United States District Court	Iorthern District of California

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

NOT	FOR	CITA	TION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

LATISHA SATCHELL,

Plaintiff,

v.

SONIC NOTIFY, INC., et al.,

Defendants.

Case No. 16-cv-04961-JSW

ORDER GRANTING, IN PART, AND **DENYING, IN PART, MOTIONS TO DISMISS**

Re: Dkt. Nos. 61, 62

Now before the Court for consideration are the motions to dismiss filed by Yinzcam, Inc. ("Yinzcam"), Golden State Warriors, LLC ("Warriors"), and Signal 360, Inc. (f/k/a Sonic Notify, Inc.) ("Signal 360") (collectively, "Defendants"). The Court has considered the parties' papers, relevant legal authority, the record in this case, and the parties' oral argument at the hearing. For the reasons set forth in the remainder of this Order, the Court GRANTS, IN PART AND DENIES, IN PART, Defendants' motions to dismiss.

BACKGROUND

A. Factual Background.

The Warriors organization offers its fans a mobile application ("the App"), developed by Yinzcam, which provides "an interactive experience for fans by delivering scores, news, and other

On September 29, 2017, Plaintiff filed a statement of recent decision. (Dkt. No. 86.) Yinzcam argues the submission is untimely. However, the case submitted by Plaintiff was decided after the Court held the hearing in this case. Although Local Rule 7-3(d)(2) suggests Plaintiff should have asked for leave to submit the opinion, Plaintiff complied with the rule by not including any argument about the case. The Court will accept Plaintiff's filing, and it has considered the opinion, as it would any other legal authority available to the Court.

information relevant to the organization[.]" (FAC, $\P\P$ 2, 4; *see also id.* $\P\P$ 29-30, 33.) Plaintiff's claims in this putative class action arise from her allegations that, through the App, Defendants "systematically and surreptitiously intercept[] consumers' oral communications without their consent." (FAC at 1:23-24.)

Plaintiff alleges the Warriors partnered with Signal360 "to integrate Signal360's beacon technology" into the App. According to Plaintiff, Signal360 designed its software so that a block of source code would turn on the microphone of a user's smartphone, or other electronic device, and would constantly record all audio, including personal and private conversations. Thus, Plaintiff alleges the App effectively functions as a "bug." Plaintiff alleges Signal360 "owns and controls the Bug's code base that Yinzcam and [the Warriors] put" in the App. (*Id.* ¶ 66.) Plaintiff alleges Yinzcam "developed and maintained the codebase of the" App "and ensured the deliverability of the App to the Google Play Store and, ultimately, consumers." (*Id.* ¶ 67.)

Signal360 uses traditional Bluetooth beacons and an audio beacon that functions even when a user has disabled Bluetooth reception on a smartphone or mobile device. According to Plaintiff, Signal360 and the Warriors understood that the App would function as a bug and they directed Yinzcam to integrate this bug into the App. (FAC \P 3-4, 7-9, 22-23, 27, 34-38, 41-42, 65-67.)³

[The Warriors] and Signal 360, programmed the Warriors App to instantly initiate the Bug once the App was installed and opened. The Bug then executed commands programmed by ... Signal 360 to communicate with Signal360's servers. The Signal360 servers would then respond with a command to turn on the Bug, which was programmed at the request of [the Warriors]. Specifically, [the Warriors] worked with ... Signal360 to specifically identify rules and terms for their beacon scheme and knew that those rules and terms would be transmitted to the tens of thousands of devices and,

Whether the App described in this Order functions as Plaintiff alleges it does is disputed. However, that is not a matter the Court can resolve on this motion. Accordingly, the facts set forth herein are accepted as true for purposes of this Order.

This is the second iteration of Plaintiff's complaint. The Court described the beacon technology in more detail in its Order granting, in part, and denying, in part, Defendants' motions to dismiss Plaintiff's initial complaint. *See Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 999-1000 (N.D. Cal. 2017). Plaintiff describes the beacon technology in paragraphs 22-28 of her FAC.

