Litigation Trends and Best Practices for Mitigating Website Legal Risk

Dalton Cline and Ameena Khan Per

In addition to plaintiffs' litigation, the first eight months of 2025 saw regulators enforcing a patchwork of state data protection and privacy laws, with enforcement actions penalties ranging from $85,000 to $1.2 million in addition to specific injunctive relief.

Introduction

In today's marketplace, your website is an integral part of your organization's business processes—it enables online transactions, hosts thought leadership materials demonstrating your expertise and visually communicates your brand. However, the personal data you collect through your website is also a significant source of legal risk.

In recent years, website operators across industries have been blindsided by a surge of thousands of lawsuits claiming that common digital practices—like offering chatbots, tracking website analytics, using embedded video, utilizing session replay tools or even deploying common automatic information collection technologies like cookies and pixels—violate state and federal law. More than one thousand suits have been filed in California alone in the past two years, and plaintiffs in these cases allege potentially millions of dollars' worth of damages. It appears that no business is safe from these suits; from consumer retail to industrial manufacturing, from entertainment to energy, businesses in every industry must be prepared to respond to these lawsuits.

In addition to plaintiffs' litigation, the first eight months of 2025 saw regulators enforcing a patchwork of state data protection and privacy laws, with enforcement actions penalties ranging from $85,000 to $1.2 million in addition to specific injunctive relief. Reviewing litigation trends and best practices to avoid liability is critical for all organizations.

Litigation Trends

High-dollar litigation can be broken down into three chief categories: (1) state wiretap claims; (2) video privacy protection act violations; and (3) e-commerce transactions.

Wiretap

State wiretap claims are far and away the most common claim brought by plaintiffs against website owners. These suits claim that defendant organizations either (1) engaged in a "wiretap" (or assisted a third-party in wiretapping) by capturing the "content" of customer communications with the defendant's website, or (2) utilized technologies that qualify as a "pen register" and/or "trap and trace device" that captured non-content routing or addressing information about plaintiff's interaction with the defendant's website.

Wiretapping claims are commonly brought under state wiretapping statutes like the California Invasion of Privacy Act, Cal. Pen. Code §631(a) (CIPA), and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Stat. and Cons. Stat. Ann. § 5701 et seq. (WESCA), but may also be brought under various provisions of the federal Electronic Communications Privacy Act.

Violations under these laws can carry astronomical damages, which plaintiffs may use to pressure settlement. For example, violations of WESCA can lead to $1,000 in damages per class member (18 Pa. Stat. and Cons. Stat. § 5725(a)(1)), while violations of CIPA can be worth up to $5,000 per class member (Cal. Pen. Code § 637.2(a)(1)).

Video Privacy Protection Act

The Video Privacy Protection Act (Pub. L. No. 100-618, 102 Stat 3195 (1988), codified at 18 U.S.C. § 2710)) (VPPA), prohibits a "video tape service provider" from (1) knowingly disclosing to any person (2) "personally identifiable information" concerning any "consumer" of such provider (3) unless an exception applies (such as

(Continued on next page)

(Continued from previous page)

a disclosure to the consumer, or with their express written consent).

Although originally passed in response to Supreme Court nominee Robert Bork's video tape rental history being disclosed to a reporter, the VPPA has been brought into 21st century by plaintiffs alleging that defendants who facilitate the online delivery of digital video content qualify as "video tape service providers." There are numerous circuit splits on nearly every element of a VPPA: What kind of businesses qualify as "video tape service providers"? Is information collected by automatic information collection technologies "personally identifiable information"? What does the relationship between a plaintiff and defendant need to be for the plaintiff to be a "consumer"?

Notably, the VPPA provides a private right of action for violations and minimum statutory damages of $2,500 per violation.

e-Commerce Transactions

Multiple state laws prohibit the collection of non-essential personal data as a condition for accepting payment cards (see, e.g., the Song-Beverly Credit Card Act (Cal. Civ. Code § 1747.08), Massachusetts Consumer Privacy in Commercial Transactions Act (Mass. Gen. Laws ch. 93, § 105), Del. Code. Tit. 11, § 914(b)(1)(b), Md. Code, Com. Law § 13-317(a), N.J. Stat. 56:11-17, 6 R.I. Gen. Laws § 6-13-16(a), Kan. Stat. § 50-669a). Plaintiffs in California are entitled to statutory damages of at least $1,000.

Best Practices to Avoid Liability

Identify automatic information collection technologies used by your website.

Plaintiffs in wiretap cases allege that defendant's automatic information collection technologies, like cookies and pixels, are "pen registers" or "trap and trace" devices because they capture the "dialing, routing, addressing, or signaling information" of a plaintiff's interactions with the defendant's website. For example, these technologies capture the HTTP header information of the GET and POST requests made between the plaintiff's browser and the defendant's website server. These cases disproportionately, although not exclusively, focus on the use of the Meta Pixel and TikTok Pixel.

