Privacy Claims

Act now & create a compliance program

by: Greg Goldberg, BTA General Counsel

Last October, this column addressed a growing wave of privacy claims in California aimed at businesses whose websites use common analytics, advertising and customer-engagement tools. The issue is worth revisiting now because just last month I heard from five different Business Technology Association (BTA) members across the country who all received similar demand letters from the same California plaintiff. What started as a local problem in California appears to be spreading.

The letters generally accuse businesses of operating websites that violate California's pen register and trap-and-trace laws. They generally include screenshots of the recipients' websites and identify third-party technologies allegedly embedded in the sites. The claims can sound technical and unfamiliar, but the underlying concern is straightforward: whether a website is collecting or transmitting information about a visitor without adequate notice or consent.

For BTA members, this is not an abstract problem. Websites are often the front doors to their businesses. They include contact forms, service request portals, live chat functions, equipment quote tools, e-commerce stores, downloadable brochures, remote support links, etc. Each feature may involve code supplied by a third party, and each piece of code may collect information beyond what the business itself sees on the screen.

The allegations commonly focus on session replay software, website analytics tools, advertising pixels, chat widgets and other tracking technologies. Session replay tools can record or reconstruct a visitor's interaction with a webpage, including mouse movements, clicks, scrolling behavior, time spent on a page and, in some instances, information entered into forms. Analytics tools may capture page views, device information, browser details, referral sources, IP addresses and user behavior. Advertising pixels may transmit data to third-party platforms when a visitor views a page, submits a form or takes another action.

These tools are widely used for legitimate business purposes. Businesses may use them to determine how visitors navigate their websites, where they encounter problems and whether visitors can find what they are looking for. Potential legal issues arise when a third party receives information that a visitor reasonably believes is being provided only to the website operator.

California's pen register and trap-and-trace statute was enacted long before the modern commercial internet, but plaintiffs have argued that certain website-tracking tools function like digital versions of devices that capture dialing, routing, addressing or signaling information. Not all courts agree that the statutes apply to website functions, but businesses should take this opportunity to review how their sites work.

The first step is to identify what is actually running on the company's website. Many businesses know they use Google Analytics or a chat tool, but do not know every script, tag, cookie, pixel or software development kit that loads when a visitor opens a page. A technical audit should identify each tool, its vendor, the information it receives, the pages on which it operates and whether it is active before a visitor gives consent.

The second step is to determine whether sensitive or form-entry information is being collected or transmitted. A session replay tool should not capture data entered into contact forms, service tickets, financing inquiries, employee applications, customer login pages or other fields that could contain personal, financial, business or credential information.

Third, businesses should revisit their privacy notices and cookie-consent practices. A privacy policy should accurately describe the categories of information collected, the purposes for collection, the types of third parties receiving information and the consumer rights that may apply. A cookie banner should do more than announce that cookies exist. Where applicable, it should give visitors an opportunity to opt in before analytics, advertising, session replay and similar tracking technologies activate.

For California businesses, the California Consumer Privacy Act and related regulations should be part of the analysis. Businesses outside California should not assume they are beyond reach. A company with no California office, employees or customers may have stronger jurisdictional arguments in a particular dispute. But an out-of-state business whose website actively markets to California visitors, collects information from them or does business in the state may still face California-based claims.

More importantly, privacy expectations and state privacy laws are expanding nationally. A sound compliance program is often less expensive than a state-by-state patchwork created after a demand letter arrives. Act now and do not ignore those demand letters. ■

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.