Los Angeles Business Journal
CORPORATE COUNSEL AWARDS 2024

Corporate Counsel's 2025 Guide: Key Deadlines and Legal Trends to Watch

As legal risks continue to evolve, in-house counsel are tasked with navigating complex regulatory and compliance challenges. This article contains a collection of insights from Greenberg Glusker thought leaders that explores the Corporate Transparency Act deadline, data security threats from collaboration tools, political expression in the workplace during election season, and trends in data privacy litigation.

CORPORATE TRANSPARENCY ACT: REPORTING DEADLINE APPROACHING

By Elias Kawas

The Corporate Transparency Act (CTA) imposes far-reaching new reporting obligations on many US businesses, and the penalties for non-compliance are substantial. Exemptions include large operating companies, government entities, tax-exempt organizations and publicly traded companies. Non-compliance can lead to significant penalties, including fines up to $500 per day for civil violations and up to $10,000 and/or imprisonment for up to two years for criminal violations. With only a few months left before the **January 1, 2025** deadline to file your initial beneficial ownership reports for existing entities, we urge you to act now to comply with the new regulations.

WHY COLLABORATION TOOLS POSE A GROWING DATA SECURITY THREAT

By Peter Jackson

In 2025, reliance on external tools cannot come at the expense of security. By addressing these risks head-on, business owners can reduce their exposure to legal, financial and reputational damage.

AI-powered tools that summarize meetings, generate transcripts, or allow screen-sharing add to this risk. These records, stored on external servers, create a digital trail that businesses may not anticipate. For instance, sales teams using Loom or Slack for internal communications could be exposing proprietary business strategies and sensitive client information. During litigation, these records may surface as part of discovery, expanding the scope of what courts can access. What seems like a harmless collaboration now becomes a legal vulnerability, putting your most valuable data at risk.

Worse, workplace policies can't enforce data security when employees use personal devices or accounts outside of company oversight. Cloud-based SaaS services retain vast amounts of information, including business plans discussed in meetings, and companies often lack visibility into these storage practices.

Tools like digital whiteboards, used for brainstorming new products or services, could become targets for external information requests. Companies relying on cloud storage must contend with third-party vendors who might store or even share this data without clear safeguards.

Recent reports show a growing number of legal challenges stemming from this issue. Over 60% of global general counsel have already encountered problems caused by collaboration platforms, chat apps, or other cloud-based systems. As more businesses adopt these tools in 2025, the problem will only intensify. Regulations like GDPR and CCPA demand that businesses implement strict security measures, but many companies overlook these requirements, especially when dealing with third-party vendors.

ELECTION SEASON AT WORK: BALANCING FREE EXPRESSION AND WORKPLACE HARMONY

By Karina B. Sterman

The upcoming presidential election is not only primed to cause friction at family dinner, but also in the workplace. In anticipation of such mounting tensions, employers must proactively evaluate and establish policies about employee displays of political slogans, attire and rhetoric in the workplace. Legally, as long as restrictions on political expression do not violate anti-discrimination or harassment laws, they may be permitted. Private-sector employees generally lack First Amendment protections in the workplace. However, even if legally permitted, many employers celebrate and promote diversity in the workplace and are reticent in encroaching on political views. While employers may be inclined to respect and even encourage multiple political perspectives as part of workplace conversation, they are well-counseled to counterbalance such latitude by minimizing the inflammatory nature of fixed images and triggering slogans that have a compounding effect by virtue of their fixed omnipresence. In other words, one can walk away from or brush off a conversation one disagrees with, but it's harder to avoid a coworker sitting next to you with a desk full of mocking cartoons, bobble heads or a shirt with a slogan.

Employers should set the tone and manage expectations as to what is appropriate in the workplace, much like dress codes and other unifying workplace policies meant to minimize offensive behavior and disruption. Setting clear boundaries with simple guidelines such as prohibiting political candidate names, party logos and campaign slogans are a good place to start. These restrictions can help reduce the emotional intensity that often accompanies political expression in the workplace. By establishing and communicating these policies consistently, employers can help ensure a more civil and focused work environment, where potential conflicts or distractions related to political paraphernalia are minimized. This is at the heart of maintaining a productive and respectful environment.

DATA PRIVACY LITIGATION CONTINUES TO SURGE

By Ira Steinberg

The surge in data privacy litigation aimed at common e-commerce analytics tools continues to expand. Plaintiffs have gone beyond anti-wiretapping provisions of laws such as the Federal Wiretap Act and California Invasion of Privacy Act, to assert claims under the Video Privacy Protection Act. The Second Circuit recently allowed a case to go forward alleging that the NBA's use of analytics tools on its website violated the VPPA. This decision, though counter-balanced by more business-friendly interpretations of the VPPA in other jurisdictions, has created significant concern regarding the litigation exposure of businesses with websites featuring video content. On the other hand, the wave of website ADA litigation appears to be receding slightly as jurisdictions that had previously been hospitable to such claims are treating them far more skeptically.

Consumer facing businesses should carefully review their dispute resolution policies in light of the upsurge in data privacy claims. Businesses should be particularly careful when mixing mandatory arbitration with class-action prohibitions. Some plaintiffs firms now collect hundreds or thousands of claimants and file individual claims for all of them that cannot be consolidated as a class action because of the class action waiver. Because arbitration services usually charge the defending business an administrative fee on a per-claimant basis, these mass arbitrations can have a significant cost of defense even where the claims are weak (which they often are). Careful and strategic drafting of dispute resolution provisions is critical.

Learn more at GreenbergGlusker.com.