HUNTON

Retail GC Hot Topics

Summer 2026

PRIVACY

REAL ESTATE

LITIGATION

LABOR & EMPLOYMENT

ENVIRONMENTAL

INSURANCE COVERAGE

PRIVACY

Website Tracking Litigation and the Retail Sector:
Understanding Risks Under CIPA, ECPA, and Similar Laws

Retailers face growing privacy liability from commonplace website technologies such as cookies, tracking pixels, similar analytics, and marketing tools. Plaintiffs invoke the California Invasion of Privacy Act (CIPA) and the federal Electronic Communications Privacy Act (ECPA), statutes enacted decades before these technologies existed. These claims pose a heightened risk for retailers whose e-commerce operations depend on high-traffic websites and apps, real-time analytics, advertising technology, and customer-support chat features.

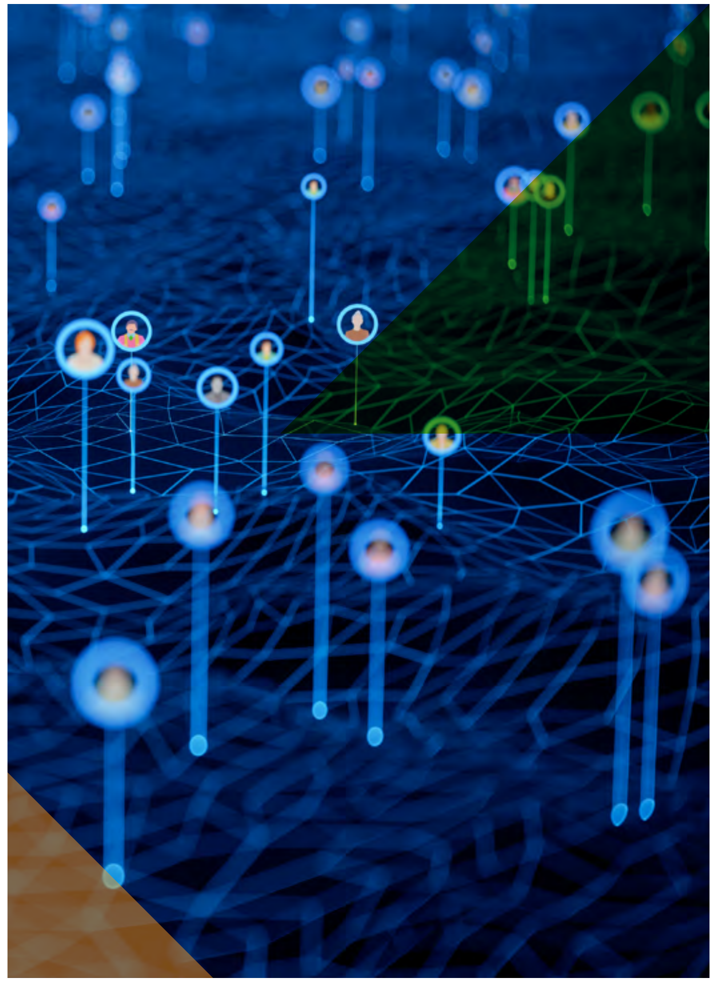
The Legal Framework

CIPA Section 631(a), among other things, prohibits willfully reading or learning the contents of a communication in transit without all-party consent. Section 638.51 bars installing or using a pen register or trap-and-trace device without a court order unless all-party consent is obtained. CIPA provides statutory damages of $5,000 per violation and does not require a showing of actual damages.

ECPA adds a federal layer of liability by prohibiting the intentional interception of electronic communications while in transit. Unlike CIPA's all-party consent standard, ECPA operates as a one-party consent regime. However, one-party consent does not apply where the interception is for the purpose of committing any criminal or tortious act. ECPA provides damages of $100 per day for each day of violation or $10,000, whichever is greater.

Litigation Surge

CIPA claims have surged, with the number of reported cases under the pen register provision growing from roughly 600 to more than 4,000 in approximately one year. Technologies such as Google Analytics, Meta Pixel, and TikTok Pixel are common targets. Because courts remain divided on whether these statutes reach common tracking technologies, a motion to dismiss is far from assured, and litigation costs mount quickly. Because CIPA provides $5,000 per violation without requiring proof of actual harm, putative class exposure can reach tens or hundreds of millions of dollars even where the merits are contested.