//

in turn, would cause the Bugs on those devices to activate and, thus, turn users' smartphones into listening devices.

That is, once consumers downloaded and opened the Warriors App, the App would engage the Bug, receive an OK from Signal360's server (per the rules created by [the Warriors]), and turn on consumers' microphones, listening and picking up any and all audio within range of a user's microphone. The Bug continued listening until its process was closed – either when the consumer's smartphone was shut off or when the consumer manually stopped the Bug's process (something consumers ignorant of the Bug would not know to do). ...

(*Id.* ¶¶ 41-42.) Plaintiff also alleges the Warriors and Signal360 are able to monitor the effectiveness of the beacons through Signal360's content management system, which tracks various metrics, including information about a particular mobile user. (*Id.* ¶¶ 9-10; *see also id.* ¶¶ 43-45.)⁴

Although Yinzcam programmed the App to ask for certain permissions, including a request to use a device's microphone, Plaintiff alleges Defendants do not ask consumers to "opt-in" to beacon technology. (*Id.* ¶¶ 31-32.) Plaintiff also alleges that the Defendants did not inform an App user that the "bug" was loaded on to a user's smartphone and;/or mobile device; nor did Defendants obtain an App user's consent to turn these electronic devices into "listening device[s]." (*Id.* ¶ 11; *see also id.* ¶¶ 32, 39.)

Plaintiff downloaded the App in April 2016 and used it at least once per day, until about July 11, 2016. Plaintiff also alleges she carried her smartphone with her "to places where she would not invite other people, and to places where she would have private conversations." (*Id.* ¶ 47.) Plaintiff further alleges that "[d]uring this entire time, the [b]ug's process was running" and continuously recorded all audio, including her private conversations without her knowledge or consent. (*Id.* ¶¶ 48-51.)

The Court will address additional allegations as necessary in the analysis.

Paragraph 10 does not contain a complete sentence. It appears to be a continuation of paragraph 9.

Northern District of California

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

R	Plaintiff's	Claime	for	Daliaf
Б.	Piainiiii S	Chaims	m	Kenei

Plaintiff's first claim for relief alleges that each of the Defendants violated 18 U.S.C. section 2511(1)(a), which makes it unlawful for any person to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication[.]" Plaintiff's second claim for relief alleges that each of the Defendants violated 18 U.S.C. section 2511(1)(b), which makes it unlawful for a person or entity to:

> intentionally use[], endeavor[] to use, or procure[] any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

- (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication;
- (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
- (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
- (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
- (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States[.]

Plaintiff alleges Defendants intercepted her oral communications. An oral communication is defined to mean "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(2).⁵ In her second claim for relief, Plaintiff presents an alternative theory of relief that the

Unlike Section 2511(1)(a), by its terms Section 2511(b) only applies to oral communications, although it prohibits interception of oral communications, inter alia, by using a device that transmits a signal through wire communications. See, e.g., United States v. Anaya, 779

Warriors and Yinzcam "procured" Signal360 to intercept her oral communications.

ANALYSIS

A. Applicable Legal Standard.

Defendants move to dismiss for failure to state a claim, pursuant to Federal Rule of Civil Procedure 12(b)(6). On such a motion, the Court's "inquiry is limited to the allegations in the complaint, which are accepted as true and construed in the light most favorable to the plaintiff." *Lazy Y Ranch LTD v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008). Even under the liberal pleadings standard of Federal Rule of Civil Procedure 8(a)(2), "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a claim for relief will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)).

Pursuant to *Twombly*, a plaintiff must not allege conduct that is conceivable but must allege "enough facts to state a claim to relief that is plausible on its face." *Id.* at 570. "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." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). In general, if the allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. *See, e.g. Reddy v. Litton Indus., Inc.*, 912 F.2d 291, 296 (9th Cir. 1990); *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246-47 (9th Cir. 1990).

