April 9, 2026

Kilpatrick's Privacy Dispatch - April 2026

by Meghan K. Farmer , Tatum Andres , Katherine S. Kubik

Washington's New AI Disclosure Law: A Leap Toward Transparency and Consumer Protection in the Digital Age

On March 24, 2026, Washington Governor Bob Ferguson signed HB 2225 into law, requiring companies to clearly disclose when consumers are interacting with AI rather than a human. The goal is straightforward: reduce deception and increase transparency as AI tools become more embedded in everyday customer interactions. The law, which takes effect January 1, 2027, also introduces targeted safeguards for AI “companion” chatbots, with a particular focus on protecting minors. For companies deploying chatbots, this is less about overhauling technology and more about tightening user-facing disclosures, product design, and user trust. It is another strong signal that regulators are focusing on how AI is presented to users, not just how it operates behind the scenes. Expect similar transparency requirements to gain traction in other states. Idaho and Georgia may soon follow with stricter requirements, so stay tuned.

States Crack Down on Algorithmic and “Surveillance” Pricing

A new wave of state action is putting algorithmic pricing practices in the spotlight. On January 27, California Attorney General Rob Bonta announced a “surveillance pricing” sweep targeting companies that charge different online prices based on consumer data. The concern? That using personal information to tailor prices may go beyond what consumers reasonably expect under the California Consumer Privacy Act (CCPA).

This enforcement push comes on the heels of New York passing the nation’s first algorithmic pricing disclosure law, signaling that regulators are no longer just watching this space, instead they are actively stepping in.

Meanwhile, Tennessee has taken a similar approach by introducing Senate Bill 1807 which prohibits businesses from setting prices for Tennessee consumers using personalized algorithmic pricing. "Personalized algorithmic pricing" means dynamic pricing set by an algorithm that uses personal data. The law includes definitions for “algorithm” and “dynamic pricing” as well as clarifies that “personal data” includes information linked or could reasonably be linked to a specific consumer or device.

The bill includes limited exemptions, such as certain subscription-based discounts where the personalized price is lower than the standard rate. If signed into law, it will take effect July 1, 2026, and violations will be treated as unfair or deceptive acts under the Tennessee Consumer Protection Act.

The bottom line:

States are moving quickly to regulate personalized pricing, some through disclosure requirements, others through direct bans and enforcement sweeps. Companies that use consumer data to adjust prices are squarely in regulators' sights.

What you need to do:

Now is the time to take a close look at your pricing practices. Identify whether you use consumer data to influence prices, what data feeds into those systems, and whether consumers would reasonably expect that use. If you operate in Tennessee, start planning now for compliance ahead of the July 1, 2026, effective date. Proactive review today can help avoid enforcement headaches tomorrow.

Kentucky Enforcement Action Against Character.AI

On January 8, 2026, the Kentucky Attorney General filed a lawsuit against Character Technologies, Inc., owner of Character.AI, an artificial intelligence chatbot designed for interactive entertainment. The complaint alleges (1) unfair, deceptive and dangerous acts and practices, (2) unfair collection and exploitation of children's data, (3) violation of the Kentucky Consumer Data Protection Act (which went into effect January 1, 2026), (4) violation of Kentucky's statutory and constitutional privacy protections, and (5) unjust enrichment.

The Kentucky Attorney General's complaint focused on the claim of unfair, false, misleading or deceptive acts and practices in relation to Character.AI's impact on minors. The complaint alleges that Character.AI misrepresented that it "was safe, age-appropriate, and responsibly moderated, despite knowing of widespread instances of harmful, explicit, and psychologically manipulative chatbot interactions with minors."

To support this allegation, the complaint asserts the following factual allegations:

1. Character.AI characters are designed to believably simulate human interaction without sufficient disclosures to its users, which encourages emotional bonds between users and the chatbots.
2. Character.AI did not have effective age verification methods and relied on a user's declared ages until late 2025. The age verifications now in place can still be easily bypassed.
3. The chatbots engaged in inappropriate interactions with children, including discussions of sexually explicit content, suicide, eating disorders, bullying and illegal drug and alcohol use, without sufficient guardrails. Warnings about suicide risks can be clicked past without further action and warnings about pro-anorexia content were surfaced after the chatbot provided dangerous advice.
4. Tools for parental oversight are limited, and minors can avoid the parental controls by changing the email address associated with the account so the weekly summary of a child's daily average time spent and top

characters engaged with is not delivered to the parent's email address.