Key Judicial Developments for Retailers

Retailers are natural targets because they operate high-traffic websites reliant on tracking technologies for advertising, analytics, and customer engagement. Recent decisions illustrate a divergence in outcomes in the courts.

In *Camplisson v. Adidas America, Inc.*, 2025 WL 3228949 (SD Cal. Nov. 18, 2025), the court denied a motion to dismiss a CIPA pen register claim by declining to credit the retailer's consent defense given its reliance on footer-based disclosures that did not require affirmative consent before tracking began. In contrast, in *Doe v. Eating Recovery Center LLC*, 2025 WL 2971090 (ND Cal. Oct. 17, 2025), the court granted summary judgment on a CIPA wiretap claim, finding no evidence that the third-party vendor actually read or attempted to read plaintiff's communications while they were in transit. The court also expressed skepticism that CIPA can be applied to internet communications, finding it's "virtually impossible to apply it to the online world."

California SB 690: A Potential Safe Harbor and Its Limits

Senate Bill 690 (SB 690) represents the California legislature's effort to provide partial relief. As amended in July 2026, the bill would revise Section 637.2—the provision that supplies CIPA's private right of action and statutory damages—to provide that only the attorney general may bring a private action alleging a violation of Section 638.51, the pen register statute, when the alleged conduct occurs on an internet website, online application, or mobile application. In practical terms, the bill would not declare the underlying tracking conduct lawful, but it would remove the private damages remedy. The current version would apply retroactively to pending Section 638.51 claims filed within two years before its operative date of January 1, 2027. SB 690 remains pending.

Practical Considerations and Risk Mitigation for Retailers

Website-tracking litigation remains a live and escalating risk. Even if SB 690 is enacted, it would address only the private right of action for pen register claims. Wiretap theories under Section 631 of CIPA and ECPA would remain available.

The case law presents a mixed picture. In many cases, plaintiffs have been able to survive a motion to dismiss where tracking pixels fire before any affirmative opt-in and disclosures are located in a footer. At the same time, a growing number of judges have expressed skepticism that CIPA reaches ordinary internet practices. Standing challenges have also gained traction, with courts dismissing claims where the plaintiff failed to allege a concrete, particularized injury. Outcomes may turn on the specific facts of each website's consent flow, the nature and timing of data transmissions, and the jurisdiction in which a case is filed.

The volume and trajectory of website-tracking litigation underscore the importance of treating consent architecture as a risk-management priority. Key steps include auditing all tracking technologies deployed on websites and apps, aligning cookie management platforms with the organization's consent approach (e.g., blocking all nonessential tracking until consent is received for a conservative approach), confirming privacy notices accurately describe data flows, reviewing vendor contracts to ensure data cannot be used in ways that increase legal exposure, and preserving website configurations and consent artifacts to support defenses. We are actively monitoring SB 690 and the developing case law. ■

REAL ESTATE

States Increasing Focus on Grocery Store Real Estate Restrictions

There is an emerging legislative trend to limit the ability of grocery store operators to use restrictive covenants to prevent competitors from occupying spaces they own, sell, or lease. These measures generally target deed restrictions, lease provisions, and similar agreements that bar a successor tenant or purchaser from operating a grocery business at a location previously controlled by a grocery chain.

Lawmakers increasingly view these provisions as contributing to prolonged vacancies, reducing consumer choice, slowing the reuse of commercial space, and exacerbating food deserts in certain communities. Academics have written and presented articles on how restrictive covenants (as well as grocery retailers retaining ownership and leasehold interests in dark sites) are contributing to food deserts in the US. In the most visible cases, a dark grocery box can remain vacant for years while also preventing another grocery operator from entering the market. Antitrust enforcers outside of the US, including in Australia, the UK, New Zealand, and Canada have already taken action against such restrictions since at least 2020.

