Privacy Daily
Reliable news on data protection and compliance

Thursday, March 5, 2026 Vol. 2, No. 43

TOP NEWS

STATES

FTC

COURTS

EUROPE

ASIA PACIFIC

TOP NEWS

GUTHRIE TABLES COPPA

House Commerce Passes Kid Package; Senate Passes COPPA 2.0

The House Commerce Committee voted along party lines Thursday to pass a package of kids' bills, including a Republican version of the Kids Online Safety Act (KOSA), as expected (see 2603030056). The Senate, meanwhile, unanimously passed its version of the Children and Teens' Online Privacy Protection Act (COPPA 2.0).

During the House committee markup, Democrats called for passage of the Senate's version of COPPA 2.0, which better protects children's privacy, they said. House Commerce Committee Chairman Brett Guthrie, R-Ky., decided to table COPPA 2.0 (HR-6291), saying both sides "feel there's been substantial progress toward a path forward." Staff members will negotiate further in the "coming days," he said.

Democrats repeatedly failed to pass amendments seeking to update the knowledge standard and preemption language included in the KOSA package (HR-7757).

The bills "simply do not meet the mark" and will leave children "less safe online than they are today," House Commerce Committee ranking member Frank Pallone, D-N.J., said during the markup. He added that Democrats for several months have engaged in legislative negotiations that ultimately failed. In addition, the package's knowledge standard will allow tech companies to turn a blind eye and avoid liability for online harm, and he expressed disappointment the committee didn't consider his subcommittee-passed data broker bill, the Don't Sell Kids' Data Act (HR-6292).

Guthrie said leadership participated in "serious engagement" and "good-faith efforts" to reach consensus with Democrats. Congress' responsibility is ultimately to its constituents, and children are being "targeted, groomed, harassed and exploited online," he said.

House Republicans' "weaker" versions of the bills put "privacy and safety at risk," said Rep. Kathy Castor, D-Fla., who previously signed onto prior versions of KOSA and COPPA, which more closely aligned with the Senate. The biggest issue was Republicans' removal of KOSA's duty of care, she said, which would have required companies to build apps and websites knowing they would be used by children.

Rep. Lori Trahan, D-Mass., said enforcement mechanisms in the package put "too much trust" in an under-resourced FTC and disempower state enforcers by preempting state law. Congress should be making up for gaps in federal enforcement, not widening them, she said.

Pallone outlined three main objections from Democrats: the knowledge standard, preemption and the lack of protections against data brokers.

Children and teens deserve privacy, Sen. Ed Markey, D-Mass., said on the Senate floor before requesting unanimous consent for COPPA 2.0, which he introduced with Sen. Bill Cassidy, R-La. The Big Tech business model has evolved much faster than federal law, and COPPA 2.0 brings children's privacy law into the "21st Century," he said. It gives parents and children "meaningful control" over personal data and bans targeted advertising for children and teens.

The era of building detailed profiles on children for manipulative purposes "must come to an end," he added. Cassidy said parents should be able to stop their children from being tracked and monetized online without consent.

The committee passed the App Store Accountability Act (HR-3149) on a 26-23 vote. It requires that app stores obtain "proper parental consent" when minors try to download or purchase an app (see 2601230053).

The committee passed Sammy's Law (HR-2657) on a 36-16 vote. The bipartisan bill from Reps. Debbie Wasserman Schultz, D-Fla., and Buddy Carter, R-Ga., creates a "parental right to know about dangerous or concerning interactions children under the age of 17 may have online." Social media platforms must provide "access to data pertaining to a parent's child through registered third-party safety apps." **— Karl Herchenroeder**

Share Article

REPUBLICAN CALLS BILL 'EXTREME'

Maine Senate Passes Comprehensive Privacy Bill With Data Minimization

A Maine comprehensive privacy bill with Maryland-like data-minimization rules narrowly passed the state Senate on Thursday despite a controversial amendment exempting political organizations. Opponents said the bill would hurt businesses while protecting politicians.

The Senate initially voted 20-14 to pass LD-1822. After voting 14-20 to defeat a motion by Sen. Bruce Bickford (R) to "table until later" the proposed amendment, the Senate voted 18-16 to pass LD-1822 as amended.

But before the bill can go to Gov. Janet Mills (D), the House must agree to the Senate's changes. Earlier this month, the House narrowly passed the privacy bill in a 71-68 vote (see 2602100043).

"The core feature of this proposal is called data minimization," said Sen. Anne Carney (D), the Senate co-sponsor of LD-1822. "Data minimization places appropriate limits on the collection of three types of data, aiming to balance legitimate use with the safety of Mainers and in particular ... children."

