Shaw
Insurance Services
530-365-2576 | www.shawinsuranceservices.com
REPORT
JUNE 2026
VOLUME 18 | ISSUE 6

Commercial Liability

# Insurers Start Excluding AI Risk in Some Policies

INSURERS ARE rapidly moving to exclude artificial intelligence-related claims from standard business insurance policies, creating potential coverage gaps for businesses that rely on AI tools for marketing, customer service, product development or daily operations.

The changes come after the Insurance Services Office, the industry's clearinghouse for policy language, introduced three new artificial intelligence exclusions for commercial general liability policies that insurers are beginning to add to coverage forms.

Roughly 86% of all U.S. property/casualty insurance policies contain some form of ISO language, meaning these exclusions could soon become widespread and leave coverage gaps for many employers when their CGL policies come up for renewal. Insurers are also starting to add similar language to other policies with a liability component.

## New coverage gap

The three new ISO endorsements include:
**CG 40 47** – The broadest form, excluding coverage for bodily injury, property damage or personal/advertising injury arising out of generative AI.
**CG 40 48** – A narrower endorsement excluding only personal and advertising injury claims tied to AI.
**CG 35 08** – An exclusion applying to products and completed operations liability coverage.

These endorsements could affect how coverage applies to certain AI-related claims, depending on policy language and endorsements..

A big concern involves Coverage B of the CGL policy, which covers claims such as defamation, invasion of privacy and misappropriation of advertising ideas among others. Under the new exclusions, those claims may no longer be covered if they arise from AI-generated text, images, audio, video or code.

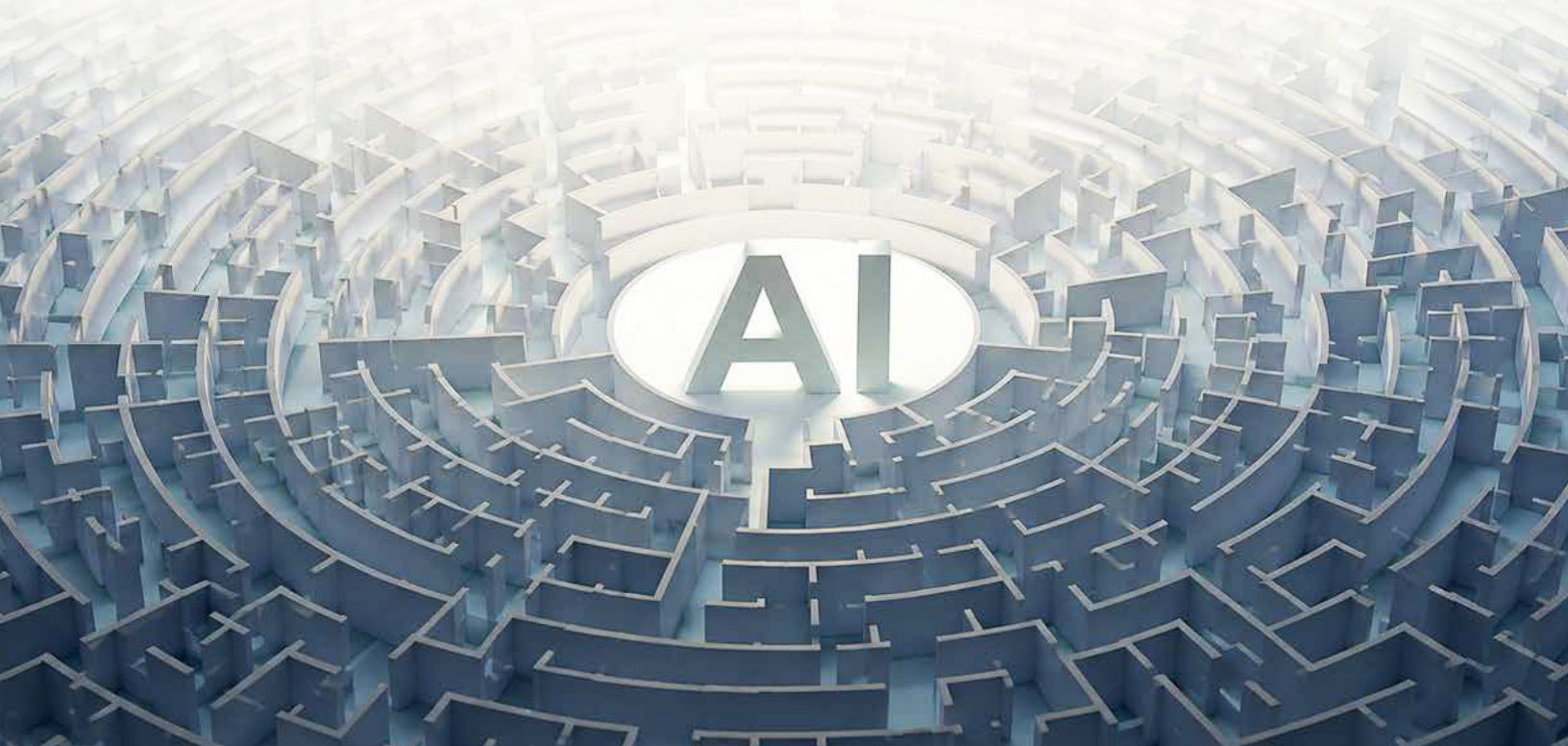
Even firms using third-party AI tools, rather than developing their own systems, may still trigger the exclusions. In some cases, incidental use of AI may be enough.

