UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

CHARMAINE TATE, individually and on behalf of all others similarly situated, Plaintiff, v. VITAS HEALTHCARE CORPORATION, Defendant.	2:24-cv-01327-DJC-CSK ORDER

A woman called a healthcare provider to discuss sensitive details about the provider's hospice care for the woman's grandmother. Unknown to the woman calling, the healthcare provider utilized a software to listen to the contents of the call and produce data about the call's purpose and resolution. Via its Terms of Service, the software creator reserved the rights to employ the data yielded from those calls for its own business and product development functions. Does the woman have a viable claim that the use of that software by the healthcare provider and the software developer violated California privacy laws?

In weighing this question, the Court must determine whether the software developer is a third party separate from the healthcare provider, or an extension of the healthcare provider itself. The Court joins a number of district courts in holding

that the developer of software used to record and analyze phone calls is a third party when the developer is able to utilize data obtained for its own purposes, separate from the interests of the parties to the call. The Court finds that the software developer in this case is capable of using the data for its own purposes, and because the use of its software was not disclosed to the caller, it may be in violation of California privacy laws. Additionally, because the healthcare provider aided the software developer in obtaining access to the client calls, it may also be held liable. Accordingly, Defendant's Motion to Dismiss (ECF No. 12) is DENIED.

BACKGROUND

Defendant VITAS Healthcare Corporation operates hospice and palliative care locations throughout California. (ECF No. 10; "FAC" ¶ 9.) It utilizes a conversation intelligence software-as-a-service ("SaaS") provided by Invoca, Inc. ("Invoca") to help analyze the more than 90,000 annual calls it receives to its call centers. (*Id.* ¶¶ 1, 36.) When a person calls VITAS, Invoca's software records and creates a transcript of the caller's speech. (*Id.* ¶ 20.) Invoca feeds that transcript to an artificial intelligence (AI) program that identifies patterns and classifies the data into a searchable database, which is then sent to VITAS. (*Id.*) This database is used by VITAS to understand what questions and concerns its callers have, so that VITAS can adjust the content it delivers to consumers and the call scripts utilized by its representatives. (*Id.* ¶ 37.) Under its Terms of Service, Invoca can also use data obtained for other limited purposes, including "to optimize and improve Services or otherwise operate Invoca's business." (*Id.* ¶¶ 33, 34.) Neither VITAS nor Invoca obtain the consent of any caller to VITAS's call center, and callers are unaware that their speech is being recorded and analyzed. (*Id.* ¶¶ 6, 40.)

In late 2023, Plaintiff Charmaine Tate called Defendant VITAS and spoke with a VITAS representative regarding hospice care for Tate's grandmother. (*Id.* ¶¶ 8, 42.) Tate alleges that the use of Invoca's software to record and analyze her and others' calls to VITAS violates the California Invasion of Privacy Act ("CIPA") sections 631(a)

(unauthorized wiretapping) and 632(a) (unauthorized eavesdropping on or recording of confidential communications), and that VITAS is liable for aiding those violations. (*Id.* ¶ 41; *see* Cal. Pen. Code[1] §§ 631(a), 632(a).) On February 28, 2024, Tate brought this action in the Sacramento Superior Court on behalf of herself and members of a proposed class, and it was removed to federal court on May 9, 2024. The proposed class for which Tate seeks certification would consist of all California residents who called VITAS's customer service line while in California and whose conversations with VITAS were intercepted and recorded by Invoca. (*Id.* ¶ 49.)

LEGAL STANDARD

A party may move to dismiss for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). The motion may be granted only if the complaint lacks a "cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). While the Court assumes all factual allegations are true and construes "them in the light most favorable to the nonmoving party," *Parks Sch. of Bus., Inc. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995), if the complaint's allegations do not "plausibly give rise to an entitlement to relief" the motion must be granted, *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009) ("*Iqbal*").

A complaint need contain only a "short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), not "detailed factual allegations," *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). However, this rule demands more than unadorned accusations; "sufficient factual matter" must make the claim at least plausible. *Iqbal*, 556 U.S. at 678. In the same vein, conclusory or formulaic recitations of elements do not alone suffice. *Id.* "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* This

[1] All undesignated statutory references are to the California Penal Code unless otherwise specified.

evaluation of plausibility is a context-specific task drawing on "judicial experience and common sense." *Id.* at 679.

