endorsed the bill on the basis that a consistent nationwide standard would strengthen trust, give consumers meaningful control over their information, and provide businesses with the certainty needed to innovate and protect data. State attorneys general would retain authority to enforce the federal standard, preserving existing enforcement infrastructure while eliminating the need for 50 separate compliance programs.

The political fault lines are familiar. Industry groups support preemption but resist broad opt-in consent. Consumer advocates resist preemption that would lower existing state protections. Enforcement would rely on the Federal Trade Commission and state attorneys general—no private right of action—a design choice that may draw criticism from consumer advocates while offering comfort to industry groups. The American Data Privacy and Protection Act (H.R. 8152) stalled over these same disputes in the 117th Congress. Whether the Act can break through remains the central question.

What Should Companies Do Now?

The legislative landscape is moving quickly. Our team is tracking the Act and the broader wave of AI and technology legislation in real time—translating developments into practical guidance for clients navigating data practices, compliance programs, and regulatory exposure. Whether you need to assess how the bill's provisions apply to your business, shape your organization's position in the legislative process, or get ahead of compliance requirements before enactment, now is the time to act. Reach out to our team for a targeted compliance readiness assessment, legislative strategy briefing, or gap analysis. Waiting until the ink is dry is a strategy with real costs.

UK DATA (USE AND ACCESS) ACT—THE FIRST YEAR

By: Noirin M. McFadden

On the first anniversary since the United Kingdom's post-Brexit reform of its data protection laws, the Data (Use and Access) Act 2025 (DUAA) became law, and we take a look back at the DUAA's first year and the changes it has brought to privacy law in the United Kingdom.

The DUAA did not have a smooth journey onto the statute book. After coming through multiple changes of UK government and two previous iterations (the Data Protection and Digital Information Bills No.1 and No.2), the DUAA finally received royal assent on 19 June 2025. Since then, elements of it have gradually come into force across the past year.

Since Brexit, the UK General Data Protection Regulation (UK GDPR) has been the basis of UK data protection law. The UK GDPR was itself an almost word-for-word restatement of the EU GDPR. This was seen as beneficial to UK and EU businesses who rely on easy transfers of personal data to and from both jurisdictions, facilitated by mutual "adequacy" decisions approving each other's laws.

The UK government was aware of the risk that if the DUAA moved the UK GDPR too far away from the EU standard, the United Kingdom could lose its EU adequacy decision. As a result, the changes made to the UK GDPR by the DUAA have been incremental, rather than a wholesale redrafting of the UK GDPR. We outline below some of the changes with particular significance to organizations doing business in the United Kingdom.

Automated Decision Making

Some of the UK GDPR amendments brought in by the DUAA could have the effect of making the United Kingdom a more welcoming jurisdiction for artificial intelligence businesses. Specifically, the DUAA loosened some restrictions on the processing of personal data in automated decision-making (ADM). Previously, this was restricted unless it was one of the following:

- Necessary for the purposes of a contract between an individual and an organization.
- Permitted by law (subject to appropriate safeguards).
- With the consent of the relevant individual.

These restrictions are now removed, and organizations are permitted to make solely automated decisions in more situations (other than decisions involving particularly sensitive, special category personal data), subject to having appropriate safeguards in place. These safeguards include that the organization must do the following:

- Provide affected individuals with information about the personal data it has used in the ADM process.
- Allow individuals to make representations of such decisions and to obtain human intervention.
- Permit individuals to contest the resulting decision.

Recognized Legitimate Interests

In order for processing of personal data to be compatible with UK GDPR, it must be justified under one of a small number of lawful bases. The most flexible of the lawful bases is the "legitimate interests" basis, but using this still requires organizations to perform a legitimate interests assessment in order to balance their legitimate interest in proposed personal data processing against the rights of the affected individuals. It has not always been clear that certain types of data processing would be regarded as balancing in favor of the organization's legitimate interests in that assessment. To provide clarity for some organizations, the DUAA has inserted a new lawful basis of "recognized legitimate interests" into the UK GDPR. These new permitted data processing activities include processing for the purposes of crime

prevention, public security, national security or defense, safeguarding, emergencies, or sharing personal data for the purposes of performing public tasks or official functions.