## The most vulnerable

The businesses likely to feel the greatest impact include:

- Marketing and advertising firms using AI-generated campaigns,
- Technology companies embedding AI into products or software,
- Manufacturers relying on AI-assisted product design,
- Professional service firms using AI to draft documents or communications, and
- Firms using AI tools in hiring decisions.

*See 'Exclusions' on page 2*



# Work Violence Prevention Training Deadline July 1

CALIFORNIA EMPLOYERS are fast approaching another important compliance deadline under the state's workplace violence prevention law.

By July 1, employers with 10 or more employees must provide annual workplace violence prevention training to staff and review their workplace violence prevention plan. The requirement stems from Senate Bill 553, which took effect July 1, 2024.

Cal/OSHA has been actively enforcing the law during workplace safety inspections, making it important for employers to ensure their plans, training and record-keeping procedures are current.

The law requires covered employers to maintain a written workplace violence prevention plan (WVPP) that addresses how the company identifies, evaluates and responds to workplace violence hazards.

## Training requirements

The law requires employers to provide effective training both upon hire and annually thereafter. Training materials must be easy for employees to understand and should address hazards specific to the workplace and employees' job duties.

Required training topics include:

- The employer's workplace violence prevention plan,
- How employees can participate in the plan,
- Definitions and requirements under Labor Code Section 6401.9,
- How to report workplace violence incidents or threats,
- Protections against retaliation for reporting concerns,
- Job-specific workplace violence hazards and preventive measures,
- Emergency response procedures, and
- The purpose of the violent incident log and how employees can access related records.

Employers must also provide employees with an opportunity to ask questions and receive additional information during the training.

## Record-keeping obligations

The law also includes extensive record-retention requirements. Employers must maintain:

- Hazard identification and correction records for at least five years,
- Violent incident logs for at least five years,
- Incident investigation records for at least five years, and
- Training records for at least one year.

## Breakdown of penalties

**Serious violations:** Fines can reach up to $25,000 per violation. This applies if an employer lacks the mandated WVPP or fails to properly train staff.

**Willful or repeated violations:** Fines scale up to a maximum of $158,727. This is triggered when an employer knowingly ignores the law or has a history of continuous non-compliance.

**Failure to keep records:** Improperly maintaining the required violent incident log or ignoring incident reporting procedures can also lead to significant civil citations.

*Continued from page 1*

# *Exclusions Filtering into Other Lines of Insurance*

AI exclusions are also beginning to appear in:

- Directors and officers liability,
- Employment practices liability,
- Fiduciary liability,
- Cyber, and
- Errors and omissions policies.

## What you can do

Organizations that fail to evaluate potential coverage gaps could find themselves uninsured for lawsuits, regulatory investigations or shareholder claims tied to AI use.

Organizations should consider taking the following steps:

- Identify where AI is being used throughout the organization.
- Strengthen internal AI governance and oversight procedures.
- Require human review of AI-generated content and decisions.
- Train employees on acceptable AI use.
- Evaluate contracts with AI vendors and third-party providers.
- Discuss AI exposures with us before renewal.
- Explore specialized protection options.

Growing Legal Threat

# Businesses See Surge in Website Tracking Lawsuits

A GROWING NUMBER of California businesses are finding themselves accused of "wiretapping" website visitors because of common online tracking tools many companies never realized were operating on their websites.

The lawsuits are being filed under the California Invasion of Privacy Act, or CIPA, a 1967 law originally written to combat telephone wiretapping and electronic eavesdropping.

Plaintiffs' attorneys are using the law to target firms whose websites use tools like cookies that collect information about visitors' online activity.

According to legal analysts, demand letters often seek settlements ranging from $15,000 to $40,000. Any business with a website could be targeted, but e-commerce firms are at particular risk.

The litigation wave has created confusion for businesses as courts have issued sharply different rulings on whether the law applies to modern website tracking technologies. Some judges have allowed lawsuits to move forward, while others have dismissed nearly identical claims.

## Lawsuit allegations

In many cases, business owners first learn about the issue when they receive a demand letter alleging their website illegally tracked visitors without proper consent.

Many of the targeted businesses are smaller firms that may not know which tracking technologies are embedded in their websites.

In some cases, tools were added years earlier by website developers, plugins, advertising vendors or software updates. Session replay software, chatbots, advertising pixels, cookies and analytics platforms can collect information about visitors' online activity.