"The first type, called personal data, can only be collected if reasonably necessary for a specific product or service requested by the consumer," said Carney. The second, sensitive data, "can only be collected if strictly necessary to fulfill the customer's request, and that highest level of private, sensitive information cannot be sold," she said. Meanwhile, the bill would prohibit selling the third type, minors' personal data, and also ban using minors' data for targeted advertising, she said.

"Contrary to what you might hear," added Carney, "these provisions do not hamstring local businesses that drive Maine's culture and economy."

Sen. David Haggan (R) opposed the bill because he said he prefers "the Connecticut model" that about 17 other states have followed. Majority Democrats' approach is "extreme" by comparison, he said. "When we ... impose stricter standards than what has become the national standard, Maine businesses will suffer."

Sen. Jeff Timberlake (R) noted that L.L. Bean, as well as Maine's chamber of commerce and other businesses oppose the bill. "That should tell us something," he said, "but I'm not sure we're listening."

Carney said the Senate floor amendment "reinforces the bill's existing exemption related to political activities." It also fixes dates that had been "drafting oversights," she said. Senators added a "more detailed description" of LD-1822's existing "First Amendment protection" because it didn't "jump out at people, and there was some concern that it was not at as front and center as it needed to be," Carney said.

However, several senators raised concerns with the amendment excluding politicians. Sen. Rick Bennett (I) said it worsens already "untenable" exemptions in LD-1822. "Why are we exempting not-for-profits ... but including for-profit businesses?" he asked. "It makes no sense to me." The amendment expands that by making political organizations especially exempt, he said.

Sen. Joe Baldacci (D) also opposed the amendment. "We can't pass laws we're going to exempt politicians from," he said. Likewise, Sen. Trey Stewart (R) questioned "exempting ourselves" from the proposed privacy law.

Comprehensive privacy bills in Alabama and Oklahoma, which hew more closely to the model seen in most other states, are also nearing the finish line (see 2602250016 and 2602190031). About 20 other states already have comprehensive privacy laws. **– Adam Bender**

Share Article

SECOND ACTION THIS WEEK

CalPrivacy Hits Ford for Opt-Out Friction in Connected Car Sweep Under CCPA

Ford and other businesses may not require email verification before processing customers' opt-out requests, the California Privacy Protection Agency said in a $376,000 settlement with the American car company. Ford's difficult opt-out process violated the California Consumer Privacy Act (CCPA),

the agency said. It was the second CalPrivacy enforcement action revealed this week, as well as the second in a sweep of connected-vehicle manufacturers.

"Another day, another CCPA action," blogged Frankfurt Kurnit privacy attorney Andrew Folks. The Ford settlement reemphasizes that opt-outs aren't verifiable under the CCPA, he said. "Ensuring these request types are honored separately and lawfully requires proper configuration within a business's consumer request platform. Many vendor tools treat opt outs as verifiable requests by default, requiring customization of off-the-shelf products."

The carmaker created unnecessary friction for consumers by requiring them to verify their identity before they could opt out of the sale and sharing of personal information collected through its digital properties and connected vehicles, the state regulator said in a news release. It also didn't process opt-outs until consumers completed an email verification step, CalPrivacy said, adding that "in response to the agency's investigation, Ford has since processed the opt-out requests that lacked verification."

Ford must change its practices by giving consumers easy ways to opt out with minimal steps, CalPrivacy decided. It must also audit tracking technologies on its website and make sure it's complying with the Global Privacy Control and other opt-out preference signals. Ford didn't comment.

"Opting out is supposed to be easy," said CalPrivacy's enforcement head, Michael Macko. "Just as unnecessary steps in the checkout process can discourage consumers from completing a purchase, unnecessary steps in the opt-out process can discourage consumers from exercising their privacy rights. We will continue to scrutinize practices that create these kinds of barriers for Californians."

Reducing friction in exercising privacy rights is also the subject of an upcoming CalPrivacy rulemaking (see 2602270064). Executive Director Tom Kemp said, "The agency has made it a priority to remove obstacles that prevent Californians from exercising their privacy rights."

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*

The regulator announced the Ford enforcement action days after a $1.1 million fine against PlayOn Sports (see 2603030046). It was also the second action in a connected-vehicles sweep, the first of which was announced in July 2023, and last year resulted in a $632,500 penalty for Honda (see 2503120037).

After consumers requested to opt out through a web form, "Ford could have processed those requests without requiring additional information," said the CalPrivacy Board decision. Instead, Ford displayed a message noting "One More Step!" It asked consumers to "check your email for confirmation, click confirm and we will start your request."