Assumption of Compatibility

An amendment by the DUAA to the purpose limitation principle of the UK GDPR now allows organizations who have been processing personal data for one purpose to further process the same data for another purpose. This is subject to certain conditions being met. This change to UK GDPR potentially reduces the compliance burden on organizations because they may not always now need to carry out a new compatibility test or legitimate interests assessment when they process personal data for a new purpose.

Data Subject Access Requests

Data subject access requests allow individuals to obtain a record of their own personal data being processed by an organization. As a result of changes made by the DUAA, certain aspects of the process of responding to data subject access requests that were set out only in caselaw and regulatory guidance have been codified into law. It is now clear in law that organizations are only required to carry out a reasonable and proportionate search for relevant personal data in response to a request. This will give organizations confidence that the searches they carry out are sufficiently broad and thorough in order to comply with the UK GDPR requirements.

Data Protection Complaints

For the first time, organizations are now required to facilitate individuals in making complaints about how their personal data has been handled. Organizations should have in place a clear mechanism for people to submit complaints, such as an electronic complaints form, to acknowledge complaints within 30 days and to respond to them “without undue delay.” The mechanism used to submit data protection complaints may vary, but such mechanism must be properly publicized and described in clear language. The Information Commissioner's Office (ICO) has published detailed guidance on complying with this new obligation and handling complaints.

Although it is not a strict requirement for organizations to have in place a data protection complaints policy, implementing a new policy or adapting an existing customer complaints policy to include data protection complaints is a useful way for organizations to be prepared for this new requirement and to ensure that staff are fully aware of it.

Privacy and Electronic Communications Regulations—Cookies and New Fines

In addition to changes to the UK GDPR, the DUAA has also amended the United Kingdom's laws regulating electronic marketing and the use of cookies or other online storage or access technologies. These are governed by The Privacy and Electronic Communications Regulations (PECR).

Organizations can now set a wider range of cookies and storage or access technologies without having to obtain users' consent under the PECR. Whereas previously, only “strictly necessary” cookies were permitted to be placed on devices without consent, organizations may now serve cookies for audience analytics and for website functionality without requiring users' consent. This does not mean the end of the cookie consent banner however, as consent remains a requirement for the use of other cookies, such as tracking and online advertising cookies.

Amendments by the DUAA have granted the UK regulator, the ICO, stronger powers to fine organizations who breach the PECR. The maximum fines have been increased from £500,000 to come into line with the maximum fine for breaching the UK GDPR, which is the greater of £17.5 million or 4% of an organization's global annual turnover.

The ICO is gradually publishing new guidance to reflect and explain the changes coming out of the DUAA and to help organizations to understand the new obligations they face, as well as the new opportunities available to them.

EDPB JUNE 2026 PLENARY SESSION—INTRODUCTION OF NEW DATA BREACH TEMPLATE

By: Veronica Muratori, Sarah Pearce

One of the more practically significant outcomes of the European Data Protection Board's (EDPB) June 2026 plenary session was the adoption of a common template for personal data breach notifications under the General Data Protection Regulation (GDPR).

The initiative is part of the EDPB's Helsinki Statement on enhanced clarity, support, and engagement, which aims to simplify GDPR compliance and strengthen consistency across EU member states.

The new common template is designed to help organizations and data protection authorities (DPAs) structure, harmonize, and unify their data breach notification processes across Europe.

Under Article 33 GDPR, controllers are required to notify the competent supervisory authority of a personal data breach without undue delay and, where feasible, within 72 hours. In practice, however, notification requirements and formats have varied across member states, creating operational complexity, particularly for organizations active in multiple EU jurisdictions.

The new template seeks to address this fragmentation by providing a standardized structure for breach notifications across the European Union. It includes predefined values and recommended tools for organizations to facilitate their completion of the form.