Rhode Island recently joined this movement through Senate Bill 2644, effective June 18, 2026. That law generally provides that a restrictive covenant concerning the use of land designated as a retail establishment where fresh food is regularly and customarily sold for off-premises consumption—including a grocery store or supermarket—is void and unenforceable, subject to certain exceptions. The State of Washington took a similar approach with House Bill 2294. Subject to certain exceptions, the law provides that a private

use restriction on real estate that prohibits or restricts the use of property as a grocery store or pharmacy is against public policy and is void and unenforceable. A similar bill has been introduced in California and is reportedly under consideration in Arizona.

Cities have also been active. Chicago and Washington, DC have enacted measures aimed at limiting the use of restrictive covenants that impede grocery operations. In Washington, DC, Code § 2-1212.61 makes it unlawful for an owner or operator of a grocery store to agree to a restrictive covenant in a contract for sale, lease, or other transfer document that prohibits the use of the property as a grocery store or food retail store, or that prohibits the use of property within one mile as a grocery store or food retail store. In addition, DC Law 25-201 establishes a mechanism for eliminating unlawful restrictive covenants from property records, including restrictions that may affect grocery uses.

Although the details vary by jurisdiction, these laws tend to operate in similar ways. Some render covered restrictions void or unenforceable as against public policy. Others prohibit a party from creating, recording, or enforcing a covenant that bars future grocery use after the original operator leaves. Definitions and exceptions also matter. Depending on the jurisdiction, the law may turn on store size, product mix, sales thresholds, or whether the operator falls within a chain-store definition. As a result, relatively small drafting differences or factual distinctions may determine whether a law applies to restrictions contained in deeds, leases, or other transfer-related documents.

Retailers should anticipate that this trend may expand. Given the current focus on increasing grocery prices, it would not be surprising to see other states or even the federal antitrust agencies take action in this space. The current focus is on grocery uses, but the underlying policy concerns, including vacancy, competition, and access to essential goods, could readily extend to other retail categories. Multistate operators should monitor not only enacted statutes and ordinances, but also bills moving through state legislatures and city councils, where real estate controls are increasingly being evaluated through antitrust and consumer-protection lenses.

In-house counsel should be aware that restrictive covenants that once were treated as standard real estate tools now require jurisdiction-specific review. Retailers should consider reviewing lease forms, recorded covenants, and transaction documents to identify provisions that may be unenforceable or that may need to be revised to reduce risk in future leasing, redevelopment, and disposition activity. We will continue monitoring activity at the state and federal level on this issue. ■

LITIGATION

Don’t Wait for a Breach:
A Retail General Counsel’s Guide to Protecting Trade Secrets

In retail, the most valuable assets often include pricing strategies, customer analytics, vendor terms, and private-label specifications. These trade secrets provide a critical edge in a hyper-competitive market. However, that advantage vanishes if proprietary data is leaked by a vendor or downloaded by a departing employee.

Under the Defend Trade Secrets Act, legal remedies often depend on whether a company took reasonable measures to maintain secrecy before a dispute arose. For general counsel (GC), trade secret protection is a governance priority, not just a litigation response.

Identify and Classify High-Value Information

The process begins with an internal audit to identify what qualifies as a trade secret.

In retail, this may include:

- Non-public markdown, margin, and promotional strategies
- Design specifications and formulas for private-label products
- Loyalty program analytics and segmentation data
- Distribution, fulfillment, and loss-prevention playbooks

Once identified, information must be classified. A “Trade Secret—Restricted” label should trigger stricter controls than a general “Confidential” tag. Establishing a cross-functional committee to review these classifications ensures that protection evolves with the business.

Implement Robust Access Controls

Retailers must share data quickly across merchandising, finance, and logistics teams, making role-based access essential.

GCs should collaborate with IT to implement:

- Multifactor authentication and encrypted drives
- Detailed logging of all access, downloads, and external transfers
- Physical security for prototype rooms and product samples
- Strictly limiting access to those who need the data to perform their roles

Strengthen Contractual Protections

Confidentiality agreements are a cornerstone of protection. Every employee, contractor, and brand partner should sign a nondisclosure agreement before viewing sensitive data. Agreements should clearly define trade secrets, set limits on subcontracting, and establish audit rights. When dealing with global vendors, GCs must verify whether these contracts are enforceable in the local jurisdiction.