DISCUSSION

CIPA provides parties to a phone call legal protection from unauthorized, third-party listeners eavesdropping or recording the contents of those calls. Section 631(a) outlines repercussions for any person:

> (1) "[W]ho, 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, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state;" or
> (2) "[W]ho uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

Section 632(a) prohibits a person from:

> "[I]ntentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio."

There are three questions the Court must consider in weighing VITAS's Motion to Dismiss (hereinafter, "Mot."). First, the Court must determine the standard to apply to Invoca's access to VITAS's caller data, specifically whether Tate must allege that Invoca actually used the data for its own purposes, or merely that Invoca was capable of doing so. Second, the Court must decide whether Invoca's software is considered a "device" under section 632(a). Finally, the Court must assess whether a common law

aiding and abetting standard should be read into section 631(a). At present, there is no Ninth Circuit precedent on these questions and district courts in this Circuit have reached different results. The Court discusses each issue in turn.

I. Whether Invoca must actually use the data it obtains for its own purposes

Section 631(a) prohibits third parties from "read[ing], or attempt[ing] to read, or to learn the contents or meaning of any message, report, or communication" "without the consent of all parties to the communication." § 631(a). Plaintiff alleges that Invoca, via its software, learns the contents of calls to VITAS without the consent of the caller, therefore violating section 631(a) as an unauthorized, third-party listener. (FAC ¶ 7.) Defendant counters that because Invoca provides its data solely to VITAS, it is not a third party but rather an extension of VITAS itself, and therefore the use of Invoca's software cannot violate section 631(a). (Mot. at 3–6.)

There are two seminal California cases that frame how courts consider third parties under CIPA: *Rogers v. Ulrich*, 52 Cal. App. 3d 894 (1975) and *Ribas v. Clark*, 38 Cal. 3d 355 (1985). In *Rogers*, Ulrich used a tape recorder attached to his telephone to record his phone call with Rogers, and then later played that recording for a third party who was not involved in the call. *Id.* at 897–98. The California Court of Appeal held that Ulrich's use of a tape-recording device did not violate section 631(a)'s restriction on eavesdropping because Ulrich himself was a party to the call, noting that "only a third party can listen secretly to a private conversation." *Id.* at 899; see *Ribas*, 38 Cal. 3d at 360, fn.3 ("*Rogers* merely held, correctly, that section 631 does not penalize the secret recording of a conversation by one of the *participants*."). In other words, Ulrich's recording device was seen as a permissible extension of Ulrich himself.

By contrast, in *Ribas*, a woman called her husband and had Clark, a third party, listen in live on her phone call as the husband allegedly confessed that he had prevented his wife from obtaining counsel during the dissolution proceedings of their marriage. 38 Cal. 3d at 358–59. The California Supreme Court held that Clark's secret monitoring was prohibited under section 631(a), noting that this kind of privacy

violation committed by a third party to the call "denies the speaker an important aspect of privacy of communication," and that the state legislature had sought to curb these sorts of privacy violations. *Id.* at 361.

The Court is tasked with determining whether Invoca's software is more similar to the permissible tape recorder used in *Rogers*, or the impermissible third-party listener in *Ribas*. That is to say, does the software function as a recording made by a party to the call, or is it a separate party entirely? Further, there is a split amongst district courts as to whether a third-party entity must actually use the data it obtains for its own purposes or if it merely needs to have the *capability* to do so to act as a third party in violation of section 631(a).

On one side of this split is *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021). *See also Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962 (N.D. Cal. 2023). *Graham* involved a web application called Noom, which utilized a software designed by FullStory to record what actions visitors took on Noom's website, including visitors' keystrokes, mouse clicks, and page scrolling. *Id.* at 827. A visitor to Noom's website sued, alleging that the software's collection of user interactions with the application constituted privacy violations under section 631(a). *Id.* at 828–29. The *Graham* court held that neither company violated section 631(a), reasoning that FullStory merely captured the user data and hosted that data on its own servers where Noom could then use the data by analyzing it. *Id.* at 832–33. The court distinguished the case from similar ones in which the software developer had actually received some sort of benefit from collecting user data itself, such as when those software developers themselves separately sold the user data. *Id.*; *see Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019). Noting these differences, the court saw FullStory's software as an extension of Noom itself because Noom was the party that was responsible for assessing the data received, with the software solely working to collect that data for Noom, and Noom alone. *Graham*, 533 F. Supp. 3d at 832–33.