The template is currently subject to a public consultation, which is open until 5 August 2026. Stakeholders are invited to submit comments on the content of the template. Following the consultation, the EDPB will determine the timeline for implementation by all DPAs within the European Union.

In addition to the data breach template, the plenary discussions featured the European Commission's Digital Omnibus proposal. While the EDPB welcomed several proposed changes within the Digital Omnibus package, it reiterated its opposition to the proposed amendments regarding the definition of personal data. The EDPB has expressed concerns that narrowing the scope of what constitutes personal data risks significantly weakening individual data protection rights.

US NATIONAL SECURITY

US NATIONAL SECURITY

SUPREME COURT'S *CHATRIE* DECISION HAS BROADER IMPLICATIONS FOR DIGITAL PRIVACY AND CORPORATE DATA GOVERNANCE

By: Jake Bernstein, Sanjeev Bhasker, Guillermo S. Christensen, Michael Culhane Harper, Whitney E. McCollum

The US Supreme Court's (the Court) recent decision in *Chatrie v. United States*, 609 U.S. ___ (2026), marks another significant development in the Court's Fourth Amendment jurisprudence governing data privacy. Building on its decision in *Carpenter v. United States*, 585 U.S. 296 (2018) (historical cell site location information), the Court held, by a 6–3 vote, that law enforcement's acquisition of Google's "Location History" data constitutes a Fourth Amendment search. The Court's reasoning reinforces the principle that individuals maintain a reasonable expectation of privacy in comprehensive digital location information even when that information is held by a third-party technology provider.

Although this case arose from a criminal matter—a robbery of a credit union—its implications extend well beyond law enforcement investigations and into everyday life. The Court's opinion reflects an increasingly sophisticated understanding of today's data-driven economy and underscores the legal significance of location data, behavioral data, and other sensitive personal information that companies routinely collect, retain, and monetize. The decision also has important implications for organizations that collect, retain, or disclose sensitive location information, particularly as courts, regulators, and legislatures continue to scrutinize commercial data governance practices.

Background—Geofences and Data Collection

The case arose from a 2019 armed robbery investigation where law enforcement obtained a "geofence warrant" directing Google to identify devices that were present within a defined geographic area during a specified period (creating a "digital geographic fence" around the purported crime scene). The warrant initially required Google to search its vast repository of location history data (Location History) and produce anonymized records for devices within the designated area before investigators sought identifying information for specific accounts. That process ultimately led investigators to identify and charge their suspect, Chatrie.

The Court held that obtaining this Location History constituted a Fourth Amendment search. Referencing its 2018 decision in *Carpenter*, the Court reasoned that Google's Location History creates a detailed record of an individual's movements and associations, revealing intimate aspects of daily life. The Court also rejected the government's argument that users forfeit constitutional protections simply because Google as a third party stores the data, concluding that the sharing of data by ordinary use of a smartphone does not amount to voluntary choice by the user, so as to implicate the third-party doctrine.

The Court did not, however, determine whether the warrant itself satisfied the Fourth Amendment's probable cause requirements. It remanded the case to the lower courts for further proceedings.

Why This Matters

Although *Chatrie* addresses constitutional limits on the government's access to data, the decision is likely to influence broader privacy rules and regulatory expectations.

First, the Court continued a trend of recognizing that digital data differs fundamentally from traditional business records. Rather than treating location information as transactional data voluntarily shared with a service provider, the Court emphasized the comprehensive and revealing nature of continuous

digital location records (your data tells people where you are—while you are there). This reasoning may influence future disputes involving other forms of granular digital information, including precise GPS data, connected device data, and potentially artificial intelligence-derived behavioral profiles.

Second, the Court's analysis further narrows the traditional third-party doctrine in circumstances involving pervasive digital technologies. Companies should expect litigants, regulators, and courts to cite *Chatrie* in questioning whether individuals meaningfully consent to extensive data collection simply because they use modern digital services.