Training and Policy Accessibility

Employees cannot protect what they do not understand. Regular training should address real-world retail risks, such as:

- Uploading internal files to personal cloud storage
- Using unapproved generative AI tools with proprietary data
- Discussing merchandising plans at industry events

Policies must be concise. If they are overly complex or buried in a handbook, they lose their effectiveness and may be harder to defend in court as a reasonable measure.

Monitor and Audit Third-Party Relationships

Retailers rely on an ecosystem of logistics, manufacturing, and tech partners. Before sharing data, vet a vendor's security posture and limit disclosure to the minimum necessary scope. Continuous monitoring, such as auditing vendor access logs and reviewing data-loss prevention alerts, is critical for early detection of an unauthorized leakage.

Prepare an Incident Response Plan

When a leak occurs, speed is vital. An incident response plan should designate the GC as the central point of contact and outline protocols for:

- Evidence preservation and forensic investigation.
- Immediate containment of unauthorized access.
- Evaluating the need for emergency injunctive relief.

A clear plan avoids panic and ensures the organization remains in a strong position should litigation become necessary.

Formalize Exit Procedures

Departing employees with access to pricing or vendor data represent a recurring risk. Offboarding should include:

- Immediate revocation of all system and facility access
- Recovery of all company devices and physical documents
- An exit interview specifically reminding the individual of their ongoing confidentiality obligations

Retailers should review recent download activity to identify potential data scraping before the employee's departure.

Legal Enforcement and Compliance

Trade secret strategies must be reviewed annually to remain compliant with evolving laws. Ultimately, a retailer's ability to win a misappropriation case depends on proving that the information was treated as a crown jewel rather than an afterthought.

By integrating these steps into sourcing, merchandising, and human resources processes, GCs can create a defensive shield that protects the company's competitive advantage and deters infringement by competitors.

LABOR & EMPLOYMENT

New Union Strategies Aim to Leverage Supply Chains of Lead Firms

Although supply chain labor has long been a primary focus for unions, the COVID-19 pandemic changed how labor viewed supply chain leverage, especially in retail. Years of planning during COVID-19 produced new approaches to creating co-employer liability for lead firms—companies that sit at the top of supply chains, franchise systems, subcontracting networks, and other business arrangements in which work integral to their business is performed by workers whose legal employer is another entity. Initial steps are now maturing into a comprehensive approach aimed at the commercial heart of the retail model. By 2027, retail's central labor challenge will be a sophisticated, top-down strategy to force lead firms into binding agreements.

Historically, unions viewed leverage as attacking the employer's own vulnerabilities—its wage-hour practices, health benefits, and working conditions. Unions now view the supply chain itself as the vulnerability. As they frame it, the prices, volumes, and deadlines the lead firm imposes on their suppliers leave those suppliers with no room to pay more, staff up, or slow down, so the supplier's treatment of workers is attributed to the lead firm that dictated those terms. The approach makes the lead firm answerable for conditions it does not directly control, and that gap is precisely what makes the leverage work.

The December 2026 conference agenda from the UNI Commerce Division of UNI Global Union, the world's largest global labor federation, illustrates the shift. One of the conference's key themes include "Growing Union Power in Value Chain", this is a direct reference to the new approach. The global federations have built the infrastructure necessary for a sustained, coordinated effort. UNI and IndustriALL, another large global union federation, launched a Human Rights Due Diligence Competence Centre, and UNI followed with a Due Diligence Toolkit, both built to drive worker demands into a lead firm's oversight of its suppliers. The EU's Corporate Sustainability Due Diligence Directive (CS3D) adds legal and financial risk, turning aspirational commitments into legally enforceable ones. That risk enhances unions ability to leverage a lead firm's own codes of conduct and due diligence commitments.

The key to this plan is replacing employer and third-party due diligence with worker-driven social auditing. Unions argue that company-controlled auditing is subject to manipulation and also leaves the lead firm's own purchasing practices beyond reach. The plan to dismantle the current due diligence regime finds some support in CS3D, which speaks to verifiers having "complete independence from the company," to be "free from any conflicts of interest," and free from "external influence, whether direct or indirect."

