



JUNE 20, 2023 • NO. 2

## Protecting Against Invasion of Privacy Chat Box Class Actions

*California has seen a recent surge of both class action and individual claims under the California Invasion of Privacy Act (“CIPA”) in which plaintiffs attack websites using “chat boxes”—live or automated instant messaging features on websites designed to help users communicate for customer service purposes. The claims have evolved, and plaintiffs now allege, in a highly generalized manner, that companies’ use of chat boxes violates web users’ privacy by allowing a third-party chat software provider to wiretap and eavesdrop on the private conversations of users who interact with the company via chat. Given the high volume at which cases have been filed and the potential for statutory damages of \$5,000 per violation, companies should take action now to protect against future litigation.*

### BACKGROUND ON CIPA

CIPA is a 1967 law which prohibits certain parties from wiretapping, eavesdropping, or recording telephone communications of private citizens. While CIPA is a criminal statute, the California Penal Code also creates a civil private right of action for CIPA violations.<sup>1</sup> CIPA Section 631 covers telegraph or telephone wire. Section 632.7 was added much later to CIPA and was specifically adopted to address the intentional recording of cellular **radio** and cordless telephone communications.<sup>2</sup>

Liability under Section 631 may exist in any of four ways. First, liability may be present when a third party taps, or makes an unauthorized connection with, a telegraph or telephone wire. Second, liability may exist where a third party eavesdrops on a conversation without the consent of all parties while the communication is “in transit,” or simultaneously. Third, anyone who “uses, or attempts to use, in any manner, or for any

purpose, or to communicate in any way, any information so obtained,” may be liable. And finally, a party may incur liability under Section 631 for helping another person or entity to commit any of the above violations.<sup>3</sup>

Section 632.7 only covers “a communication transmitted between (1) two cellular radio telephones, (2) a cellular radio telephone and a landline telephone, (3) two cordless telephones, (4) a cordless telephone and a landline telephone, or (5) a cordless telephone and a cellular radio telephone.”<sup>4</sup>

Courts do not require a plaintiff to prove actual damages to recover on a CIPA claim, but the plaintiff still must sustain an injury-in-fact to be entitled to the statutory damages. A violator must pay the greater of \$5,000 per violation or three times the amount of actual damages sustained by the plaintiff. However, even without injury, plaintiffs can still attempt

to seek an injunction to restrict the company's chat box use and the dissemination of their data to third parties.<sup>5</sup>

## THEORIES AND ARGUMENTS

Traditionally, the purpose of CIPA was to prevent non-parties from listening in on confidential communications where the parties had reasonable expectations of privacy, and/or on certain telephone communications which were more susceptible to breach. The case law interpreting CIPA over the past decades is vast; however, it has, for the most part, addressed traditional theories of liability. In 2019, lawsuits brought under CIPA began regarding website functionality and online communications, moving away from email and into website analytics tools and session-replay technology. Then in 2022, an unpublished ruling by the Ninth Circuit concerning the narrow issue of consent to use session replay technology emboldened entrepreneurial plaintiffs to file class actions under CIPA alleging that companies enable third parties to eavesdrop on their communications with website visitors.<sup>6</sup> As one district court recently observed, the decision "opened the floodgates for these cases, an unfortunate unintended consequence" of a narrow ruling.<sup>7</sup> To be sure, that was not the first case to find CIPA applies to Internet communications, but it was the first case on appeal involving a web operator's co-liability.

While California has amended CIPA multiple times, it has yet to amend CIPA to expressly cover Internet communications, nor is there any indication that the Legislature intends to do so. Despite this, class actions have seized on a grey area in the statute and the Ninth Circuit's ruling to challenge the complex and technical workings of web functionality tools.

Yet, plaintiffs in these actions typically argue that chat box features secretly wiretap conversations between web users and a website customer service representative through embedded code that automatically records and transcribes conversations for third-party vendors to simultaneously eavesdrop upon. They allege that this is done without the consent of the plaintiff, and thus constitutes a violation of Section 631 of CIPA.

