Collecting & Sharing Data

Beware of lawsuits targeting business websites

by: Greg Goldberg, BTA General Counsel

If your company relies on its website to drive customer engagement, you should take a close look at the tools running in the background. In California (and increasingly beyond), businesses are facing a surge of lawsuits alleging their websites secretly collect personal information from visitors and share it without consent.

Hundreds of lawsuits have already been filed in California, and while the legal theories are novel, some courts are allowing these cases to proceed beyond initial pleadings to the discovery phase. For BTA members, this deserves serious attention. Even if a member is not located in California, this trend is likely to spread to other states with similar privacy statutes.

California's "Trap and Trace" Law

At the center of the California lawsuits is a provision of the California Invasion of Privacy Act (CIPA). Originally, the law was designed to limit law enforcement's ability to use "trap and trace" devices that capture the phone numbers of incoming calls. CIPA forbids installing or using any "device or process" that captures electronic information that could identify the source of a communication. While the statute made sense in the telephone age, opportunistic plaintiffs' lawyers are now applying it to website tracking tools like cookies, pixels and web beacons, which may be running in the background of a website.

The lawsuits claim these technologies gather data such as IP addresses and device details, and share it with third parties for marketing purposes. The plaintiffs argue this practice is the digital equivalent of an unlawful "trap and trace."

The statute carries steep penalties: the greater of $5,000 per violation or triple the actual damages, plus attorneys' fees. Because class action lawyers are experts at aggregating individual claims, a company's exposure can add up quickly.

Are The Claims Legitimate?

Most legal experts agree CIPA was never meant to apply to website analytics. The law's history makes clear it was designed for law enforcement contexts, not marketing or customer engagement. Some courts have recognized this mismatch. For example, earlier this year, a Los Angeles County judge dismissed a trap and trace claim, finding that website visitors do not have a legally protected privacy interest in their IP addresses. He warned that a broad interpretation of CIPA could disrupt online commerce. Other courts have declined to dismiss CIPA lawsuits at an early stage, leaving businesses facing expensive litigation. The lack of clarity — and the sheer cost of defense — means companies need to be proactive.

What BTA Members Can Do Now

Most BTA members' websites are more than digital brochures. They are tools for generating leads, processing service calls and supporting e-commerce transactions. That means most members are likely utilizing some form of analytics tools. Here are steps to minimize risk:

(1) Audit your website tools — Work with your IT team or provider to identify what tracking technologies are in place. Know exactly what data they collect and whether any of it is shared with third parties.

(2) Review privacy disclosures — Make sure your privacy policy is up to date and written in plain language. If your site uses cookies, pixels or beacons, disclose that clearly. Visitors should understand what information is collected and how it is used.

(3) Consider opt-in consent — In high-risk jurisdictions like California, asking website visitors to provide express consent — through a pop-up or banner — may insulate members from claims.

(4) Limit unnecessary sharing — If your site automatically sends visitor information to third parties, ask whether it is truly necessary. The less data you share, the less exposure you have.

The Big Picture

This moment is both a warning and an opportunity for BTA members. Privacy lawsuits like the ones highlighted here represent a broader trend: plaintiffs' attorneys are investing huge sums to convince courts that commonly used website tools violate existing technology laws. Although individual penalties may be modest, class action exposure may be considerable. Members who take steps now — auditing websites, tightening disclosures and capturing consent — can reduce their risk and demonstrate to customers that they take data privacy seriously. In today's climate, that is not just smart risk management — it is good business. ■

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.