As the UNI conference material illustrates, the near-term strategy will focus on two areas: artificial intelligence and health and safety. AI captures the zeitgeist—the fear of displacement and of skilled work reduced to menial tasks. That fear makes it a potent subject for a leverage campaign because it reaches past the workforce to customers, investors, and regulators who share it, giving a union an audience primed to see the lead firm as the driving force in workplace disruptions. Threatened AI dislocations also fit the unions' "just transition" framing perfectly, converting a technology rollout into a moral question, and making every operational decision a potential subject of stakeholder engagement. Framed this way, AI shifts the argument from working terms to operational ones, giving unions leverage over how the lead firm runs its business, not merely how it treats the people inside it.

Health and safety appears tactical but works strategically because simply asking the question "how safe" positions the lead firm as putting profits over people. The garment campaign runs this play openly. The June 2026 report *Mitigating Heat Stress in the Garment, Footwear, and Travel Goods Sector*, for example, sets out what firms already have in place and then argues it falls short of the danger workers face. Heat is only one front. Third-party violence, harassment, burnout, working while sick, staffing cuts, delivery windows, or speed targets each trace up the chain. Retail's promises of speed and convenience—rapid replenishment and high-velocity fulfillment—translate directly into physical hazard at every link, putting the lead firm that set those terms on the hook for the harm they produce.

The ultimate objective is binding agreements with lead firms—a global framework agreement, the international accord, or both. Each is offered to the lead firm as a lifeline, the way to mitigate the very supply chain risk the campaign built against it. Recognizing the playbook can assist lead firms in evaluating the value of that proposition. ■

What Retailers Need to Know About the Proposed Faster Labor Contracts Act

On June 9, 2026, the US House of Representatives passed the Faster Labor Contracts Act, HR 5408. The bill now moves to the Senate. If enacted and signed into law, it could significantly change how retailers negotiate first collective bargaining agreements with newly recognized unions, by replacing today's open-ended process under the National Labor Relations Act (NLRA) with an expedited framework that could end in binding arbitration.

Under current federal labor law, retailers—like other employers—must bargain in good faith, but they are not required to reach an agreement, accept a particular proposal, or make concessions, and there is no set deadline for a first contract. HR 5408 would fundamentally change that. It would impose an accelerated bargaining schedule—approximately 120 days total—that would move the parties from bargaining to mediation and, ultimately, to binding arbitration.

Key Requirements Under HR 5408

- Management would have 10 days to meet and begin bargaining after receiving a written request from a newly recognized or certified union.
- The parties would be required to make every reasonable effort to reach and sign a first contract.
- If no agreement is reached within 90 days, either party could request mediation through the Federal Mediation and Conciliation Service.
- If mediation does not resolve the dispute within 30 days, the matter would be referred to a three-person arbitration panel, whose first-contract decision would be binding for two years.

For retailers, the most significant practical risk is that first-contract terms could be set by arbitrators, rather than negotiated voluntarily at the bargaining table. The expedited schedule imposed by this bill alters bargaining leverage and requires employers to respond rapidly and strategically to bargaining demands from newly recognized unions. The potential for a non-negotiated binding contract to be imposed at the conclusion of every bargaining effort deprives retailers of their traditional power and the right to refuse terms that are harmful to their business.

Retail businesses depend on flexible operating models to respond to changing customer demand, seasonal fluctuations, staffing needs, and global market conditions. A regime that allows third-party arbitrators to set first-contract terms on wages, scheduling, benefits, safety rules, leave policies, and other workplace conditions could create substantial legal and operational risk for retailers managing dynamic, multilocation workforces.

Potential legal challenges to HR 5408 are already being discussed. Critics argue that, by departing from the NLRA's traditional framework of requiring good-faith bargaining without compelling agreement on particular terms, the bill invites challenges grounded in freedom of contract principles and constitutional doctrines, including the Takings Clause, non-delegation doctrine, and Appointments Clause. Critics also contend that the proposed bill could unconstitutionally bind workers to first contract terms without a ratification vote.

