Privacy Daily
Reliable news on data protection and compliance

Thursday, April 2, 2026 Vol. 2, No. 63

TOP NEWS

'CABINS THE DAMAGES'

7th Circuit Rules BIPA Amendment Limiting Damages Applies Retroactively

The 7th U.S. Circuit Court of Appeals' decision Wednesday that a 2024 amendment to the Illinois Biometric Information Privacy Act (BIPA) applies retroactively is a win for businesses, privacy lawyers told us. While some lawyers believed the ruling would likely limit the amount of litigation filed under the statute, another said the impact on litigation is to be determined.

The Illinois legislature amended BIPA, which passed in 2008, to provide more clarity around damages after a 2023 decision determined that the law as written meant that every use of biometrics without consent counted as a violation (see 2502210037).

That 2024 update specified that damages are limited to one recovery per person, not per scan, though questions lingered over whether the amendment would apply retroactively (see 2506260013).

In a consolidated case before the 7th Circuit, Chief Judge Michael Brennan ruled that the amendment was a "remedial change" to BIPA, which "makes it 'procedural' under Illinois law, so courts should apply the amendment to cases pending at the time the statute was enacted." Judges David Hamilton and Candace Jackson-Akiwumi also signed on to the opinion.

The amendment "did not alter any substantive rights or the number of injuries [that plaintiffs] sustained," Brennan added. It "simply changed the statutory award of damages available to plaintiffs."

The ruling "cabins the damages available," said Matthew Wolfe, a Shook Hardy privacy lawyer, in an interview. "It says very clearly, 'your ceiling is $1,000 per violation per claimant.'" The limit applies to all cases pending at the time the amendment passed.

This is "important" in practice, Wolfe said, because plaintiffs were "frequently" arguing that "damages could be really, really huge" at $1,000 per violation, which they counted as every time an individual's biometrics were scanned.

"The outcome is a welcome one for defendants who have pending BIPA actions," said David Saunders, a privacy and cybersecurity lawyer at McDermott Will. "The theory that Plaintiffs were advancing [was] that the Illinois legislature would prospectively fix 'annihilative' BIPA damages, but leave the many pending lawsuits subject to those same damages would have been an absurd result."

"This is one of those opinions where the correct legal answer is also the one that is practical," Saunders told us in an email.

Fisher Phillips lawyer Danielle Kays also said the decision was a "great win for companies." There's a "tide turning," and the opinion is a "reinforcement of some of the language" in BIPA.

The decision is most impactful for cases similar to the three consolidated in the appeal, which were all single-plaintiff cases, she told us, noting that most of the litigation started after 2023's *Cothron v. White Castle*.

"What's interesting in those cases is [that] these are statutory damages, and there's no requirements of there being harm," Kays noted. "In fact, in almost every BIPA case that I've seen—which is many—there has been no harm to the plaintiff," since "no information was breached." The claim is "simply a violation of the notice in the statute."

This means that between *Cothron* and the BIPA amendment, many cases were filed asking for "hundreds of thousands to even sometimes millions" in damages "for one person where there was no actual … harm," Kays said.

As a result, single-plaintiff cases will be the first to be affected by the 7th Circuit's ruling, she said, but the federal appeals court "reiterated and reinforced some very good points regarding damages, and that will affect class actions" as well.

Wolfe agreed. Though $1,000 per violation is significant in both single-plaintiff cases and class actions, in many of the latter, "plaintiffs were taking the position" that "there's a whole world of damages available out there for each claimant," he said. They used that argument "to try to drive up settlement value and increase pressure on defendants to settle cases before class certification, before summary judgment and before trial."

The 7th Circuit decision "changes some of the leverage that's available to the parties in class actions," Wolfe said, adding that he thinks "this ruling basically kills off the single-plaintiff cases, because now [they] would be suing for $1,000, which is essentially [a] small-claims case in Illinois."

He noted that BIPA litigation has decreased in recent years "because a lot more companies are compliant now than they were three to five years ago," meaning "there are fewer targets out there" for lawsuits. Now that the 7th Circuit ruling also makes it "very difficult" for single-plaintiff cases to move forward, he predicted even fewer of these suits but said he expects to see class actions continue.

"Even $1,000 per plaintiff is still potentially attractive in a class action, because … you may have thousands or even millions of plaintiffs once they're aggregated in a certified class," Wolfe said.

Kays, however, said she's "not sure that [the decision] curbs the cases" filed under BIPA. "That's to be determined." But the ruling does affect the "valuation" of cases, she added.

No Damages Guarantee

Kays also noted that the appeals court said "courts have discretion to decide whether to award damages at all," and "plaintiffs are not guaranteed any specific recovery in the first place."