Finally, the opinion reinforces the belief that location information occupies a special place within privacy law because it can reveal sensitive information about an individual's health, religion, political activities, employment, personal relationships, and daily routines. This principle increasingly appears across federal and state privacy statutes, Federal Trade Commission enforcement actions, and international privacy frameworks.

Practical Implications for Businesses

For organizations that collect or process location information, *Chatrie* serves as another reminder that sensitive data governance has become a strategic legal issue rather than merely a compliance exercise.

Companies should consider the following:

- Reviewing what categories of location and mobility data are collected, how precise that data is, and whether all collection remains necessary for identified business purposes (e.g., are there zero-knowledge proof alternatives).
- Reassessing retention periods for historical location information and other highly sensitive datasets.
- Evaluating internal governance surrounding responses to law enforcement requests, subpoenas, warrants, and other legal processes involving customer data.
- Confirming that consumer-facing disclosures accurately describe location data collection, retention, sharing, and deletion practices.
- Monitoring how courts interpret *Chatrie* in future litigation involving geofence warrants and other forms of digital investigative techniques.

Looking Ahead

As data privacy continues evolving, *Chatrie* is unlikely to be the Court's last word on digital footprints. Because the Court expressly declined to determine the ultimate constitutionality of the geofence warrant at issue, significant questions remain regarding what degree of geographic scope, temporal scope, and particularity will satisfy the Fourth Amendment. Future cases will likely address those issues directly.

Beyond criminal investigations, however, the broader message is clear. Courts increasingly recognize that comprehensive digital datasets—particularly precise geo-location information—deserve heightened legal scrutiny because of the insights they reveal about an individual's livelihood. As legislatures, regulators, and courts continue to reshape privacy laws, organizations that collect sensitive personal information should anticipate greater expectations regarding transparency, necessity, data minimization, and governance.

For companies operating in today's data-driven economy, *Chatrie* represents another step in the continuing evolution of privacy laws from rules governing traditional records and physical searches to principles designed for digital datasets. More broadly, it reinforces growing expectations around transparency, data minimization, retention discipline, and governance for organizations handling sensitive personal information.

LITIGATION CORNER

LITIGATION CORNER

GDPR LITIGATION—GERMANY'S ROLE IN PRIVATE ENFORCEMENT

By: Andreas Müller

Under the General Data Protection Regulation (GDPR), enforcement of data protection obligations is not limited to supervisory authorities. The GDPR also provides data subjects with a direct right to bring private claims against controllers or processors for compensation of both material and nonmaterial damages (including damages for pain and suffering, injunctive relief, and disclosure of information relating to the processing of their personal data). The most prominent and pressing actions concern the compensation of damages for pain and suffering for GDPR violations, as these claims do not require a direct monetary loss. Although individual claims are usually rather low in these proceedings, they may quickly increase if large numbers of data subjects are affected by the same violation.

Recently, the Representative Actions Directive (Directive (EU) 2020/1828) has moved into the spotlight in the context of claims for nonmaterial damages under the GDPR. This directive further empowers qualified consumer organizations to bring collective redress actions on behalf of consumers, enabling aggregation of individual GDPR claims into a single proceeding, provided such claims are based on substantially similar factual circumstances, and entitling affected individuals to sign up to such proceeding without monetary risk and, in case of success, obtain direct compensation from the defendant—comparable to class actions in the United States.