The bill's passage reflects ongoing developments in labor policy that may influence union organizing activity. Both the proposed legislation and the surrounding labor relations environment could lead to an increase in organizing petitions, particularly where first-contract negotiations are at issue. Retailers should consult with labor counsel to understand the potential risks posed by HR 5408 and develop a plan to address them. ■

ENVIRONMENTAL

Update on Implementation of California's EPR Program

In May, after much anticipation and delay, California's Office of Administrative Law (OAL) officially finalized the California Department of Resources Recycling and Recovery's (CalRecycle) permanent regulations for the state's extended producer responsibility (EPR) program for single-use packaging and food serviceware. The new regulations went into effect on May 1, 2026, when OAL approved them and filed them with the secretary of state. To comply, producers had until June 1 to register with the producer responsibility organization (PRO) or CalRecycle, and to apply for either independent producer status or a small producer exemption. Producers also faced a May 31, 2026, deadline to submit 2023 baseline data, 2025 supply data, and a 2025 source reduction report, with an individual source reduction plan due August 3, 2026. Producers that fail to meet these deadlines risk enforcement action, including statutory penalties of up to $50,000 per violation per day following a 30-day notice-and-cure period. Simultaneously, Circular Action Alliance (CAA), the PRO tasked with administering the program, published guidance on illustrative fees for obligated producers. Illustrative fees are described as "good faith, non-binding fee rate ranges intended to support producers in planning, internal budgeting, and early consideration of source reduction, reuse, and refill strategies ahead of formal program plan approval and final fee setting." The illustrative fees are intended to aid producers in budgeting, and planning, but may not reflect additional costs based on the newly finalized regulations. CAA also published a separate early fee schedule tied to producers' 2025 supply data, with an estimated invoice date in August 2026.

On June 15, 2026, CAA hit another major milestone, submitting its draft California Program Plan to the SB 54 Advisory Board. A public comment period on the draft plan runs through August 14, 2026, after which CAA intends to submit a final program plan to CalRecycle in October, with CalRecycle approval to follow. CAA anticipates publishing final fee rates in October 2026.

The final regulations have drawn legal challenges from multiple directions. In early June, environmental groups challenged the regulations in state court, arguing they fail to comport with the statute by exempting certain plastic packaging and allowing "polluting technologies," such as chemical recycling, to count toward recycling targets. Separately, a coalition of 17 state attorneys general and the National Association of Wholesaler-Distributors (NAW) are challenging SB 54 on First Amendment, due process, and dormant commerce clause grounds. NAW is the same organization that was recently successful in obtaining a preliminary injunction to block enforcement of Oregon's EPR law for its members while its litigation challenging that law is pending.

For manufacturers and retailers of packaged goods, the near-term picture is one of firm deadlines layered on top of financial and legal uncertainty. Because registration, baseline reporting, and source-reduction reporting obligations are now in effect, producers should establish compliance processes that include identifying opportunities to improve data quality over time. At the same time, final fee rates are not expected until October 2026, leaving producers to budget against a moving target for now. Pending litigation adds a further layer of risk, since the outcome could require producers to revisit compliance strategies. We will continue to monitor these developments as CAA's program plan moves toward final approval and as the litigation progresses. ■

INSURANCE COVERAGE

When BIPA Claims Hit:
Insurance Challenges for Retailers

Retailers continue to deploy biometric tools across their businesses. Fingerprint-based time clocks, facial recognition, loss prevention technology, and customer identity-verification tools can all improve efficiency and security. But for retailers with operations in Illinois, those tools can also create meaningful exposure under the Illinois Biometric Information Privacy Act (BIPA).

That exposure is not just a privacy issue. It is also an insurance issue. When a BIPA demand letter or lawsuit arrives, retailers often look to their liability policies for defense and indemnity. Although recent Illinois federal court decisions suggest that coverage may be harder to secure, policyholders are not without insurance coverage options.