/

F.2d 532, 534-35 (9th Cir. 1985) ("Congress prohibited the interception of oral communications pursuant to both the fourteenth amendment (subparagraph (a)) and the commerce clause (subparagraph (b)). The dual proscription against the interception of oral communications and the concomitant unusual statutory structuring, therefore, is explained by Congress' desire to legislate under both constitutional grants of authority.").

Plaintiff alleges that that during the time the App was on her phone, Defendants "intercepted (by listening in and recording) Plaintiff's ... private conversations, including oral communications[.]" (FAC \P 63.) Although courts have found telephone calls fall within the definition of wire communications, *see*, *e.g.*, *Siripongs v. Calderon*, 35 F.3d 1308, 1320 (9th Cir. 1994), Plaintiff's allegations and arguments focus on alleged interception of oral communications. The Court finds no meaningful distinction between Plaintiff's two claims for relief, and it analyzes each claim together, rather than separately.

1

3 4

5

6

7

8

9 10

11

13

12

14 15

16

17

18

19

20

21 22

23

24

25

26

27

28

B. The Court Grants, In Part, and Denies, in Part, the Motions.

The Wiretap Act provides a private right of action for "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter ... from the ... entity, ..., which engaged in that violation[.]" 18 U.S.C. § 2520(a). In order to state a claim under either Section 2511(1)(a) or 2511(1)(b), Plaintiff must allege the Defendants intercepted an oral communication. The Court previously determined that Plaintiff could not rely on a theory of joint and concerted action to state a claim and required Plaintiff to "identify with particularity the precise manner in which each Defendant is alleged to have violated the Wiretap Act." Satchell, 234 F. Supp. 3d at 1007. Plaintiff continues to rely on a theory of joint and concerted action and argues that "no one Defendant, acting alone, could have carried out the interceptions." (Dkt. No. 70, Opp. Br. at 11:18.)

In Freeman v. DirecTV, Inc., the Ninth Circuit was presented with the issue of whether 18 U.S.C. section 2707 provided "a private cause of action ... against those who aid and abet, or conspire with, electronic communications service providers in unlawfully disseminating the contents of electronic communications," in violation of 18 U.S.C. section 2702, and concluded it did not. 457 F.3d 1001, 1002 (9th Cir. 2006). The court reasoned that the language of the two statutes was "straightforward" and did not use "the terms 'conspiracy' or 'aiding and abetting." Id. at 1006. The plaintiffs argued that Congress must have intended to provide for secondary liability by "including in [section] 2707 the term 'engaged." Id. at 1005. The court "decline[d] to give the term 'engaged' the broad construction urged" by the plaintiffs, which it found "contrary to the context in which the term is used." Id.

The court noted that Section 2707 used the term engaged "twice; both times the term is used in conjunction with 'violation.' Section 2707 does not define the violation – it provides, under certain circumstances, the remedy for a person aggrieved by a violation that is defined in other sections, such as [section] 2702. Because there is no language in [section] 2702 suggesting secondary liability," the court found "no textual support for [the plaintiff's] contention that Congress explicitly provided for aiding and abetting or conspiracy claims." *Id.*

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Section 2511 is "not as textually limiting as" Sections 2702 and 2707, because Section 2702 imposes "liability on a particular group, electronic service providers – and then specifies the limited circumstances that ... will subject that particular group to liability." *Id.*, at 1009. In contrast, Section 2511 imposes liability on "any person' and then lists a number of prohibited actions." Id. at 1008. Although Sections 2702 and 2511 differ in that respect, the Freeman court also stated that Section 2511 "does not explicitly provide for secondary liability." 457 F.3d at 1008; see also id. at 1006 ("if Congress intended to impose secondary liability by targeting aiding and abetting action, it certainly knows how to do it") (citing Central Bank of Denver N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164, 177 (1994)).

