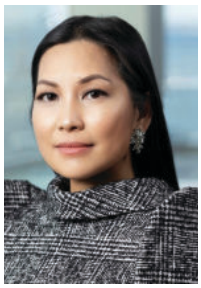
ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
FEBRUARY 28, 2024

Does your website invite litigation? Here's how to avoid risks.

■ CAURIE PUTNAM

Technology-related litigation in the United States and Canada grew in 2023 and is expected to grow in 2024 as well, according to Norton Rose Fulbright's Annual Litigation Trends Survey.

We checked in with leaders in the technology litigation space in Western New York to find out what technology-related litigation trends and risks they're seeing and how companies can stay ahead of them.


Mercado Clark

At Phillips Lytle, litigation in the tech space has been very busy, according to Anna Mercado Clark, a partner and leader of the firm's Data Privacy and Cybersecurity and e-Discovery Practice teams and co-leader of the firm's Cryptocurrency and Blockchain team.

In addition to the usual breach of contract litigation involving companies and third-party service providers, Clark says there's been a rise in Americans with Disabilities Act website compliance litigation and litigation based on website tracking technologies over the past few years.

She is also seeing a rise nationally in litigation related to artificial intelligence, as well as litigation pertaining to the protection of children's data.

"We have kind of a renewed interest and a lot of legislative activity on that front in particular in California," said Clark, who is also an adjunct professor of law at Fordham University School of Law. "There is an increased attention on youth privacy and growing issues with minors use of social media. There's also an effort on the federal level to update the Children's Online Privacy Protection Act (COPPA), so we expect litigation to arise out of that."

When it comes to companies protecting themselves from technology related litigation, one recommendation Clark has is to consider using enterprise-specific solutions as opposed to publicly available solutions, so they have more control over their data.


Greene

Paul Greene is partner and chair of the Privacy and Data Security and Artificial Intelligence and New Technologies Practice Groups at Harter Secrest & Emery, which represents companies of all sizes; all of which, if they have a website, can be at risk for potential litigation.

"The website is certainly the front door and publicly facing surface that an organization has, and many of the common tracking tools and common technologies used in websites have been the focus of a lot of the litigation risk currently out there," Greene said.

He says the litigation risk from websites often originates from companies seeing their website as a communication tool first and not being aware of the privacy and data protection risks that can arise from things like Meta pixel, an analytics tool that tracks website visitor activity.

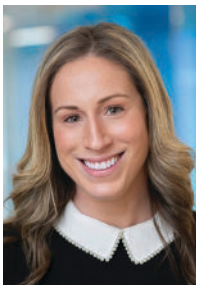
"It's very useful but it also can end up sending personal information like the pages that you view and your IP address to Meta,"

Greene said. "So that desire to create maximum visibility into the user experience and the way that consumers use your website creates a data flow by which personal data can move to a third party."

That movement of personal data to Meta, Google Analytics or similar platforms has led to a slew of litigation globally alleging things like wiretapping and invasion of privacy under various state laws, said Greene, who notes the pace of those litigations is increasing.

Greene says the most important action companies can take to assess and mitigate risk when it comes to website tracking is to engage in a comprehensive review of what their website does, how it collects information, who it shares that information with and how long that information is kept.

At Nixon Peabody, Jenny Holmes, a partner and deputy leader of the Cybersecurity & Privacy team, sees increasingly more companies dealing with litigation stemming from a myriad of data breaches and data privacy issues that are often accidental in the sense businesses don't fully understand the technology they're using.


Holmes

"Understanding the data you're collecting and what you're doing with it and why is so important," said Holmes, who notes this begins by developing programs that allow companies to use the data and be transparent with consumers about that use. "Transparency when it comes to collection of data is really important and best practice."

She recommends not moving too quickly when it comes to adopting new technologies, such as artificial intelligence tools, and taking the time to talk to legal counsel before implementing new technologies to ensure they don't put the company or consumers at risk.

She recommends data mapping for tools that are already in use, so a company can better understand the data they're collecting, what they're doing with it, and why.


Szczepanski

Kevin Szczepanski is a partner and co-chair of the Data Security & Technology Practice Area at Barclay Damon, where he concentrates his practice primarily on insurance-coverage litigation and cyber risks. He is also the host of Barclay Damon Live: Cyber Sip, the firm's biweekly cybersecurity podcast.

Szczepanski explains that when cybersecurity first came into society's consciousness years ago the focus was chiefly on security and what businesses needed to do to protect their systems from threats like denial of service or ransomware attacks, but that is changing.

"What we're seeing in the last few years is what I call the paradigm shift from security to privacy," Szczepanski said. "We're still concerned about security, but we're increasingly concerned about the effect of a breach or a cyber-attack on the data."

Szczepanski says the concerns of everyday people about what a business is doing with their data and how they are protecting it are playing a significant role in increasing the frequency and cost of litigation.

Three steps Szczepanski says companies can take to decrease their risk of litigation stemming from technology are risk management, vendor management, and cyber insurance.

"You want to purchase cyber insurance," Szczepanski said. "It's a great tool. Not only can it cover the costs that you incur if you suffer a data breach or a ransomware attack, but it will pay for your defense and any judgment or settlement against you if you find yourself in a data breach class action or other cyber litigation."

For any company that doesn't have cyber insurance, Szczepanski recommends finding an insurance broker who specializes in cyber insurance to have a candid discussion about the condition of your network, the data that you have, and the costs – which, he notes, have leveled off or even dipped in some cases recently.