The language of the statute specifies that plaintiffs are "entitled to at most one recovery," she said. "The court said that by including the qualifier 'at most,' the amendment indicates that the plaintiff allowing thousands of violations might not even be entitled to the full award of liquid damages permitted at all."

That serves as a "reminder that the full [amount] of liquidated damages may not be available" for a violation of BIPA and may "affect the valuation of other cases too," Kays added.

In addition, Saunders said, while "it may be too early to call it a trend," the 7th Circuit's opinion continues the recent shift of "appellate courts that are starting to rein in overreach by Plaintiffs who seek to push privacy theories of liabilities that are not supported by the statutory text."

"However, the fact that this was an issue that had to be resolved on appeal demonstrates what these BIPA and other privacy-based litigations are really about: a money grab by the Plaintiffs bar," he argued. "It highlights the fundamental misalignment of incentives in privacy litigation today."

State Court Opinion

A caveat to the 7th Circuit ruling is that it's a federal court weighing in on how it believes a state court would rule, and Illinois courts will have the final call.

"It's possible" that the Illinois Supreme Court could disagree with the 7th Circuit's decision, but Wolfe said he "would be surprised" if that happened, as the federal appeals court "carefully follow[ed] Illinois law." But in order for the state's high court to rule, a different case would have to make its way through the Illinois court system, he said.

Kays said the 7th Circuit "did a really good job of laying out the law, and clearly … setting forth why … this was a remedial remedy and not a substitute one," thus making the amendment retroactive. The appeals court also addressed the plaintiffs' arguments, so overall, "the logic is very clear."

She agreed that the state court could decide the issue differently, but Wednesday's ruling was "a very well-reasoned decision," making a different view unlikely. **– Kara Thompson**

Share Article

'INTO THE WEEDS'

State Privacy Enforcers Showing Increased Reliance on Technical Teams

State privacy enforcers are increasingly relying on technologists and technical experts, allowing attorneys general to pursue more granular cases companies must account for, enforcers and a privacy counsel told us this week at the IAPP Global Summit in Washington.

California, Delaware, Maryland, Connecticut, Colorado and Texas are among the states building privacy teams with technical backgrounds.

Regulators are "really getting into the weeds," said Sourcepoint General Counsel and Chief Privacy Officer Julie Rubash. "They're getting more sophisticated, especially in California. They're starting to hire technologists to be part of their investigation teams and really understand what's going on. And so companies can no longer just put something up that looks good, that doesn't actually work on the backend. They really need to test and test and test and make sure it works from all different angles and that there's no consumer confusion. Otherwise they're going to get hit with enforcement actions."

Delaware Deputy Attorney General John Eakins, on the sidelines at IAPP, noted the hiring of his team's new technologist. It "really helps me analyze cases, understand the tech stack, what's going on behind the scenes and help shape an investigation," he said. Additionally, Delaware can lend its technical expertise when collaborating in multistate investigations, he said.

Delaware is a member of the Consortium of Privacy Regulators, which includes California, Colorado, Connecticut, Indiana, New Jersey and Oregon (see 2510080008). Eakins said most of Delaware's privacy work involves collaboration with other states. And while Delaware hasn't formally settled cases under its comprehensive privacy law, which took effect in January 2025, Eakins is expecting some potential turnaround in 2026. "I'm always hopeful," he said. "We definitely have work that we're doing, and there's things that are open. And we're always hopeful that they get resolved, so I would expect there's going to be a resolution this year."

Eakins and Oregon Assistant Attorney General Jordan Pahl said there are a lot of "commonalities" between state privacy laws, which allow the consortium to pursue overlapping claims. Pahl said Oregon is particularly focused on ensuring companies are offering clear disclosures to consumers. Piling on privacy disclosures in response to new state laws can "create confusion and can create messes of disclosures where what we want to be apparent to consumers isn't apparent to consumers," she said. "That's something that we're really focused on: the clarity of disclosures."

Figuring out the "sweet spot" between opt-in and opt-out consent is a "major" issue on "everyone's radar," said Rubash. The California Privacy Protection Agency's recent settlement with PlayOn Sports (see 2603030011) showed the potential for conflicts between opt-in and opt-out consent, she said.

CalPrivacy alleged PlayOn didn't provide a sufficient opt-out mechanism, while failing to honor universal opt-out preference signals. By directing students and other users to instead opt out through the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA), PlayOn "violated the company's responsibility to provide its own method for consumers to opt-out," CalPrivacy said.