"Ford deemed as 'expired' all requests" in which consumers didn't click to confirm their email, the agency said. "This resulted in Ford not processing dozens of requests to opt-out within the period required by the CCPA." The company processed them after CalPrivacy began investigating, said the agency, adding that Ford didn't "intend" to require the verification before consumers could opt out.

"Nevertheless, Ford's practice … impermissibly required consumers to submit a verifiable consumer request" and "created unnecessary friction for consumers to exercise their opt-out rights." The company violated Section 7026(d) of the agency's CCPA regulations.

CalPrivacy said it had jurisdiction over Ford because the car company does business in California, has annual gross revenue exceeding $26.625 million and annually sells and shares personal information of 100,000 or more consumers and households. The company cooperated with the regulator during the investigation, producing documents, answering questions and engaging in "candid discussions about Ford's privacy practices," the agency noted.

Privacy4Cars CEO Andrea Amico noted that when Honda was fined by CalPrivacy, the car company "prioritized and overhauled" its "online privacy experience in a matter of weeks." The fining of a second manufacturer "should send a strong signal to both manufacturers and their affiliated dealerships that consumers must always be presented with prominent and easy-to-understand disclosures, and be given clear choices about their personal data—whether it's sharing it or opting-out and having it deleted," the automotive data security vendor's founder said in an email to *Privacy Daily*.

The order shows an "unrelenting" California privacy agency, Shook Hardy privacy attorney Josh Hansen posted on LinkedIn. "CalPrivacy acted despite concluding this was an unintentional violation." Companies should take away from the action that they "must only request what is needed to process an opt-out request," Hansen added. **— Adam Bender**

Share Article

STATES

DeSantis-Proposed Florida AI Bill of Rights Passes Senate

A proposed Florida AI bill of rights passed the state Senate by an overwhelming majority after a week-long delay on the floor and amid reports of White House intervention (see 2602260049).

Senators voted 35-2 for SB-482 Wednesday. The Florida House received the bill Thursday but its prospects in that chamber are unclear. HB-1395, which is the House version of the AI bill of rights, hasn't moved since January.

Jai Jaisimha, co-founder of the Transparency Coalition, emailed us Thursday that his "understanding is that the House in [Florida] opposes the bill so [it's] unlikely to advance." The coalition is a nonprofit that advocates for AI accountability.

The Florida Senate adopted two amendments: One notes that the bill wouldn't "prohibit the sale or disclosure of information specifically authorized by federal law," while the other clarifies proposed restrictions on educational use of AI.

Gov. Ron DeSantis (R) had proposed the AI measure even though an executive order by President Donald Trump sought to stop state regulation of the nascent technology (see 2512120042). Responding Wednesday to reports that the Trump administration intervened in Florida's deliberation over the DeSantis proposal, the White House said it never told states they can't enact child safety protections (see 2602250074).

The American Consumer Institute and R Street, two free-market think tanks, ranked the Florida bill as No. 5 on a list of "worst state regulatory ideas" related to AI in a report released Tuesday.

The groups criticized Florida's proposed AI bill of rights for trying to pack "many distinct regulatory ideas [into] one measure, including privacy and data collection mandates, parental controls and child safety issues, political advertising limitations, and defamation rules." They added that the measure "represents a sweeping degree of state AI policy meddling, much of which would be more appropriately handled by Congress in comprehensive AI and privacy legislation—if at all." **—AB**

Share Article

Oregon Legislators Pass Bills on Immigration Privacy, AI Chatbots

An Oregon immigration privacy bill will go to Gov. Tina Kotek (D). Meanwhile, another Oregon measure to regulate AI companion chatbots bill neared the finish line.

The Senate agreed to concur with House amendments and repass the immigration bill (SB-1587) in an 18-11 vote Wednesday that broke along partisan lines with Democrats in the affirmative and Republicans in the negative. The bill would prohibit public bodies from sharing information with data brokers unless the broker pledges not to use it for immigration enforcement purposes (see 2603030051).

The Oregon House voted unanimously the same day for the AI chatbots bill (SB-1546). Among other things, the bill would require AI operators to disclose that companions are artificial. The Senate previously passed the bill by a 26-1 margin but must vote again to concur with House changes before it can go to the governor.

Share Article

FTC

FTC Weighs 'Harms and Benefits' of Regulation, Says Consumer Protection Director

An FTC priority is "drilling down" into the harms and benefits related to consumer protection, including with privacy, the agency's Consumer Protection Bureau Director Chris Mufarrige said Thursday.