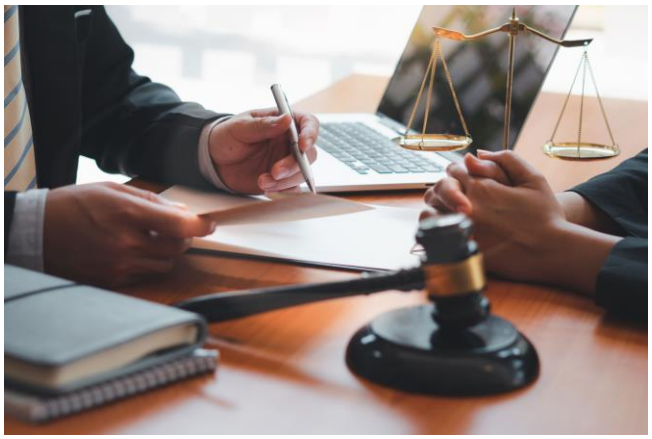
In Germany, there are currently three principal types of proceedings pursued against controllers processing large volumes of personal data: (i) collective redress actions by consumer protection associations; (ii) collective actions based on assigned claims pursued by special-purpose claim vehicles; and (iii) individual claims by data subjects. In comparison to other EU member states, it seems German courts are at the forefront of dealing with these matters.

Collective Redress Actions Brought by Consumer Protection Associations

Case Before the Higher Regional Court of Schleswig-Holstein (5 VKI 1/26) Against META—Pending

This collective redress action targets Meta Platforms Ireland Limited's (Meta) large-scale use of personal data for artificial intelligence (AI) training and allegedly addictive AI system design, based on two core allegations: (i) that Meta unlawfully uses personal data from Facebook and Instagram users to train its AI systems under the "legitimate interest" basis (Art. 6(1)(f) GDPR), and (ii) that Meta's AI systems are designed to promote addictive behavior, particularly affecting minors.

The plaintiff further accuses Meta of misleadingly communicating that data was used for training its "Llama" large language model, whereas the actual focus was training its advertising AI system "GEM," and of using personal data of minors and unregistered third parties without a legal basis and without an effective opt-out mechanism.



The plaintiff seeks standardized minimum compensation of up to €7,000 per affected individual (plus monthly accruals), varying by age group and user status (registered versus unregistered), for both AI training data use and addictive system design.

This is one of the first large-scale EU collective redress actions targeting AI training practices, combining GDPR nonmaterial damages claims with arguments on addictive design. If accepted by the court, it would introduce a standardized damages model applicable to a broad range of data-driven businesses, ranging from online platforms to financial service providers. Companies should monitor whether courts accept standardized damages for AI training, the use of unregistered users' and minors' data, and addictive product design as an independent basis for nonmaterial damage claims.

Case Before the Kammergericht (Higher Regional Court of Berlin) (20 VKI 1/25) Against X (Formerly Twitter)—Dismissed

The Higher Regional Court of Berlin dismissed a GDPR-based collective redress action against X, which alleged: (i) unlawful abuse of data power to influence political opinions and undermine democratic processes, and (ii) a data breach via an application programming interface bug allowing third parties to link usernames with phone numbers and email addresses. The claim sought standardized minimum damages of €750 (data power abuse) and an additional €250 (data breach) per affected individual.

The court dismissed the claim as inadmissible, holding that the alleged privacy harms require individualized assessment and are not suitable for collective redress. The case is now pending before the German Federal Court of Justice.

The court held that the asserted nonmaterial damages were not “essentially similar” as required under § 15 VDuG (the German law transposing the Representative Actions Directive), since liability and damage depend significantly on individual circumstances, in particular on the type of data affected, user behavior, duration of use, and the subjective impact on each data subject. The court also confirmed, with reference to recent Court of Justice of the European Union (CJEU) caselaw (C-526/24—Brillen Rottler), that claimants must positively establish: (i) a GDPR infringement, (ii) actual material or nonmaterial damage, and (iii) a causal link between the GDPR infringement and the incurred material or nonmaterial damage. Merely demonstrating and relying on a GDPR infringement is not sufficient.

The decision confirms that GDPR nonmaterial damages are inherently individualized and, with a robust litigation strategy, are manageable for defendants. Companies should monitor the Federal Court of Justice's review—and a likely CJEU referral—on the “essential similarity” requirement, ensure they have a lawful basis for tracking and personalized advertising, and note that individual claims remain a viable risk capable of generating substantial aggregate exposure at scale.

