May 27, 2025

Kilpatrick's Privacy Dispatch – May 27, 2025

by Meghan K. Farmer , Tatum Andres , Katherine S. Kubik , Henry W. Tharpe

---

Here are some recent privacy and cybersecurity related news stories that caught our attention over the past couple of weeks.

California Privacy Protection Agency (CPPA) Issues New Proposed Regulations

The CPPA has released updated draft regulations for public comment, now open until June 2. The agency's latest analysis estimates that Year 1 compliance costs for in-state businesses will be about $1.2 billion—a substantial decrease from the original $3.4 billion projection.

Do these revised cost estimates align with your organization's privacy compliance planning?

What you should do:
Review the proposed regulations, assess your current compliance strategy, and consider submitting feedback before the June 2 deadline.

Learn more here.

Some relief for companies from website tracking litigation? Tester Plaintiffs Cannot Bring CIPA Claims, Says Federal Court

A new case has been decided: In Rodriguez v. **Autotrader.com**, Inc., a California federal court held that a self-proclaimed "tester" plaintiff lacked standing to sue under the California Invasion of Privacy Act (CIPA). The plaintiff admitted she visited the website specifically to test for privacy violations, leading the court to conclude she could not claim injury when her expectations were "ultimately met."

The bottom line:
This decision offers a major defense for businesses facing CIPA lawsuits filed by repeat plaintiffs who target websites for litigation purposes. It also underscores the importance of setting and disclosing privacy expectations clearly.

What you should do:
Don't take your foot off the gas just yet. Review your company's website Privacy Policy, cookie banner (or similar interactive notice), and tracking technologies to ensure compliance. Make sure your company has a

clear understanding of how data is collected and shared, and that users are provided with clear notice and meaningful options to affirmatively consent or opt out to strengthen your defenses against potential CIPA claims.

In case you missed it: Michigan's Attorney General has filed a lawsuit against Roku, alleging that the company collects and shares children's personal data and video viewership data in violation of COPPA and the VPPA, respectively.

The complaint claims Roku systematically gathers sensitive information from children—including voice recordings, geolocation, and browsing history—without proper parental notice or consent, and shares this data with third parties. The complaint contrasts Roku's child-facing experiences (which lacks children's profiles) against similar platforms that allow parents to set up and manage their children's viewing experience.

Why it matters:
Children's privacy and online safety remain a focal point for regulators.

Our take:
The complaint takes an expansive view of COPPA applicability, namely that persistent identifiers tied to child-directed TV channels is enough to trigger the statute's applicability (even when Roku might not have had any knowledge of which members in a household actually viewed those channels). If you've considered COPPA inapplicable to your company in the past, consider re-evaluating your company's approach to COPPA in light of that theory.

Click here to view the press release.

Illinois Federal Court Dismisses BIPA Claim Against Hyundai Over Driver Monitoring Technology

A federal court in Illinois has dismissed a class action suit filed under the Illinois Biometric Information Privacy Act (BIPA), finding that Hyundai did not "collect, capture, or otherwise obtain" biometric data by use of its Forward Attention Warning System (FAWS) installed in certain vehicles. FAWS operates to monitor a driver's eye position and warns the driver via a visual alert on the center display screen when it detects signs of inattention, such as when the driver looks away from the road for too long, closes their eyes, or displays inconsistent driving patterns.

The bottom line:
Even though FAWS monitors drivers' eye and facial position to detect inattentiveness, the court held that merely offering a tool capable of biometric processing does not amount to biometric data collection under BIPA. This case reinforces that BIPA liability requires more than designing or enabling a system capable of biometric data collection, it requires actual collection or control over the data. The decision aligns with prior rulings where the court held that providing a tool capable of facial scanning is not the same as collecting biometric data, and that BIPA did not apply when data remained solely on a user's device.

Our advice:

Companies that deploy biometric technology should consider this business-friendly nuance of BIPA applicability when designing products and services that might implicate biometrics or similar scanning. Counsel therefore face fewer roadblocks enabling tools that may scan physical attributes but don't capture biometrics compared with those that create and access biometric information.

Be sure to follow the firm's LinkedIn page to see more of these news snippets with our commentary.