To read the full blog post, click here.

Looking Ahead to Privacy (and Similar) Issues for 2026

Privacy law evolved at a dizzying pace in 2025. Regulators brought headline-making enforcement actions, courts continued to shape the boundaries of existing statutes, and state legislatures advanced new laws.

Much of that activity centered on familiar pressure points: privacy notices and opt-out mechanisms, telemarketing and text messaging practices, and the collection and use of sensitive data, particularly biometric information, health data (such as the Healthline CCPA enforcement), and children's and teen's personal information (including actions against Roku in multiple jurisdictions).

Newly effective laws echoed those same priorities. For example, Maryland's comprehensive privacy law and several children's privacy statutes in states like New York and Colorado place new limits on how children's data may be used for advertising and related purposes, while Colorado also expanded consent requirements for certain biometric processing affecting both consumers and employees. In parallel, changes at the federal level including the FCC's expanded revocation-of-consent rule, continued to reshape expectations around consumer choice and control.

We expect that momentum to carry into 2026. To help you keep track, we've pulled together the key privacy laws and regulatory developments to watch in the year ahead.

To read the full blog post, click here.

California Attorney General Secures $1.4 Million Settlement with Jam City for CCPA Violations

California Attorney General Rob Bonta reached a settlement with Jam City, Inc. requiring the mobile gaming company to change its advertising practices and pay $1.4 million in civil penalties for violations of the California Consumer Privacy Act.

Jam City allegedly committed two categories of violations. The company failed to provide CCPA-compliant opt-out methods across all 21 of its mobile applications, despite the fact that it collected and shared consumer information almost entirely through these gaming apps. Jam City also disclosed data belonging to minors aged 13 to 16 years without obtaining the affirmative opt-in consent that California law requires for this age group (for some, but not all games, Jam City directed users reporting an age under 16 to experiences without targeted advertising).

This enforcement action demonstrates that mobile application developers are better off integrating opt-out mechanisms directly into their apps rather than relying solely on external privacy policies or website-based tools. Companies must also obtain consent or disable targeted adverting to minors aged 13 to 16 (e.g., based on inferred or reported age).

California Attorney General Rob Bonta has steadily expanded CCPA enforcement through settlements targeting deficiencies in consumer opt-out mechanisms, sensitive data handling, and children's privacy. The Jam City matter builds on recent actions against companies for allegedly failing to provide an accessible method to opt out of the sale of personal information and for inadequate protections for minors.

Taken together, these enforcement actions signal a sustained and increasingly sophisticated approach by the California Attorney General's Office to CCPA compliance, particularly in the mobile and digital advertising ecosystems. Companies that collect or share personal information through online applications should expect heightened scrutiny of in-app opt-out functionality, age-based consent mechanisms, and disclosures related to sensitive data.

NetChoice has sued Virginia to block the state's new social-media law (SB 854), which is set to take effect January 1.

The 41-page complaint, filed in federal court, argues that the law violates the U.S. Constitution and is therefore unenforceable. SB 854 would limit minors under 16 to one hour per day on social media unless a parent provides consent for more time, and it allows parents to further reduce usage. The challenge is the latest in a growing line of cases where NetChoice has successfully pushed back against state efforts to regulate minors' online activity, including recent lawsuits in Louisiana, Georgia, and Colorado—where courts have already blocked similar laws on First Amendment grounds.

The bottom line:
Virginia's law is unlikely to take effect as written. Courts across the country are signaling strong constitutional concerns with state attempts to regulate minors' access to social media, and early injunctions in other states suggest SB 854 may face the same fate.

What you need to do:
Companies operating social-media platforms or offering youth-directed features should monitor the Virginia litigation closely and prepare for rapid shifts in compliance requirements. Consider assessing current parental-consent flows, time-management tools, and minor-specific settings now, so you can adapt quickly depending on how the courts rule. We're also closely following litigation challenging the Texas law on app store age verification.

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