A Signal Year in Business Law

2025's legal currents for office technology dealers

by: Greg Goldberg, BTA General Counsel

It was a legally consequential year for the business of keeping American offices running. Lawmakers, regulators and courts made clear that the work of supporting back-office operations, technology stacks and image creation is a form of high-risk infrastructure.

The most sweeping developments came from data privacy legislation, which continued its advancement across the United States. With no federal privacy law in sight, more than a dozen states enacted or significantly updated comprehensive privacy statutes. For MSPs, the influx of rules means grappling with a patchwork of consumer data rights: access, deletion, portability and, increasingly, transparency around automated decision-making.

For enterprises that now offer predominantly cloud-based and SaaS solutions, this regulatory quilt may pose practical compliance challenges. For example, an MFP may be sold in Ohio, managed from Texas, store data in Virginia and sync logs to a backup in Oregon. Such distributed arrangements now come with more stringent obligations: explicit disclosures, purpose limitations and retention rules that demand sharper contract language, and clearer operational boundaries. Amid this fragmentation, one unifying trend did emerge: service providers are undeniably on the hook. Many states expanded the definitions of "data processors" and "service providers," imposing direct responsibilities where previously only the data owner was accountable. In many states, the days when an MSP could leverage a customer's privacy policy for legal protection are over.

On the cybersecurity side, Washington, D.C., and several state governments sharpened expectations around incident reporting. Federal agencies updated guidance under the Cybersecurity and Infrastructure Security Agency's (CISA's) cyberincident reporting rules, encouraging industry-specific reporting channels and threatening enforcement for firms that fail to disclose breaches.

And while few small MSPs think of themselves as "critical infrastructure," the rising number of ransomware attacks on schools, hospitals and local governments has pushed regulators to reconsider what counts.

Perhaps the most chilling development for the industry did not come from regulators, but from the courts. The expansion of negligence and breach-of-contract liability for service failures became a defining theme of 2025. High-profile litigation — such as the case between Delta Airlines and cybersecurity firm CrowdStrike — sent a tremor through the MSP community. The underlying message was simple: If a provider's tools, configurations or updates cause client downtime or data loss, courts are increasingly willing to treat those failures as actionable misconduct.

For many years, MSPs have relied on limitation-of-liability clauses as an all-purpose cap on potential damages. In 2025, judges signaled that such protections are not invincible. Terms must be conspicuous, reasonable and — crucially — aligned with the actual services performed.

Meanwhile, those relying more heavily on equipment sales received a pleasant surprise: tax legislation expanded Section 179 of the Internal Revenue Code regarding expensing and bonus depreciation allowances for qualifying property. The changes effectively reduced the after-tax cost of capital equipment — from large enterprise printers to server racks — giving customers an incentive to modernize infrastructure they often neglect in favor of client-facing gear.

Finally, a quieter but no less consequential trend emerged: broader expectations of transparency in automated systems, including artificial intelligence (AI)-driven monitoring tools. With the Federal Trade Commission sharpening its scrutiny of algorithmic claims and the White House issuing revised AI governance guidance, MSPs found themselves having to explain — sometimes to clients, sometimes to regulators — just how their AI tools arrive at decisions.

Taken together, the year's developments signal a new legal paradigm for the office technology and managed IT worlds. Industries that once lived largely in the shadows — fixing printers, patching servers and quietly working in the background — now sit at the center of regulatory and legal attention. The upshot is simple: 2025 marked the moment when the rest of the country realized that the people who install endpoints, secure networks and keep documents moving are, in effect, stewards of critical infrastructure assets. For business owners, the mandate is clear: Understand your data flows. Update your contracts. Treat cybersecurity not as a service line, but as a legal obligation. And above all, prepare — because the regulatory tide is rising. ■

Greg Goldberg, partner at Barta | Goldberg, is general counsel for the Business Technology Association. He can be reached at ggoldberg@bartagoldberg.com or (847) 922-0945.