On the other side of this split is *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891 (N.D. Cal. 2023). *Javier* involved Assurance IQ, LLC's use of a software developed by ActiveProspect Inc., which tracked website visitors' keystrokes, mouse clicks, data entry, and other interactions. *Id.* at 894. In weighing the plaintiff's section 631(a) claim, the *Javier* court critiqued *Graham*'s reasoning that a third-party software developed would need to use the data for its own purposes in order for it to violate section 631(a). *Id.* at 900. The *Javier* court noted that there is already a use requirement in one of section 631(a)'s discrete clauses ("us[ing], or attempt[ing] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained"), and therefore it would be improper to impute that use requirement to all of section 631(a). *Id*. The court in that case also noted that in *Ribas*, the California Supreme Court never considered the wife's friend's intentions or her use for the information obtained, and so to consider a third party's intent in obtaining data here would similarly be improper. *Id.*; *Ribas*, 38 Cal. 3d at 360–61.

The Court finds *Javier*'s reasoning to be more persuasive. Section 631(a)'s text, which prohibits a third party from "learn[ing] the contents or meaning of any message," does not actually contain a use requirement. *See id.* at 899–900; § 631(a). But in a separate section, separated by a semicolon, the statute then prohibits a party from "us[ing], or attempt[ing] to use" any obtained information. § 631(a). The statute outlines several ways for its restriction to apply and does not limit its application solely to parties that directly use the data they obtain from listening in on a call. In other words, an entity can violate the statute by learning the contents of the message *or* by using information obtained from listening in on a conversation. Similar to the California Supreme Court and *Javier* court, this Court finds it unnecessary to consider a third party's intention to collect or use data from a call. *See Ribas*, 38 Cal. 3d at 360–61. Obtaining that data while reserving the capability to utilize it makes a third party distinct from one of the parties to the call and may trigger a violation of section 631(a).

This reading of the statute's plain text is also in line with what the California Supreme Court has made clear: that the state legislature's "express objective in enacting section 631" was to protect callers from having an outsider "tap [their] telephone *or listen* in on the call." *Ribas*, 38 Cal. 3d at 363. Because Invoca's software effectively "listen[s] in" on user calls, independently analyzes that data, and the company reserves the capability to then use that data for its own purposes, Invoca's software may be in violation of 631(a).

Moreover, while the Court does not find *Graham* persuasive, even *Graham* itself does not help Defendant here. While *Graham* likewise involved claims of improper collection of data rather than *use* of that data, critically in *Graham* the plaintiffs did not allege that FullStory collected the data and could use it for its own purposes. Rather, they attacked FullStory's storage of user information on its servers, framing that storage itself as a violation of section 631(a). *Id.* at 828, 832–33. The district court rejected the plaintiff's argument, noting that "there are no allegations here that FullStory intercepted and used the data itself," and highlighted that FullStory's software simply recorded data that was then analyzed by Noom, rather than FullStory. *Id.* at 832–33. But here, Plaintiff *does* allege that Invoca has the capability to analyze the data itself and further, that Invoca expressly reserves the ability to use that data for its own purposes. (FAC ¶¶ 30–35.)

Defendant's reliance on *Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962 (N.D. Cal. 2023) to argue that an alleged third party that merely records data for a legitimate party to a call does not violate section 631(a) is similarly unavailing. (*See* Mot. at 4–5.) *Yockey* involved Rite Aid and Kaiser Permanente's utilization of a software developed by Salesforce to create transcripts of online chat messages sent on the companies' website. *Yockey*, 688 F. Supp. 3d at 967–68. Interestingly, and to Defendant's detriment, that case specifically recognized that the inquiry into whether a third-party acts as an extension of a part to the call hinges on "whether the third party 'ha[s] the *capability* to use its record of the interaction for any other purpose.'"

See id. at 972, quoting *Javier*, 649 F. Supp. 3d at 900. The plaintiffs in that case did not sufficiently allege that the third party could use any data obtained for its own purpose—they were not able to point to evidence beyond the third party's possession of user data to substantiate their claim. *Id.* at 972–73. But here, as discussed next, Plaintiff does properly allege that Invoca has that capability, namely Invoca's express reservation of that ability in its Terms of Service. VITAS' own case citations support the argument that Invoca's ability to use the data it collects for its own purposes is itself sufficient to establish a violation of section 631(a).