Privacy Daily
Reliable news on data protection and compliance

EDITORIAL & BUSINESS HEADQUARTERS:
PO Box 91850, Washington, DC 20090

ISSN 3067-0446

Published by Warren Communications News Inc.
PO Box 91850, Washington, DC 20090
202-872-9200
https://warren-news.com
https://privacy-daily.com
info@warren-news.com

Send news materials to
privacydailynews@warren-news.com

Follow us on: X (formerly Twitter) | LinkedIn

Adam Bender, Deputy Managing Editor

EDITORIAL:
Paul Warren, *Chairman & Publisher*
Daniel Warren, *President & Editor*
Timothy Warren, *Executive Managing Editor*
Brian Feito, *Managing Editor*
Adam Bender, *Deputy Managing Editor*
Karl Herchenroeder, *Associate Editor*
Dugie Standeford, *European Correspondent*
Kara Thompson, *Assistant Editor*
Hannah Prince, *Deputy Managing Editor*
Seth Arenstein, *Copy Editor*

Albert Warren, Editor & Publisher 1961-2006

BUSINESS:
Sheran Fernando, *Chief Operating Officer*
Brig Easley, *Executive VP - Controller*
Gregory E. Jones, *Director of IT Services*
Annette Munroe, *Director of Operations*
Katrina McCray, *SMSD Manager*
Loraine Taylor, *Administrative Assistant*

SALES:
William R. Benton, *Sales Director*
Bruce Ryan, *Account Manager*
Jim Sharp, *Account Manager*
Kenny Johnson, *Account Manager*
Matt Long, *Account Manager*
Matt Peterson, *Account Manager*
Walt Sierer, *Account Manager*

"It's challenging to get opt-in consent and offer an opt-out that's going to satisfy the regulators," Rubash said. "Do they get express consent or implicit consent, put up a notice in order to not be low-hanging fruit for this litigation while also not creating dark patterns or confusion with consumers?" Companies are receiving repeated demand letters from regulators, so it's a "major issue" trying to keep up with conflicting requirements and do "the right thing," she said. **– Karl Herchenroeder**

Share Article

STATES

Kentucky Smart TV Privacy Bill, ALPR Bill Head to Governor's Desk

A Kentucky bill regulating data collection related to automated content recognition (ACR) technology (see 2603110031) and legislation restricting usage of automated license plate readers (ALPRs) (see 2602190018) were delivered to the governor this week after being signed by the Senate President and Speaker of the House.

HB-58 limits the use and sale of ALPR data and sets a 90-day retention period if it's for use in a criminal or insurance investigation. It was delivered to Gov. Andy Beshear (D) on Tuesday after passing the House on a 70-19 vote. It passed the Senate with a 34-2 vote on March 24.

HB-692 amends the Kentucky Consumer Data Protection Act by requiring consumers to opt in or out concerning their smart TVs and monitors using ACR technology (see 2603260030). It passed unanimously in the Senate and the House Tuesday, with 38-0 and 88-0 votes, respectively, and was delivered to the governor Wednesday.

Share Article

WHITE HOUSE

CDT Raises Privacy Concerns Over Trump's Election Order

President Donald Trump's executive order on elections will "further erode Americans' privacy," the Center for Democracy & Technology said Thursday by email.

Trump issued the order Tuesday seeking to restrict mail-ballot voting, prompting constitutional challenges.

The order "calls for more reliance on data with known errors and outdated information, and injects chaos into states' carefully planned mail voting processes," said CDT Policy Analyst Isabel Linzer. In addition, "It's a privacy and practical nightmare that raises unacceptable risks, disenfranchising voters and stoking baseless fears about voter fraud that make our elections less trusted as we head into the midterms."

Share Article

COURTS

Bipartisan Coalition Urges Supreme Court to View Geofence Warrants as Constitutional

Geofence warrants are a critical tool for law enforcement and their constitutionality should be upheld, argued a bipartisan coalition of 31 states and the District of Columbia in support of the federal government's position in an amicus brief to the U.S. Supreme Court Wednesday.

The filing is in *U.S. v. Chatrie,* which the high court is set to hear this session. In case 25-112, the government served Google with a geofence warrant for device location data in an attempt to find the culprit behind a bank robbery. After the initial warrant, the government sought additional data from Google without another warrant, leading to the arrest of Okello Chatrie. The question in *Chatrie* is whether the use of a geofence warrant violates the Fourth Amendment (see 2602020025).

"Geofence warrants are a modern investigative tool used to identify unknown perpetrators tied to a specific place and time," and "courts across the country are now grappling with how to apply traditional Fourth Amendment principles to that new technology," said the coalition, co-led by Michigan Attorney General Dana Nessel (D) and Iowa AG Brenna Bird (R).

The Supreme Court "should make clear that the Constitution does not categorically ban those investigative methods" and rather, "longstanding doctrine requires courts to evaluate whether a warrant is supported by probable cause, sufficiently particular, and reasonably executed," they continued.

The coalition added that "a categorical ban on warrants limited to the time and place of criminal activity would harm States' sovereign interests in public safety by eliminating a judicially supervised tool that can be more precise than traditional alternatives."