Though most of these cases are in the early stages, courts have thus far generally rejected these arguments for several reasons by interpreting the plain language of the statute and

finding that third-party service providers do not fit the bill as "wrong actors." Unfortunately, however, the results have not been uniform. For example, one California federal court considered a plaintiff's allegations that an Internet chat box communication taking place via the user's handheld smart phone was a telephonic communication sufficient to survive a motion to dismiss.<sup>8</sup>

Regarding third-party "wrong actors," plaintiffs have since evolved their theories of liability, particularly under Section 631, and have turned to a more traditional aiding and abetting theory, alleging that the websites enable third-party software providers to spy on their assumed private conversations and use the data for various targeted advertising and other purposes for their own gain.

Without any iota of evidence, plaintiffs are now claiming the third-party software is "integrated" with Meta subsidiaries like Facebook and WhatsApp, which allows the sharing of web users' private information obtained from the chat box as data in a unified system.<sup>9</sup> Once this data has been harvested through its subsidiaries and used to identify user interests, Meta then profits by selling the advertising space and directing targeted ads to the web users through its brands like Facebook and WhatsApp. This theory, however, should not withstand a motion to dismiss in part because it lacks specificity and calls for unsupported speculation about integrations between third-party vendors and Meta.<sup>10</sup>

## HOW TO PROTECT AGAINST CIPA CHAT BOX CLAIMS

Companies that use or are considering using customer chat functionality on their websites should be aware of this recent wave of both class action and individual litigation because, even without actual injury, statutory damages can impose significant monetary damages. Companies can face a minimum of \$5,000 per violation, in addition to plaintiffs' attorney's fees and costs. And litigation is expensive, even if the claims are without merit. To protect against potential litigation, companies should be sure to update their privacy policies, terms of use, and disclosures, both on their websites and in their chat box features, to assure that web users have proper consent for the use of chat transcripts and content.

Contact [Ana Tagvoryan](#), [Harrison Brown](#), [Sharon Klein](#), [Alex Nisenbaum](#), [Nicole Bartz Metral](#), or another member of Blank Rome's [Privacy Class Action Defense](#) group to discuss how to update privacy policies and other documents, and to protect against CIPA claims as this issue continues to develop.

**Ana Tagvoryan**  
424.239.3465 | [ana.tagvoryan@blankrome.com](mailto:ana.tagvoryan@blankrome.com)

**Harrison Brown**  
424.239.3433 | [harrison.brown@blankrome.com](mailto:harrison.brown@blankrome.com)

**Sharon Klein**  
949.812.6010 | [sharon.klein@blankrome.com](mailto:sharon.klein@blankrome.com)

**Alex Nisenbaum**  
949.812.6011 | [alex.nisenbaum@blankrome.com](mailto:alex.nisenbaum@blankrome.com)

**Nicole Bartz Metral**  
424.239.3483 | [nicole.metral@blankrome.com](mailto:nicole.metral@blankrome.com)

*The Privacy Class Acton Defense group would like to thank **Summer Associate Sierra Lactaoen** for her work on this client alert.*

- 
1. Cal. Pen. Code §637.2.
  2. *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183 (2021).
  3. Cal. Pen. Code §631.
  4. *Montantes v. Inventure Foods*, 2014 WL 3305578, at \*4 (C.D. Cal. July 2, 2014).
  5. Cal. Pen. Code §637.2.
  6. *Javier v. Assurance IQ*, 2022 WL 1744107 (9th Cir. May 31, 2022).
  7. *Byars v. Hot Topic, Inc.*, 2023 WL 2026994, at \*9 (C.D. Cal. Feb. 14, 2023). *Byars v. Goodyear Tire & Rubber Co.*, 2023 WL 1788553, at \*5 (C.D. Cal. Feb. 3, 2023).
  8. *Byars v. Goodyear Tire & Rubber Co.*, 2023 WL 1788553, at \*5 (C.D. Cal. Feb. 3, 2023).
  9. First Amended Class Action Complaint, 4, *Valenzuela v. Keurig Green Mountain, Inc.*, 2023 WL 3707181 (N.D. Cal. May 24, 2023).
  10. Order Re: Motion to Dismiss, 7, *Valenzuela v. Keurig Green Mountain, Inc.*, 2023 WL 3707181 (N.D. Cal. May 24, 2023).