VITAS maintains that Invoca's collection of data is solely for the use of VITAS and that Invoca cannot use the data for any other purposes. (Mot. at 4–6.) VITAS points to a "Business Association Agreement," which it states precludes Invoca from utilizing any data obtained for its own purposes. (*Id.* at 6, fn.3.) VITAS does not attach a copy of this Agreement as an exhibit nor does it explicitly describe its contents; and in any event the Court is precluded from relying on such factual assertions in resolving a motion to dismiss under Rule 12(b)(6). *See Arpin v. Santa Clara Valley Transp. Agency*, 261 F.3d 912, 925 (9th Cir. 2001) ("[E]vidence outside the complaint . . . should not be considered in ruling on a motion to dismiss."). Regardless of any Business Association Agreement, Invoca's Terms of Service expressly reserve the ability to use "Client Data, as reasonably necessary for Invoca to provide and enhance its provision of services." (FAC ¶ 33.) Under these Terms of Service, Invoca *may* use the data obtained from calls placed to VITAS to improve its own product and services. Invoca's software has already allegedly violated the caller's privacy; whether Invoca actually uses the contents of the call for its own purposes is not legally relevant. *See Javier*, 649 F. Supp. 3d at 900.

Accordingly, the Court finds that Invoca, via its software, is a third party, distinct from both Plaintiff Tate and Defendant VITAS, and that Invoca's ability to use the data obtained for its own purposes may be sufficient to trigger section 631(a) liability.

////

II. Whether Invoca's software is an "electronic amplyfying or recording device"

Finding that Invoca is a third party, the Court must then determine whether it is a recording device under section 632(a). As relevant here, section 632(a) prohibits third parties from using a "recording device to eavesdrop upon or record the confidential communication" of a call, but does not provide a definition of "device." § 632(a). Defendant VITAS asserts that Invoca's software is not a "device" under CIPA. (Mot. at 7–8.) District courts have defined "device" differently depending on which section of CIPA a claim arises under. For example, in *In re Google Location History Litigation*, 428 F. Supp. 3d 185, 193 (N.D. Cal. 2019) ("*Google Litigation*"), the court analyzed a software under a different section of CIPA—section 637.7(d)—and found that "[s]oftware like Google Maps, Chrome, etc. are not 'devices' within the meaning of CIPA because they are not 'equipment.'" But courts have also reached contrary results. In *Gladstone v. Amazon Web Servs., Inc.*, 2024 WL 3276490, *8 (W.D. Wash. July 2, 2024), the court turned to the federal Wiretap Act for a definition of "device" under CIPA and found "that 'device,' as used in section 632, can include software." After weighing these two approaches, the Court agrees with *Gladstone* that section 632(a)'s definition of "device" can include Invoca's software.

Federal courts apply state rules of statutory construction when interpreting a statute from that state. *See In re Lares*, 188 F.3d 1166, 1168 (9th Cir. 1999). The first step in that inquiry is to "scrutinize the actual words of the statute, giving them a plain and commonsense meaning." *Cal. Tchrs. Assn. v. Governing Bd. of Rialto Unified Sch. Dist.*, 14 Cal. 4th 627, 633 (internal quotations omitted). If no ambiguity exists, the plain language of the statute governs. *People v. Snook*, 16 Cal. 4th 1210, 1215 (1997) ("*Snook*").

Defendant VITAS urges the Court to look to *Google Litigation*, 428 F. Supp. 3d 185, and *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764 (N.D. Cal. Dec. 14, 2017), both of which conclude that a software is not a device under CIPA. (Mot. at

8.) However, neither case is applicable because they both analyze "devices" under section 637.7(d), rather than section 632(a). *Google Litigation* involved a tracking software that collected and stored user data. 428 F. Supp. 3d at 187–88. A user sued under section 637.7, alleging that the software improperly tracked and stored their location, but the district court dismissed the claim, finding that downloaded software is not a device within the meaning of section 637(d). *Id.* at 193–94. And in *Moreno*, when faced with a similar set of facts, the court reached the same conclusion, positing that software is not a "device" under section 637(d). 2017 WL 6387764 at *5.

But section 637.7(d)'s text explicitly restricts its definition of "electronic *tracking* device" (emphasis added) to that specific section, rather than to other sections such as 632(a) which use the more generic phrase "electronic device". *See* § 637.7(d) ("As used in this section, 'electronic tracking device' means . . ."). And even if its definition were used to inform other sections, section 637.7 is concerned with electronic tracking devices that are clearly meant to be physical and thus is not a proper consideration for defining "device" under section 632(a). Specifically, section 637.7(d) defines an "electronic tracking device" as one that can be "attached to a vehicle or other movable thing" which evinces the statute's emphasis on proscribing physical tracking devices. *See* § 637.7(d). Section 632(a), however, lacks any language suggesting that an "electronic amplifying or recording device" must be physical in nature. Relying on the more specific text of section 637.7(d) to inform section 632(a) is misguided, given section 637.7(d)'s explicit focus on tangible devices.

