NOT FOR PUBLICATION

FILED

JUL 9 2025

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NORA GUTIERREZ, on behalf of herself and all others similarly situated,

Plaintiff - Appellant,

v.

CONVERSE INC., a Massachusetts Corporation,

Defendant - Appellee,

and

DOES, 1 through 25, inclusive,

Defendant.

No. 24-4797

D.C. No.
2:23-cv-06547-KK-MAR

MEMORANDUM*

Appeal from the United States District Court
for the Central District of California
Kenly Kiya Kato, District Judge, Presiding

Argued and Submitted June 10, 2025
Pasadena, California

Before: BYBEE, IKUTA, and FORREST, Circuit Judges.
Partial Concurrence by Judge Bybee.

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

Plaintiff Nora Gutierrez appeals the district court's grant of summary judgment for Defendants Converse Inc. and Does 1 through 25 (Converse). We have jurisdiction under 28 U.S.C. § 1291, review de novo, *Donell v. Kowell*, 533 F.3d 762, 769 (9th Cir. 2008), and affirm.

Gutierrez alleged that Converse aided and abetted violations of section 631(a) of the California Invasion of Privacy Act (CIPA) by Salesforce, a third party that helped operate Converse's website chat function. Gutierrez argues that genuine disputes of material fact exist as to whether Salesforce violated the first, second, and fourth clauses of section 631(a).

Gutierrez's first clause claim fails because no evidence exists from which a reasonable jury could conclude that Salesforce "by means of any machine, instrument, or contrivance, or in any other manner, intentionally tapped, or made any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system." *See* Cal. Penal Code § 631(a). The record is devoid of evidence that Salesforce made an unauthorized connection through a telephone wire, line, cable, or instrument with the messages sent by Gutierrez.

Gutierrez's second clause claim fails because no evidence exists from which a reasonable jury could conclude that Salesforce "read[] or attempt[ed] to read" the

"contents or meaning of any message, report, or communication" sent by Gutierrez. *See id.* Gutierrez argues that the encryption that Salesforce appends to every chat message, as well as a spreadsheet that allegedly shows logins from various Salesforce accounts, creates a genuine issue of material fact as to whether Salesforce accessed chat data. But this evidence is insufficient to defeat summary judgment on the second clause, which requires that Salesforce read or attempted to read *her* chat message. At best, this evidence shows that Salesforce *could* read messages sent through the Converse chat feature.

Gutierrez's fourth clause claim fails because she has not established an underlying violation of section 631(a)'s first or second clause. *See id.* (explaining that one may be liable for "aid[ing]" or "caus[ing] to be done any of the acts or things mentioned above in this section").

AFFIRMED.

BYBEE, Circuit Judge, concurring in part and concurring in the judgment:

I agree with the majority's decision to affirm the district court's grant of summary judgment as to the second and fourth clause claims on evidentiary grounds. I write separately because I think the first clause claim should be affirmed for a different and more obvious reason: As I read it, § 631(a)'s first clause does not apply to internet communications.

Let us begin with the statute. The first clause penalizes:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system . . . .

Cal. Penal Code § 631(a). In other words, it penalizes the use of any instrument to wiretap (or "make[] any unauthorized connection") "with any telegraph or telephone wire, line, cable, or instrument." *See id.* Even assuming that Salesforce wiretapped or made an "unauthorized connection" with Gutierrez's chat message, does the phrase "any telegraph or telephone wire, line, cable, or instrument" contemplate an

online chat message sent on a smartphone?[1]

Today's smartphones do not send messages over a "telephone wire" as that phrase was understood in 1967 when the California legislature passed CIPA. In 1967, telephones were connected to wires on both ends of a phone call and had one use—you picked up the phone to dial and call another phone. Today, our smartphones not only lack wires, but they also are cameras, atlases, phone directories, music players, weather stations, newspapers, clocks, and more. Most important, smartphones are mini-computers capable of accessing the internet, something the California legislature had never heard of (or could have imagined) in 1967. For this reason, simply sending a message on an iPhone (and through an internet browser) does not automatically implicate § 631(a). Instead, the statute, as passed in 1967, focuses on the wiretapping of telegraph or telephone wires—it criminalizes, as relevant here, the wiretapping of a telephone call. *See Flanagan v. Flanagan*, 41 P.3d 575, 577 (Cal. 2002) (CIPA "was enacted in 1967, replacing prior laws that permitted the recording of *telephone conversations* with the consent of one party to the conversation. The purpose of the act was to protect the right of privacy

[1] Because the messages here were sent on a smartphone (more specifically, an iPhone), we need only consider the "telephone" part of this definition, and not the "telegraph" part.

by, among other things, requiring that all parties consent to a recording of their *conversation*.") (emphasis added).[2]

---

[2] Because the text is unambiguous, and does not apply to the internet, we need not consider additional tools of statutory interpretation, including the California Supreme Court's willingness, in the face of ambiguity, to "apply a legal text to technologies that did not exist when the text was created." *See Apple v. Super. Ct.*, 292 P.3d 883, 887 (Cal. 2013).