Case Before the Kammergericht (Higher Regional Court of Berlin) (24 VKI 1/25) Against a Global Short-Form Video Social Media Platform—Pending

This collective redress action challenges a global short-form video social media platform's large-scale use of personal data for behavioral advertising and monetization, seeking standardized minimum damages of up to €2,000 per affected individual. The plaintiff alleges that the platform compiles extensive behavioral and personality profiles, including special categories of data and data of minors, without a sufficient legal basis and that its algorithms are designed to foster user dependency, particularly affecting minors. In addition, the plaintiff accuses the platform of unlawfully transferring personal data to unsecure third countries. The claim seeks standardized minimum damages per age group of €2,000 (under 16), €1,000 (16–21), and €500 (21 and above).

This case illustrates the growing use of collective redress as a private enforcement mechanism. Business models relying on behavioral profiling and targeted advertising face heightened risk where the legal basis for processing is inadequate. Companies should reassess their use of engagement-driven features and note that special categories of personal data, data of minors, and international transfers to third countries remain key liability risks.

Collective Actions Based on Assigned Claims

A further enforcement model involves special-purpose "claim vehicles" that purchase GDPR nonmaterial damage claims from data subjects for a nominal amount (approximately €40–€50 per data subject) and pursue them in a single, large-scale lawsuit against the controller brought by the claim vehicle in its own name (unlike the proceedings under the "Collective Redress Actions" paragraph above, which are brought on behalf of the affected data subjects). The (disputed and still unanswered) key legal question will be whether GDPR nonmaterial damages claims are strictly personal in nature and therefore cannot be assigned.

Such lawsuits are being prepared against leading global technology companies, alleging that their tracking technologies (including web analytics and business tracking tools) integrated into third-party websites and apps result in the collection and processing of personal data, including special categories of personal data, without valid consent. German courts have already awarded up to €5,000 per individual in related individual claims, finding that consent obtained via website operators was invalid due to insufficient information. Website and app operators are equally responsible for ensuring a lawful basis for data collection and processing—not only the operators of the tracking tools. Companies should review their consent management tools and update consent texts and data processing information accordingly. The amounts awarded in individual claim lawsuits may increase materially if enforced by means of a claim vehicle demanding compensation in hundreds or even thousands of cases—provided the respective assignment solution is considered lawful.

Individual Claims

A large number of claims are being brought by individuals against Meta based on its Meta business tools embedded on third-party websites and apps, resulting in the transmission of personal data, including special categories, to Meta without, in the plaintiffs' view, a sufficient legal basis. The standardized factual pattern enables plaintiff law firms to scale these cases as mass individual claims (see the "Collective Redress Actions" and "Collective Actions" paragraphs above).

Plaintiffs allege that Meta's tracking tools collected detailed online behavior, including special categories of data, without valid consent, causing a "loss of control" over personal data that constitutes nonmaterial damage under Article 82 GDPR. Several courts have confirmed the absence of a valid legal basis and held Meta liable.

Courts have awarded nonmaterial damages ranging from €250 to €5,000, including: (i) Higher Regional Court of Dresden, €1,500 (judgments of 3 February 2026, case numbers 4 U 196/25, 4 U 292/25, 4 U 293/25, and 4 U 296/25); (ii) Higher Regional Court of Jena, €3,000 (judgment of 2 March 2026, case number 3 U 31/25); (iii) Higher Regional Court of Munich, €250–€750 (judgments of 18 December 2025, case numbers 14 U 881/25e, 14 U 1068/25e, 14 U 1314/25e, and 14 U 2300/25e); (iv) Higher Regional Court of Naumburg, €1,200–€1,250 (judgments of 5 February 2026, case numbers 9 U 124/24 and 9 U 44/25); (v) Regional Court of Leipzig, €5,000 (judgment of 4 July 2025, case number 05 O 2351/23); and (vi) Regional Court of Siegen, €5,000 (judgment of 9 October 2025, case number 8 O 439/2023 KN01 001 (470)).

Meta has appealed, and a landmark ruling from the German Federal Court of Justice is expected.