Gladstone, which considers the definition of "device" under the federal Wiretap Act, provides a more helpful framework for deducing what "device" means under section 632(a). 2024 WL 3276490. Courts routinely look to federal law in interpreting CIPA, which was modeled off the Wiretap Act. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act."), quoting *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018); *see also* 18 U.S.C. § 2510 et seq. In *Gladstone*, the district

court turned to the Wiretap Act to help determine whether a software developed by Amazon that recorded and analyzed call information should be considered a device under section 632(a). The *Gladstone* court considered two factors—first, that the majority of federal courts nationwide applying the federal Wiretap Act have landed on a definition of "device" that includes software. *See United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) (collecting cases); *see also In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1087 ("Software is an '[e]lectronic, mechanical, or other device' which 'can be used to intercept a wire, oral, or electronic communication.'"). Second, the court considered the California Supreme Court's instruction that "all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Gladstone*, 2024 WL 3276490 at * 8, quoting *Javier v. Assurance IQ, LLC,* 2022 WL 1744107, *2 (9th Cir. May 31, 2022); *see Ribas*, 38 Cal. 3d 355.

These factors together support a reading that software can be a device under section 632(a). Invoca's software, while not a physical device, has the capability to *record* confidential information made in calls and reproduce those calls and data extracted from them for VITAS or Invoca. That is to say, even though it is not physical, the software functionally operates in a way that is reasonably envisioned by the statute. And like in *Gladstone*, the recording undertaken by the software infringes on the very privacy right that the California Legislature sought to enshrine in CIPA. *See Ribas,* 38 Cal. 3d at 359 ("In enacting this statute, the Legislature declared in broad terms its intent 'to protect the right of privacy of the people of this state' from what it perceived as 'a serious threat to the free exercise of personal liberties [that] cannot be tolerated in a free and civilized society.' [Citation.] This philosophy appears to lie at the heart of virtually all the decisions construing the Privacy Act.")

Because the software can record conversations and in doing so, violates the privacy of at least one of the callers, the Court finds that Invoca's software can be considered a "device" under section 632(a).

III. Whether VITAS can be held liable for aiding, agreeing with, employing, or conspiring with Invoca

Under 631(a), an entity that "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who *aids, agrees with, employs, or conspires with any person or persons* to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section" may be held liable. § 631(a) (italics added). Defendant VITAS argues that it lacks the requisite intent under an "aiding and abetting" standard because it did not know that Invoca was allegedly violating section 631(a). (Mot. at 7.)

The plain text of section 631(a) is unambiguous on this issue: the statute requires that a party "aids, agrees with, employs, or conspires" with another party. § 631(a). It does not require that a party aid *and* abet. *See Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1130 (S.D. Cal. 2023) ("Defendant's contention that 'aids' means 'aiding and abetting' ignores the 'agrees with, employs, or conspires with' language of the clause."). VITAS's proposed "aiding and abetting" standard goes beyond what the statute requires, and there is no basis to read in a common law standard of aiding and abetting when the statute itself is clear. *See Snook*, 16 Cal. 4th at 1215 ("If there is no ambiguity in the language, we presume the Legislature meant what it said and the plain meaning of the statute governs."). Instead, to establish a violation a plaintiff need only prove that a party (VITAS) aided, agreed with, employed, or conspired with a third party (Invoca) as it violated section 631(a). As discussed above, Plaintiff Tate has pled facts that would support a viable claim that Invoca has violated the statute. Plaintiff's claims that VITAS has supported Invoca in doing so by allowing Invoca access to the calls and has presumably paid Invoca to analyze the data those calls yield are sufficient to implicate section 631(a). Accordingly, the Court finds that VITAS may be found liable under section 631(a) for its role in assisting Invoca's monitoring and analysis of calls made to VITAS.

////

CONCLUSION

In accordance with the above, IT IS HEREBY ORDERED that Defendant's Motion to Dismiss (ECF No. 12) is DENIED.

IT IS SO ORDERED.

Dated: **January 8, 2025**

Hon. Daniel J. Calabretta
UNITED STATES DISTRICT JUDGE

DJC5 – tate24cv01327.MTD