For what it is worth, CIPA's legislative history suggests that § 631(a) only criminalizes eavesdropping or wiretapping on telephone conversations. Speaker of the California State Assembly Jesse M. Unruh said as much in a press release prior to CIPA's passage. The legislation sought to criminalize the use of electronic bugging devices, what Unruh called "tiny devices," and would allow "private parties who suffer injury due to eavesdropping without their consent [to] file civil suit to recover substantial money damages."

The preamble of CIPA, § 630, titled "Legislative declaration and intent," codifies Unruh's understanding. It states:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.
>
> The Legislature by this chapter intends to protect the right of privacy of the people of this state.
>
> The Legislature recognizes that law enforcement agencies have a legitimate need to employ modern listening devices and techniques in the investigation of criminal conduct and the apprehension of lawbreakers. Therefore, it is not the intent of the Legislature to place greater restraints on the use of listening devices and techniques by law enforcement agencies than existed prior to the effective date of this chapter.

If the California legislature wanted to apply § 631(a) to the internet, it could do so by amending that provision or adding to CIPA's statutory scheme. Indeed, it "augmented the statutory scheme in 1985, 1990, and 1992 'to take account of privacy issues raised by the increased use of cellular and cordless telephones.'" *See Smith v. LoanMe, Inc.*, 483 P.3d 869, 873 (Cal. 2021) (quoting *Flanagan*, 41 P.3d at 580 (compiling amendments)). For example, the California legislature added § 632.7 in 1992. That provision criminalizes nonconsensual interception and recording of "a communication transmitted between," among other things, "two cordless telephones." Cal. Penal Code § 632.7. The California legislature also added § 632.01 in 2017. That provision punishes anyone who violates § 632(a) (a section that penalizes eavesdropping) and then "intentionally discloses or distributes, in any manner, in any forum, including, but not limited to, Internet Web sites and social media . . . the contents of a confidential communication with a health care provider . . . ." *See* Cal. Penal Code § 632.01. California has failed to update § 631(a) to account for advances in technology since 1967. It is not our job to do it for them.

Cal. Penal Code § 630. This section sounds in retroactivity—CIPA seeks to criminalize the use of "advances" *predating* its passage. Its last paragraph provides helpful specificity—the "advances" it speaks of are identified as "listening devices." This is yet another reason to construe the statute as concerning the tapping of telephone conversations, not chat messages sent over the internet.

Unless and until then, plaintiffs like Gutierrez are not without recourse, thanks to the California Consumer Privacy Act of 2018 (CCPA). CCPA requires that businesses inform consumers of the "categories of personal information to be collected and the purposes" for that collection, "the categories of sensitive personal information to be collected," and "the length of time the business intends to retain each category of personal information." Cal. Civ. Code § 1798.100. Section 1798.150 creates a private cause of action for "[a]ny consumer whose nonencrypted and nonredacted personal information . . . or whose email address . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information . . . ."[3] Cal. Civ. Code § 1798.150.

This statute likely covers the allegations here, so why do plaintiffs (like Gutierrez) prefer to contort § 631(a) to apply to internet communications? It may be about the money—CIPA allows plaintiffs to recover $5,000 per violation compared to just $750 per violation under the CCPA. *Compare* Cal. Penal Code

[3] The statutory scheme is extensive and sets out additional consumer rights. *See*, *e.g.*, § 1798.106 (consumer right to correct inaccurate personal information); § 1798.135 (permissible uses of consumer information); § 1798.110 (consumer right to know what information is collected); § 1798.121 (consumer right to limit use and disclosure of personal information); § 1798.125 (consumer right of no retaliation).

§ 637.2 *with* Cal. Civ. Code § 1798.150. In a class action like this one, the difference in total recovery (and attorneys' fees) could be millions of dollars.

In my view, § 631(a)'s text, legislative history, subsequent augmentation, and relative ambiguity compared to the CCPA (which explicitly provides recourse for internet privacy violations like this one) compel the conclusion that § 631(a)'s first clause does not apply to the internet. Until and unless the California appellate courts tell us otherwise, or the California legislature amends § 631(a), I refuse to apply § 631(a)'s first clause to the internet.

One final note. Gutierrez asserted that our unpublished memorandum disposition in *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022), held that the entirety of § 631(a) applies to internet communications. This is misleading. *Javier* is not precedential, as it is an unpublished disposition. And *Javier* only considered § 631(a)'s second clause, which prohibits nonconsensual reading of a communication in transit over a wire. *Id.* at *1. It is far from clear whether *Javier*'s alleged "holding"—that "[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications"—even applies to § 631(a)'s first clause.[4]

[4] *Javier* has led to a raft of § 631(a) litigation, as documented by the Chamber of Commerce's amicus brief in this case. This has given California's federal courts ample opportunity to consider whether § 631(a)'s first clause applies to internet communications. These courts have overwhelmingly agreed it does not. *See*, *e.g.*, *Cody v. Ring LLC*, 718 F. Supp. 3d 993, 999 (N.D. Cal. 2024) ("Clause one

For the foregoing reasons, I concur in the judgment as to first clause claim.

of Section 631(a) prohibits telephonic wiretapping, which does not apply to the internet, and so cannot support [Plaintiff's] claims.") (citing three cases finding the same); *Rodriguez v. Ford Motor Co.*, 722 F. Supp. 3d 1104, 1115 (S.D. Cal. 2024) (finding the same and citing five additional cases).