Companies using tracking technologies for behavioral or targeted advertising are themselves controllers under the GDPR and must ensure a valid legal basis for the processing. Any data collection or cookie storage without valid prior consent may give rise to GDPR and ePrivacy violations. Companies should review and update their consent mechanisms and information accordingly. Even if the awarded amounts are rather low on an individual basis, the collective action mechanisms (see the “Collective Redress Actions” and “Collective Actions” paragraphs above) may materially increase the related risks.

Is Germany the Place to Go for Private GDPR Litigation?

Given comparatively low litigation costs and German courts' demonstrated tendency to award significant nonmaterial damages in favor of data subjects, Germany is increasingly emerging as the key jurisdiction for private data protection enforcement. Although the claims per individual are comparably low, the number of affected individuals is potentially very high, leading to high total amounts. Although lawsuits are currently mainly initiated against very large online platforms, the representative action models outlined above may pose a risk to any company suffering a cyber breach where personal customer data has been unlawfully acquired or disclosed. Companies falling within the scope of the GDPR should reassess their compliance with applicable data protection laws to mitigate litigation exposure and potential financial liability.

AI LISTENS, BUT DOES IT PRINT?: VOICEPRINT BIPA CLAIMS IN THE NORTHERN DISTRICT OF ILLINOIS

By: RiKaleigh Omosheyin

The next major frontier in biometric privacy litigation may involve not fingerprints, face scans, or workplace time clocks, but the human voice.

A new cluster of lawsuits recently filed in the Northern District of Illinois allege that major artificial intelligence (AI) companies used recordings of plaintiffs' voices to create voiceprints, voice embeddings, or other speaker-specific representations for generative AI training and voice model development without the notice and written release required by the Illinois Biometric Information Privacy Act (BIPA).

While a number of states have enacted biometric privacy regulations, BIPA is considered among the most comprehensive. BIPA is significant because it creates a private right of action and permits recovery of statutory damages of US$1,000 or actual damages, whichever is greater, per negligent violation and US$5,000 or actual damages, whichever is greater, per intentional or reckless violation, along with attorneys' fees, costs, and injunctive relief. 740 Ill. Comp. Stat. 14/20. Multiple collections, captures, or acquisitions of the same biometric identifier or biometric information from the same person using the same method of collection constitute a single violation for purposes of recovery under Section 15(b). Likewise, multiple disclosures to the same recipient using the same method constitute a single violation under Section 15(d).*Id*. 14/20(b)–(c), as amended by Ill. Pub. Act 103-0769.

The statute applies to private entities and regulates both “biometric identifiers” and “biometric information.” A “biometric identifier” expressly includes a voiceprint, along with fingerprints, retina or iris scans, and scans of hand or face geometry. *Id*. 14/10. “Biometric information” covers information based on a biometric identifier that is used to identify an individual, regardless of how it is captured, converted, stored, or shared. *Id*. Before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric identifier or biometric information, a private entity must provide written notice that the biometric data is being collected or stored; disclose in writing the specific purpose and length of term for which it is being collected, stored, and used; and obtain a written release. *Id*. 14/15(b). Entities in possession of covered biometric data must also maintain a publicly available retention and destruction policy. *Id*. 14/15(a).

Much of the BIPA litigation to date has involved fingerprint time clocks, facial recognition, or identity-verification systems. These new suits, however, push the statute into a different arena: whether the data used to build and train AI systems contains speaker-specific biometric representations. The complaints allege that the defendants ingested audio recordings, extracted speaker-specific voiceprints or voice embeddings unique to each speaker, and used those biometric representations to train, refine, or deploy generative AI voice models. The complaints assert claims under several BIPA provisions, including Section 15(a), which requires a publicly available retention and destruction policy; Section 15(b), which requires written notice, disclosure of purpose and retention period, and a written release before collection or acquisition; and Section 15(c), which prohibits selling, leasing, trading, or otherwise profiting from biometric identifiers or biometric information. Some complaints also assert disclosure and data-security claims under Sections 15(d) and 15(e). The complaints further allege that none of the defendants disclosed the biometric nature of their data processing, obtained the required written releases, or published retention schedules required for entities in possession of covered biometric data.