Section 2511 applies to a broader class of persons or entities than Section 2702. However, under both Section 2707 and Section 2520, a private right of action lies only against a person or entity who "engaged in that violation." The Court finds that Freeman's reasoning about the construction of the phrase "engaged in," as used in Section 2707, would apply equally to the phrase as used in Section 2520(a) and does not provide for secondary liability. In the context of this case, Plaintiff must allege each Defendant actually intercepted her oral communications. Cf. In re Carrier IQ, Inc. Consumer Privacy Litig., 78 F. Supp. 3d 1051, 1090 (N.D. Cal. 2015); Kirch v. Embarg Management Co., 702 F.3d 1245, 1248 (10th Cir. 2012) (finding that Section 2520(a) "does not encompass aiders or abettors" and stating that "the person or entity ... which engaged in that violation is the person or entity that intercepted, disclosed, or intentionally used the communication") (internal quotations omitted and emphasis added).⁶

Plaintiff's additional authority is *Rackemann v. LISNR*, *Inc.*, No. 17-cv-00624-TWP-MJD, 2017 WL 4340349 (S.D. Ind. Sept. 29, 2017). The plaintiff in that case is represented by Plaintiff's counsel in this case. The defendants are the Indianapolis Colts, Inc., LISNR, Inc. and Adept Mobile, LLC. The allegations against each of those defendants are similar to the allegations against the Warriors, Signal 360, and Yinzcam, respectively, in this case. (See Rackemann v. LISNR, Inc., No. 17-cv-00624, Dkt. No. 1, Complaint.)

The Rackemann court denied the defendants' motion to dismiss. As to Adept Mobile, the court found the allegations sufficient to state an interception claim, reasoning that "[o]ther courts have concluded (at least at the motion to dismiss stage) that allegations of defendants working in concert or participating in the interception of communications can suffice to state a claim." Id., 2017 WL 4340349, at *8. To the extent the court's decision to deny the motion to dismiss is premised on a conclusion that such a theory is viable, the Court respectfully disagrees for the reasons set forth above and in its prior order. Satchell, 234 F. Supp. 3d at 1007-08.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

The Wiretap Act defines intercept to mean "the aural or other acquisition of the contents of any ... oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The Ninth Circuit has construed the term intercept to mean that one must "actually [acquire] the contents of a communication[.]" United States v. Smith, 155 F.3d 1051, 1058 (9th Cir. 1998) (emphasis in original). In *Smith*, the court noted the ordinary meaning of the term "acquire" is "the act of acquiring or coming into possession of" something. 155 F.3d at 1055 n.7 (citing Webster's Third New International Dictionary 18-19 (1986)); accord Webster's New Collegiate Dictionary (1979) at 10-11 (defining acquire to mean "to come into possession or control of often by unspecified means" and "acquisition" as "the act of acquiring"). Subsequently, the Ninth Circuit held that "acquisition occurs 'when the contents of a wire communication are captured or redirected in any way." Noel v. Hall, 568 F.3d 743, 749 (9th Cir. 2009) (quoting United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992)).7

The Court previously found Plaintiff's allegations that the App used a microphone on a smartphone, or other mobile device, to record surrounding audio, including conversations, were sufficient to show "capture" of the contents of an oral communication. It also concluded, contrary to Plaintiff's arguments, that the term "acquire' requires some measure of possession or control over the contents of any oral communications that are 'captured.'" Satchell, 234 F. Supp. 3d at 1007. Using that definition of acquire, the Court found Plaintiff's allegations were sufficient to show Signal360 engaged in interception but were not sufficient to show the Warriors or Yinzcam had done so. *Id.* at 1007-08.8

In Smith, the court held the ordinary meaning of the term "acquisition" was broad enough to encompass the act of retrieving and recording a voicemail message from a company's voicemail system. 155 F.3d at 1055 n.7, 1059. That conclusion was based on a definition of "wire communication" that included communications held in electronic storage. Id. at 1055. Congress subsequently amended the Wiretap Act to "eliminate[e] storage from the definition of wire communication." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002). In order for a wire communication to be intercepted, "it must be acquired during transmission, not while it is in electronic storage." *Id.* In other words, interception requires "acquisition contemporaneous with transmission[.]" Id.; see also id. (noting that "ordinary meaning of 'intercept" ... "is 'to stop, seize, or interrupt in progress or course before arrival') (quoting Webster's Ninth New Collegiate Dictionary 630 (1985)).