Privacy and advocacy groups, however, have argued for the prohibition of geofence warrants, arguing that they breach the privacy of innocent people who happened to be near crime scenes (see 2603030048).

"Without access to this critical technology, countless violent crimes may go unsolved, undoubtedly making our communities less safe and denying justice to victims," said Nessel in a press release Thursday. "The Fourth Amendment is a cornerstone of our Constitution, but it was never intended to serve as a shield for criminal activity."

"When supported by probable cause and judicial approval, geofence warrants are vital, constitutional tools that allow law enforcement to protect the public without compromising fundamental rights," she added.

Some privacy and technology scholars have also argued that the Fourth Amendment has lost its original meaning, but the Supreme Court's ruling in *Chatrie* could restore it (see 2603300015).

Share Article

EUROPE

CNIL Offers Guidance on Human Resources Data Retention

French watchdog CNIL published a reference guide Thursday to help organizations determine appropriate data-retention periods for human resources activities.

The document covers the most common human resources processing activities, such as recruitment, compensation management, protection of property and people, and monitoring and recording telephone calls in the workplace.

Its guidance isn't mandatory, but CNIL said it hopes the document will make it easier for users to locate information more quickly on relevant retention periods for their processing activities.

The guide applies to all public and private employer organizations whose personnel are subject to French law, CNIL said, according to a translation. It's "particularly useful for data protection

officers, GDPR contacts" and staff working in human resources departments or information systems management.

Share Article

Dutch Group Confident in Suit Against Meta for Child-Harming Addictive Features

California's recent landmark judgment against Meta for coercive design features that addict children (K.G.M. v. Meta) "strengthens our confidence in our own proceedings," said Jullaya Vorasuntharosoth, campaign director of Dutch nonprofit SOMI, in an email Thursday.

SOMI, or Stichting Onderzoek Marktinformatie (Market Information Research Foundation), launched a class action against Meta in the Copenhagen City Court this week on behalf of Danish kids and parents "who have had their rights violated and suffered mental harm through the use of Facebook and Instagram," it said in a news release.

Meta didn't immediately comment. The litigation follows a Sept. 29 letter that SOMI sent Meta, to which the company "essentially did not respond," the group said.

The lawsuit alleged that Meta's practices violate the GDPR, Digital Services Act and AI Act, along with several Danish laws, SOMI said. Facebook and Instagram are deliberately designed to be addictive, it said, arguing that Meta "has systematically exploited the psychological vulnerabilities of children and adolescents in order to maximize user engagement, collect personal data, and generate advertising revenue."

SOMI also said Meta has failed to implement effective age-verification measures, allowing kids to access the platforms with minimal oversight. As a result, children have been deliberately exposed to addictive features and harmful content without meaningful protection.

Additionally, SOMI charged, Meta has been aware of the harms associated with its platforms for a long time but chose not to make changes.

The lawsuit stressed the broader societal impacts of Meta's platform designs as well, noting that features such as infinite scrolling, algorithmic recommender systems and beauty filters have been linked to rising levels of depression, anxiety and other problems.

The lawsuit seeks a court order declaring that Meta has violated applicable laws and ordering it to modify or remove harmful design features from its platforms. SOMI is also calling for Meta to be compelled to put effective age verification in place and to stop marketing and monetizing services based on the collection of children's data.

The litigation seeks compensation of 25,000 Danish krone ($3,900) for each affected minor for psychological and social harm suffered. People are eligible to participate if they used Facebook or Instagram while living in Denmark and were younger than 18 at any time after Feb. 28, 2023, SOMI said.

SOMI has similar lawsuits pending against the company in the Netherlands, Belgium and Germany, it noted.

Share Article

Ofcom Pushes Platforms for Risk Assessments, Updates OSA Enforcement Activities

The U.K. Office of Communications (Ofcom) on Wednesday ordered dozens of tech firms to submit their second-year harms risk assessments and children's risk assessments by July 31.

The regulator said it's keeping pressure on platforms to "put safety by design front and center of their operating models." Failure to provide the information could mean enforcement action, it added.

Under the Online Safety Act, tech companies are required to assess and mitigate the risk of people encountering illegal content. In addition, those platforms likely to be accessed by kids must gauge and mitigate the risk of users younger than 18 encountering certain kinds of harmful material, Ofcom said.

Later this year, "categorized" services, which the regulator expects to include some of the most widely used social media and search services, must publish summaries of their risk assessment, "forcing them to be transparent about their view of the risks they pose."

Ofcom also updated several enforcement actions Tuesday.

Among others, it provisionally found reasonable grounds to believe that First Time Videos failed to comply with OSA requirements to use highly effective age checks to protect children. The company has 20 days to respond.

Share Article