These cases raise questions BIPA does not expressly answer. A threshold issue will be whether the defendants' alleged use of audio recordings to train AI voice systems involved extracting or storing speaker-specific voice features sufficient to constitute a statutory “voiceprint” or “biometric information,” as opposed to merely using audio files as generalized training data. As with any newly filed complaint, the allegations remain unproven.

For AI companies, biometric compliance cannot be an afterthought. Dataset provenance, licensing, consent, retention policies, deletion capability, and technical documentation may all become central litigation issues. Companies developing, purchasing, or deploying AI tools that process audio, images, video, or other biometric-adjacent data should consider the following steps:

- *Map the data*. Identify whether any stage of development or deployment involves voices, faces, fingerprints, or other identifiers that could qualify as biometric identifiers or biometric information.
- *Review dataset provenance*. Confirm where training data originated; whether it was scraped, licensed, purchased, or user-submitted; and whether the source permitted biometric processing and AI-training uses.
- *Assess Illinois exposure*. BIPA risk may arise when Illinois residents' biometric identifiers or biometric information are involved, regardless of where the company is headquartered.
- *Document notice and consent*. If a system creates or uses voiceprints, or other person-specific biometric representations, evaluate whether disclosures and written releases cover the actual

use, including training, testing, model development, and commercialization.

- *Adopt retention and deletion rules*. Maintain written retention and destruction schedules for biometric identifiers and biometric information.
- *Avoid overclaiming*. Marketing statements that a tool is "anonymous," "nonbiometric," "consent free," or "privacy safe" should be vetted carefully against how the system actually works.

If courts allow BIPA claims to proceed in this context, the result could reshape how AI companies source audio data, structure licenses, document consent, and design model-training pipelines. If courts reject the theory, legislators may face pressure to update biometric statutes to address AI training directly. Either way, the biometrics debate no longer centers only on point-of-use scanners. It now reaches the datasets and models that may capture and reproduce human identity itself.

EDITORS AND AUTHORS

EDITORS

Whitney E. McCollum
Partner
Seattle, San Francisco

Michael J. Stortz
Partner
San Francisco

Dr. Thomas Nietsch
Partner
Berlin

AUTHORS

Cameron Abbott
Partner
Melbourne

Jake Bernstein
Global AI and Innovation Partner
Seattle

Sanjeev Bhasker
Partner
Washington, DC, Miami, Charlotte

Corey Bieber
Partner
Chicago

William R. Bradley, II
Associate
Seattle

Vivian K. Bridges
Associate
Washington, DC

Emre Cakmakcioglu
Lawyer
Melbourne

Guillermo S. Christensen
Partner
Washington, DC

Dr. Ulrike Elteste
Counsel
Frankfurt

Destinee S. Evers
Associate
Seattle

Annaliese Filippis
Lawyer
Melbourne

Eric F. Vicente Flores
Associate
Washington, DC

Lauren M. Flynn
Government Affairs Advisor
Washington, DC

Scott J. Gelbman
Government Affairs Advisor
Washington, DC

Michael Culhane Harper
Partner
Washington, DC

Madison Jeffreys
Lawyer
Melbourne

Daniel Knight
Partner
Melbourne

Marne Marotta
Partner
Washington, DC

Noirin M. McFadden
Consultant
London

Andreas Müller
Associate
Berlin

Veronica Muratori
Counsel
Milan

RiKaleigh Omosheyin
Associate
Chicago

Alex Parker
Lawyer
Melbourne

Sarah Pearce
Partner
London

Rob Pulham
Special Counsel
Melbourne

Katy M. Ramos
Associate
Los Angeles

CYBER LAW WATCH BLOG

Find additional insight on cyber risk mitigation and management at cyberlawwatch.com

K&L GATES

K&L Gates is a fully integrated global law firm. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.