Now & Next
Cybersecurity & Privacy Alert

February 26, 2024

CIPA class action litigation: The new, expensive risk of data analytics software

By **Stacy M. Boven**

Stacy M. Boven

Hundreds of CIPA class actions have been filed against businesses using third-party data analytics software to improve the user experience on their websites, costing companies big bucks in the process. Here are strategies to protect your business.

What's the impact?

- Under threat of a multimillion-dollar class action suit for violation of the California Invasion of Privacy Act (CIPA), many businesses are entering into prelawsuit settlements that may not protect against future litigation.
- Courts are split on how to interpret CIPA claims, and this uncertainty creates an opportunity for class action claimants to pull companies into protracted, expensive litigation.
- Businesses should take proactive measures to reduce the likelihood of CIPA litigation and prepare for an efficient defense if CIPA claims arise.

Recently, in California, there has been a deluge of consumer class action suits claiming that the use of chatbots, session replay, tracking pixels, and other data analytics software violates CIPA.

This flood is precipitated by the statutory penalties for CIPA violations that push class action damages claims into the millions.

As a result, many plaintiffs' firms are churning out form demand letters and filing ostensibly identical complaints against companies that refuse to settle. This puts any business that incorporates third-party software in its public website at risk of multimillion-dollar class action litigation.

A new application of CIPA

The California Invasion of Privacy Act (CIPA), California Penal Code Section 631(a) imposes fines and other penalties for four kinds of wiretapping:

- Intentional wiretapping;
- Willfully attempting to learn the contents or meaning of a communication in transit over a wire;
- Attempting to use or communicate information obtained as a result of engaging in either of the previous two activities; and
- Aiding, agreeing with, employing, or conspiring with a third party to engage in any of these prohibited "eavesdropping" activities.

Plaintiffs' firms are now using this statute—which was originally intended to address telephone wires, not website data analytics—to claim that using third-party data management software amounts to aiding wiretapping in violation of the fourth clause of CIPA Section 631(a).

Inconsistent treatment of CIPA claims in California courts

State and district courts are doing their best to apply CIPA's antiquated language to new technology, but the hundreds of recent complaints have created a murky, inconsistent legal landscape. Some courts have rejected CIPA claims, finding that the use of third-party software is more akin to a *legal* tape recorder than an *illegal* third-party eavesdropper. Other courts have held the opposite, at least at the pleading stage. Many cases are moving forward to discovery and forcing businesses to decide between paying to litigate or paying to settle claims that courts may eventually decide are illegitimate.

Until an Appellate Court or the Supreme Court in California issues a clarifying ruling, plaintiffs' firms have a lot of latitude to threaten and leverage massive class action litigation. As a result, any company that has a website should take measures to proactively defend against this threat.

How businesses can protect against CIPA class action claims

While the state of the law remains uncertain, businesses should take the following steps to insulate themselves as much as possible from CIPA class action claims:

STRENGTHEN YOUR DEFENSES

Make sure your website terms of use, cookie policy, and privacy disclosures are accurate, current, and formatted in a manner that isn't just compliant with California and federal law but also designed to provide your company with the strongest protections against CIPA claims. For example, whether a privacy policy is actually protective may depend on where it is located on your website, how it appears to website users, whether it requires affirmative consent, etc. Also, consider incorporating enforceable arbitration clauses, when possible, to limit the time and expense of any future class action claims.

IF YOU RECEIVE A DEMAND LETTER FROM A CONSUMER CLASS ACTION FIRM, ACT FAST TO UNDERSTAND THE EXTENT OF THE THREAT

Correspondence identifying purported CIPA violations will include clues as to the seriousness of the claims. For example, consider the following:

- Does the law firm have a reputation for filing consumer class actions?
- Has this law firm filed similar CIPA lawsuits?
- How big is the purported class?
- Is the purported class identified with any kind of specificity or supportive evidence?
- Are the claims generalized or specific to your company?
- Does the demand letter include an offer for settlement?
- Do the claims fall within the purview of an enforceable arbitration agreement, etc.?

MAKE A SWIFT, BUT STRATEGIC RESPONSE

Once you have determined the extent of the threat, determine whether an early settlement is an option and, if so, whether it is the right choice for your business. The cost/benefit analysis goes beyond the simple calculation of whether it is cheaper to litigate or settle. For example, some companies may wish to quickly and quietly dispose of the matter but should be aware that any private settlement outside of court may not protect them from future claims from other plaintiffs not included in this purported class.

PREPARE FOR THE WORST

If you determine there is a credible threat of litigation, issue a litigation hold to preserve evidence and data, conduct an internal investigation, and communicate internally in a manner

that avoids creating additional, non-privileged evidence. You'll need evidence that can be used to challenge the class certification as well as the CIPA claims, and it's important to gather it in a way that preserves the attorney/client privilege whenever possible.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Stacy M. Boven
415.984.8312
sboven@nixonpeabody.com