Why BIPA Matters to Retailers

BIPA regulates the collection, use, storage, and disclosure of biometric identifiers such as fingerprints, hand scans, and facial geometry. The law matters because biometric technology often sits inside routine business functions throughout the retail sector. On the workforce side, it may be used for employee timekeeping or access control. On the customer side, it may appear in fraud prevention, store security, digital identity verification, or other consumer-facing tools. Retailers also tend to use these systems at scale. A single practice may be rolled out across many stores, applied to a large hourly workforce, or embedded in customer-facing systems handling high transaction volume. That can increase both compliance risk and litigation exposure. Although BIPA's 2024 amendments reduced certain damages concerns, the statute remains an active source of claims.

The Coverage Question

Companies facing BIPA claims have often turned to commercial general liability (CGL) policies. But insurers have increasingly relied on exclusions to deny coverage, particularly exclusions addressing access to or disclosure of confidential or personal information, statutory violations, and employment-related practices. Whether coverage exists still depends on the wording of the policy, the policy year, and the governing law. But the recent trend has favored insurers.

Recent Cases Point to a Tougher Coverage Landscape

In *Sentinel Insurance Co. v. Majestic Auto Glass, LLC*, 2026 WL 663820 (N.D. Ill. Mar. 10, 2026), the court held that an access/disclosure exclusion barred coverage for a BIPA claim.

In *JJM Group Limited v. West Bend Mutual Insurance Co.*, 2025 WL 3267286 (ND Ill. Nov. 21, 2025), the court reached a similar result in a case involving fingerprint collection and use for commercial purposes and also found no coverage for related non-BIPA claims.

The same pattern appeared in *Harleysville Lake States Insurance Co. v. Thermoflex Waukegan, LLC*, 2025 WL 2778458 (ND Ill. Sept. 30, 2025). There, the court enforced an access/disclosure exclusion in a 2017 policy involving biometric timekeeping, but the insurer still owed a defense under 2015 and 2016 policies that did not contain the same exclusion. For retailers, that is an important reminder that older policy years may matter.

In *Phoenix Insurance Co. v. Ackercamps.com*, 805 F. Supp. 3d 901 (SD Ill. 2025), the court likewise held that an access/disclosure exclusion barred coverage for claims involving facial recognition software.

One recent case offers a different lesson. In *Thornley v. Citizens Insurance Co. of Am.*, 2026 WL 851407 (ND Ill. Mar. 28, 2026), the court denied the insurer's motion for judgment on the pleadings because there were factual disputes over whether the insurer had waived its exclusion-based defense or raised it too late. Even where an exclusion appears strong, claim-handling issues may still matter.

Suggested Action Items for Retailers

Retailers can take several practical steps, including:

1. Reviewing all policy years for changes in exclusion wording
2. Assessing other potential sources of coverage, including cyber, technology E&O, and management liability policies
3. Evaluating whether a complaint includes non-BIPA claims that may still trigger a duty to defend
4. Reviewing reservation of rights and denial letters carefully for waiver or other claim-handling issues

For retailers, BIPA is an operational, litigation, and insurance issue. As courts continue to enforce exclusions, early coordination among legal, risk, and business teams may make a meaningful difference when a claim arrives. ■

EDITORS

Latosha Ellis
Partner
Insurance Coverage Litigation

Tyler Laughinghouse
Counsel
Labor and Employment

CONTRIBUTORS

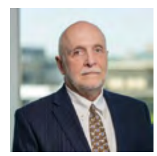
Geoffrey B. Fehling
Partner
Insurance Coverage Litigation

Armin Ghiam
Partner
Intellectual Property

Kevin Hahm
Partner
Antitrust and Consumer Protection

Robert Quackenboss
Partner
Labor and Employment

Rachel Saltzman
Partner
Environmental



Joseph Anthony Turzi
Partner
Labor and Employment

Mark R. Vowell
Partner
Real Estate

Holly A. Brady
Counsel
Data, Cyber, and Privacy

Cecilia Kim
Associate
Data, Cyber, and Privacy

Sadie Mapstone
Associate
Administrative Law

Alex D. Pappas
Associate
Insurance Coverage Litigation

Hak Stepanyan
Associate
Complex Commercial Litigation

Mary Stoney
Associate
Labor and Employment

HUNTON