Privacy "tends to be the trickiest of the issues" when it comes to determining the "harms and benefits of certain data practices," he told attendees at a George Mason Law School event.

The FTC's recent workshop on data-driven economics (see 2602260070), however, reflects the issue's "seriousness" and that it's a commission priority, Mufarrige said. The workshop demonstrated the "broader theme" that the commission believes it's important that "economists play a critical role in the development of our consumer protection cases," including "privacy in particular," he said.

It also signaled that the FTC wanted to hear from academics and researchers to better understand digital markets and how the commission's work impacts that space, Mufarrige said.

Beyond this, Mufarrige said kids' and teens' privacy remains a priority, citing the FTC's inquiry last year, under Section 6(b) authority, seeking information from tech companies about AI chatbot interactions with young users (see 2509110068 and 2512170059).

He also noted the series of FTC COPPA cases last year (see 2509030057, 2509300054 and 2509020069), and said the commission expects more this year.

The Fair Credit Reporting Act (FCRA) is also a priority, Mufarrige said, adding that he finds financial services apps offered to teens to be an "interesting area ... where the FTC should be focused."

Another focus is ensuring the commission take[s] seriously any use of the "unfairness" or "cost-benefit prong," the director said. The last administration "tended to paint with a broad brushstroke about data practices," whereas this administration's focus is centered on whether "the practices [are] harming consumers," he said.

While the former and current FTC agree that geolocation data should be considered sensitive data, many other types of data or data collection from the past administration are going to be reevaluated through the cost and benefit lens on a case-by-case basis, Mufarrige added. **—KT**

Share Article

COURTS

Federal Judge Allows Privacy Case Against Allstate to Continue

Allstate must face several claims in a privacy lawsuit accusing it of tracking consumer location data and phone usage without consent, which it used to make decisions about insurance rates and coverage, a judge ruled Tuesday.

Since the plaintiffs said the software development kit (SDK) Allstate used to track consumers' movements "collects all manner of personal data regardless of how one uses the device, and they each allege that they downloaded an SDK-integrated app," they have shown they are entitled to relief, Judge Jeremy Daniel of the U.S. District Court for Eastern Illinois said in case 1:25-cv-00407.

Additionally, "because the complaint directly alleges fraud," a "heightened pleading standard applies," the judge found. But the plaintiffs meet that standard by pleading sufficient facts "to notify each defendant of [its] alleged participation in the scheme."

Further, "the complaint adequately pleads lack of consent to survive a motion to dismiss." The federal wiretapping claims were also allowed to stand, as the Fair Credit Reporting Act violation satisfied the crime/tort exception, the court ruled.

The federal court, however, dismissed claims that Allstate violated the Computer Fraud and Abuse Act and the California Computer Data Access and Fraud Act, since the plaintiffs failed to claim loss or damages under either statute.

Texas Attorney General Ken Paxton (R) filed a similar lawsuit against Allstate in January 2025 (see 2501130047).

Share Article

CIPA Decision Raises Bar for Standing in Privacy Claims, Lawyers Say

The recent dismissal of a privacy case concerning violations of the California Invasion of Privacy Act (CIPA) could mark a "significant shift" in how federal courts are evaluating injury claims in privacy cases, Fisher Phillips lawyers said in a blog post Thursday.

In *Maghoney v. Dotdash Meredith,* the plaintiff visited a health website twice and entered search terms about sexually transmitted infections. Despite expecting these searches to remain private, the site's advertising platform intercepted the information and transmitted it to third parties. This violated CIPA, the Confidentiality of Medical Information Act and was an invasion of privacy under the California Constitution, Maghoney argued.

But the U.S. District Court for Southern California found searches related to sexually transmitted infections "do not form a legally protectable privacy interest" and therefore can't be a concrete injury, the blog said. As such, the case was dismissed for lack of standing, though the plaintiff was granted leave to amend.

"The court honed in on the speculative and conclusory allegations that are regularly asserted in CIPA cases and asked 'where is the harm?'" the Fisher Phillips lawyers said. "Other courts facing similar claims may start to take guidance from this court's decision to interrogate plaintiffs' allegations that appear amorphous and abstract."

The case "raises the standard" for bringing CIPA claims and proves that "specific, concrete harm" is needed to establish standing, the blog said, nor is sharing metadata not linked to personally identifiable information enough for a privacy claim. Further, it "signals that courts may no longer accept generic or conclusory allegations in privacy lawsuits."

Share Article

Suit Claims Meta Misleads Consumers About AI Glasses' Privacy Features

Meta was hit with a class-action complaint Wednesday accusing it of misleading consumers about the privacy features of its AI glasses.