Many organizations may not even be aware that their website uses these automatic information collection technologies. This is common when the development and maintenance of the website has been outsourced to a third party. Organizations who choose to use automatic information collection technologies like non-essential cookies, pixels and session replay software should evaluate their use cases and determine if the value of such use is commensurate with the potential litigation risk.

Ensure metadata concerning viewed videos does not include the video title.

Although the VPPA does contain a "consent" defense, the requirement is too difficult to meet to be practical in most cases. The VPPA requires that the consent be written and obtained "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" (18 U.S.C. § 2710(b)(2)(B)(i)), meaning that organizations may rely on express or implied consent to a privacy notice.

Instead, organizations should seek to fall outside one or more statutory definitions. For example, an effective risk mitigation technique to avoid liability under the VPPA is to review the metadata that is being transferred and ensure that the website does not transmit the title of the video to any third party. The VPPA defines "personally identifiable information" as "information which *identifies a person as having requested or obtained specific video materials* or services from a video tape service provider" (18 U.S.C.A. § 2710(a)(3)). By removing video title, from metadata collected by third-party integrations, such as analytics tools, advertising pixels, content delivery networks and customer data platforms, the information would not be considered "personally identifiable information."

Distinguish between essential and incidental personal data collected in e-commerce transactions.

Litigation related to e-commerce transactions, particularly under the Song-Beverly Credit Card Act, focuses on non-essential personal data collected during check-out that plaintiffs allege was a "condition" of the transaction.

While collection of a consumer's payment card information, billing address and shipping address may be required to complete the transaction, information collected that is incidental to the transaction, such as phone number, should be clearly indicated as optional.

Review user interface elements to ensure enforceability of Terms of Use.

Website Terms of Use are often used to lower the risk of costly litigation through mandatory arbitration, class action waiver, choice of venue, choice of law and limitation of liability clauses. However, many organizations have been surprised to find that these carefully considered provisions were not binding on plaintiffs. A defendant seeking to enforce the provisions of a website's Terms of Use must demonstrate the formation of a valid contract. Therefore, state law principles of contract regarding contract formation govern, which include, in relevant part, consent to the terms of the contract.

Many organizations use "advisements," which are short statements alerting users to the existence of a Privacy Notice and Terms of Use, to put users on notice to the existence of these terms and argue that the user consented to the terms. However, courts have closely scrutinized these advisements and articulated ever-higher standards for enforceability. The following are best practices identified from case law:

- **Uncluttered layout.** Present only essential elements—core fields and the advisement—and remove nonessential content.
- **Advisement visible in context.** Ensure the advisement appears on the same screen as the action button without scrolling.
- **Equivalent prominence.** Match the advisement's font, color and size to surrounding text of comparable importance.
- **Reasonable conspicuousness.** Place the advisement in a position that interrupts the natural flow—ideally immediately above the action button.
- **Distinct hyperlinks.** Make links to Terms of Use and Privacy Notice clearly distinguishable—use all caps, underlines, bold and a contrasting color.
- **Textual concordance.** Align action button text with the advisement language (e.g., "Continue" where the notice says "By clicking 'Continue' you agree..."; "I agree" where "I agree" is referenced).
- **Explicit arbitration reference.** State that agreement includes acceptance of mandatory arbitration.
- **Explicit jury waiver.** State that agreement includes a waiver of the right to a jury trial.
- **Affirmative assent.** Require *active acknowledgment* (e.g., clickwrap or checkbox). Clickwrap is more defensible than passive browsewrap.

Conclusion

Website data collection practices now carry outsized litigation and enforcement risk, which will likely only increase as time goes on. Engaging a qualified attorney who understands current litigation trends to evaluate your website, advise on legal risk and provide court-tested best practices is a great way to not only reduce your legal exposure, but also safeguard your brand, budget and customer trust.

Dalton Cline is a member of the Dentons Global Data Privacy and Cybersecurity Group based in Louisville. As a Certified Information Privacy Professional (CIPP/US, CIPM, CIPT), he routinely advises businesses of all sizes in a variety of industries and sectors regarding compliance with domestic and international data privacy and cybersecurity laws and regulations, litigation risk and best practices. Prior to joining Dentons, Dalton was a privacy analyst at a large public university.

Ameena Khan Per is an Associate of McBrayer PLLC, practicing in the firm's Louisville office. Her practice primarily focuses on data privacy and security, intellectual property and trademarks. Her primary expertise is in data privacy and cybersecurity law, where she advises clients on a variety of privacy matters, including compliance with privacy and data security laws and drafting privacy policies. Ameena has hands-on experience with technology-related issues, which brings a unique and vital perspective in successfully negotiating agreements involving personal data and developing creative governance solutions that blend well with existing business practices. ■

Cline

Per