## What lawsuits are alleging

The lawsuits often focus on websites' use of technologies such as:

- **Meta Pixel.** This is a snippet of tracking code that businesses install on their websites to measure, optimize and build audiences for their Facebook and Instagram ad campaigns.
- **Google Analytics.** This code is embedded in the website to track how a visitor interacts with the site.
- **Session replay software.** This tool reconstructs a visitor's journey on a website or app by logging user interactions and playing them back as a video-like simulation.
- **AI-powered chat tools.** These include chatbots, which can monitor how users interact with a site.

Plaintiffs argue these tools function like illegal "pen registers" or "trap and trace" devices under CIPA by intercepting communications between website visitors and the business without first obtaining proper consent.

## Diverging judgments and pushback

In April alone, several courts issued conflicting decisions involving nearly identical allegations over website tracking technologies.

- One federal court allowed claims against CNN to proceed, while another dismissed similar claims against USA Today.
- California state courts also split over lawsuits involving online retailer Wildflower Brands.
- Some judges have ruled that CIPA was intended for telephone surveillance and should not apply to websites.
- Others have concluded plaintiffs alleged enough privacy harm for lawsuits to proceed.

One federal judge described the statute as "a total mess" when applied to modern technology and called on lawmakers to rewrite it. Business groups have pushed lawmakers to clarify the law and curb what critics describe as abusive litigation tactics.

## What you can do

The exposure can be significant because CIPA allows statutory damages of $5,000 per violation. Plaintiffs' attorneys often use the threat of class-action litigation and mounting legal costs to pressure businesses into settling quickly.

Privacy attorneys recommend that businesses:

- Conduct audits of all tracking technologies operating on their websites, particularly third-party tools that may begin collecting information without user consent.
- Review cookie banners, consent mechanisms and privacy policies to ensure they accurately disclose what information is collected and when tracking begins.
- Require visitors to affirmatively opt in before certain tracking tools activate.

Shaw Insurance Services

Human Resources Risk

# EEOC Homes In on DEI, 'Reverse Discrimination'

THE TRUMP administration has stepped up its campaign against corporate diversity, equity and inclusion initiatives and "reverse discrimination," announcing settlements and lawsuits against notable employers such as Nike as well as smaller companies.

The new push is being conducted under President Trump's executive order and Equal Employment Opportunity Commission guidance addressing when DEI-related practices may create compliance concerns under federal law. Since 2025, the Department of Justice and the EEOC have been targeting employers for these violations, alongside typical workplace discrimination claims involving gender, race and religion.

Some recent legal actions include:

- The EEOC is attempting to enforce a subpoena against Nike as part of an investigation into whether the company's workforce representation goals discriminated against white employees and applicants. The agency pointed to company statements about building a "representative" workforce and internal diversity targets.
- The agency sued Coca-Cola Beverages Northeast, alleging the company violated Title VII by holding a women-only networking event that excluded male employees while paying participating women to attend.
- The Justice Department recently settled with PayPal over a pandemic-era investment initiative focused on minority-owned businesses. Federal officials said the case reflects the administration's broader effort to eliminate what it considers unlawful DEI programs.

At the same time, employers should not assume that scaling back DEI efforts eliminates legal exposure. The EEOC continues to pursue traditional discrimination claims involving harassment, retaliation and hiring bias.

## Proceed with caution

Employers that overreact by dismantling compliance programs may create new problems.

Eliminating anti-harassment training, suspending pay equity reviews or abandoning workplace complaint procedures can increase the risk of discrimination claims and weaken defenses if litigation occurs.

Instead, legal experts recommend that employers carefully review workplace policies and programs to ensure hiring, promotions, compensation and development opportunities remain merit-based and job-related.

Key steps employers may want to consider include:

- Reviewing employee handbooks and anti-discrimination policies.
- Auditing hiring and promotion practices for neutral, job-related criteria.
- Ensuring mentorship and leadership programs are open to all employees.
- Continuing anti-harassment and anti-discrimination training.
- Conducting pay equity reviews under attorney-client privilege.
- Carefully evaluating DEI language used in recruiting materials and internal communications.
- Documenting employment decisions thoroughly.
- Avoiding demographic quotas or preferences tied to protected characteristics.

Another growing concern is reverse discrimination lawsuits by white employees, which has become more common, particularly after a recent Supreme Court ruling made it easier for majority-group plaintiffs to bring discrimination claims.

## Review your coverage

With employment litigation risks rising from multiple directions, employers should also review their employment practices liability coverage.

EPLI policies can help cover legal defense costs, settlements and judgments arising from discrimination, harassment and wrongful termination claims.

As enforcement activity intensifies, maintaining strong EPLI coverage may become increasingly important for businesses of all sizes.

If you have any questions regarding any of these articles or have a coverage question, please contact your broker at:

2275 North Street Anderson, CA 96007
Phone: 530.365.2576
www.shawinsuranceservices.com