Meta has "marketed its new line of AI 'smart' Glasses as responsible, safe, and engineered to address the privacy concerns that define the AI era," promising "the Glasses were 'designed for privacy, controlled by you,'" the plaintiffs told the U.S. District Court for Northern California in case 3:26-cv-01897. But "that promise is false."

Whistleblower accounts have shown that footage from the glasses "is not processed privately or locally," but "transmitted to Meta's servers and then routed to a subcontractor in Kenya, where human workers manually view and label the footage to train Meta's AI models," the complaint said.

"No reasonable consumer would understand 'designed for privacy, controlled by you' … to mean that deeply personal footage from inside their homes would be viewed and catalogued by human workers overseas," the complaint added. "Meta chose to make privacy the centerpiece of its pervasive marketing campaign while concealing the facts that reveal those promises to be false."

The class-action suit contains many charges, including violations of the California Unfair Competition Law, the California False Advertising Law and the New Jersey Consumer Fraud Act, among others.

Meta's smart glasses have been controversial, with the Electronic Privacy Information Center (see 2602170025) and the U.K. ICO (see 2603040001) slamming the company for its plan of adding facial recognition technology to the glasses.

Share Article

EUROPE

CNIL Consults on Guide About AI in Health Care

French watchdog CNIL and the High Authority for Health (HAS) want input on a draft guide on AI in health care settings, the DPA said Thursday.

The guide is intended to address health care professionals' questions about their obligations and the best practices to implement, CNIL said, according to a translation. It cited a French Hospital Federation survey that found that 65% of public health institutions are already using AI in the care context.

While these technologies and their use are "undeniably promising, they raise numerous questions" about governance, patient information, digital security and more, the DPA said.

HAS and CNIL led a working group that studied issues in the care sector related to data protection, the DPA said. The group's draft guide aims to clarify the applicable legal and regulatory framework and obligations to which health care professionals and organizations are subject and to establish best-practice recommendations for the rollout of AI systems that are compliant, ethical and secure, it said.

The draft contains 10 fact sheets relating to the different stages of deployment and use of AI, from acquisition to uninstallation, and two on governance and the specifics of AI generative systems.

It classifies best practices into three levels, from "standard" to "advanced" to those that must be systematically adopted to avoid noncompliant, inappropriate or dangerous behaviors, CNIL said.

The guide applies to all actors in the health care sector and covers all AI systems with a direct impact on patient care. Comments are due April 16.

Share Article

ASIA PACIFIC

OAIC: Stores Should Be Cautious About Using Facial-Recognition Technology

Australian retailers should use an Administrative Review Tribunal decision on facial-recognition technology (FRT) in stores as a "useful case study, rather than a green light for deployment of biometric technologies," Privacy Commissioner Carly Kind said in a statement Thursday.

The Office of the Australian Privacy Commissioner (OAIC) issued a decision in 2024 aimed at clarifying the safeguards applicable to FRT, Kind noted. Bunnings, a leading home improvement retailer, had been using FRT for several years in more than 60 stores to tackle serious crime and theft by repeat offenders, she said.

The DPA found the company noncompliant with the Privacy Act, and the recent tribunal decision, which the watchdog hasn't appealed, provided further guidance, Kind said (see 2602050001).

The tribunal found that Bunnings faces a serious problem with violence and theft, that the threat is unique because of the size and layout of its stores, and that many of its products can be used as weapons, such as axes, screwdrivers and drills, Kind noted.

The administrative decision highlighted the data security and minimization protections that Bunnings had in place, concluding that although the use of FRT involved a significant intrusion into people's privacy, the company was entitled to use it for the limited purpose of fighting significant crime and protecting its staff and customers.

The decision didn't disturb OAIC's original findings that Bunnings failed to properly notify customers of its use of FRT, that there weren't appropriate policies and procedures in place to govern its use, and that the Privacy Act's safeguards apply in the context of biometric technologies, even when they collect and keep personal data only for milliseconds, Kind said.

Australian stores want and need to deploy FRT, and they have demanded greater certainty about how privacy law applies, Kind said. The tribunal decision shows that the country's privacy law allows a balancing of the interests of the public to have privacy and the need to protect public safety, she added.

OAIC will now issue specific updates to existing guidance to reflect the administrative decision and ensure that stores have revised information on its regulatory approach, Kind said.

The updates will also stress that the Bunnings decision "confirms a high bar for the use of facial recognition technology" and that entities must conduct a detailed risk assessment specific to their circumstances before launching it, Kind wrote.

Share Article