The Court stated that, "[a]t the pleadings phase, the Court [finds] the allegations regarding the manner in which Signal360 designed its beacon technology are sufficient to allege that

1. Plaintiff States an Interception Claim Against Signal360 and the Warriors.

Plaintiff alleges that Signal360's software records "all audio at all times – which would necessarily include users' private conversations – and then (ii) analyzes[s] that recorded audio for beacon tones." (FAC ¶ 7; see also id. (the software is a "'bug' designed for mobile devices").) Plaintiff further alleges that the "Bug" "temporarily recorded audio and retained portions of the audio for further analysis." (FAC ¶ 42.) According to Plaintiff, when a beacon is detected, the bug can send "that information" to Signal360 and the Warriors "through Signal360 [sic] content management system." (FAC ¶ 9; see also id. ¶ 43.) Similarly, Plaintiff alleges that once the App is installed and open, Signal360 programmed certain commands that permitted the "Bug" to communicate with Signal360's servers, and she alleges that Signal360 and the Warriors had "access to the data generated by the Bug and the Warriors App." (¶¶ 41-45, & Fig. 6 (emphasis added), 66.)

For the reasons set forth in its previous Order, the Court finds Plaintiff alleges facts to show Signal360 engaged in acts that would qualify as interception under the Wiretap Act. *Satchell*, 234 F. Supp. 3d at 1008. The Court also finds the Plaintiff's allegations that the Warriors had access to information generated by the Bug and the App is, at this stage, sufficient to show interception as to the Warriors. *Cf. Amati v. City of Woodstock Illinois*, 829 F. Supp. 998, 1008 (N.D. Ill. 1993) ("If a wiretap is placed on an individual's telephone and the conversation is recorded yet never listened to, the individual's conversations would be chilled if he knew of the wiretap. This would be so even if the individual was assured no one would listen to his conversations, because the individual's privacy interests are no longer autonomous. Rather, his privacy interests are subject to another's power.").

The Court previously found Plaintiff had not alleged sufficient facts to show Signal360

Signal360 'intercepted,' *i.e.* it acquired the contents of, Plaintiff's communications." *Satchell*, 234 F. Supp. 3d at 1007-08. The Court did not intend to suggest it found Plaintiff could state a claim based solely on "design" or to suggest Plaintiff could state a claim under Section 2512 of the Wiretap Act. It simply found the allegations sufficient to reasonably infer Signal360 had the requisite control over the oral communications and, thus, had actually acquired them. Thus, the facts were sufficient to show Signal360 engaged in acts that would qualify as interception.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

intercepted an oral communication. 234 F. Supp. 3d at 1008. Plaintiff has cured those defects in her FAC. Specifically, Plaintiff cites at least four instances where she had her phone with her, the App was running, and she had conversations about private matters, including non-public information during a business meeting and private financial matters. (FAC ¶ 49.)

Accordingly, the Court DENIES, IN PART, the motion to dismiss. Plaintiff may proceed on her claims against Signal360 and the Warriors.⁹

2. Plaintiff Fails to Allege Yinzcam Intercepted an Oral Communication.

Yinzcam argues Plaintiff still fails to state a claim against it. The Court agrees. In *In re* Carrier IQ, the plaintiffs asserted a claim for violations of the Wiretap Act against a software developer, Carrier, IO, Inc., and various manufacturers of mobile devices. The plaintiffs alleged Carrier IQ represented that the software was a "'network diagnostics tool' for cell phone service providers" but "in reality" it "collect[ed], and transfer[red], sensitive personal data off of a user's mobile device." 78 F. Supp. 3d at 1061. Although the plaintiffs in *In re Carrier IQ* did allege sufficient facts to show the manufacturers were involved in the installation of the software, there were no allegations that those manufacturers "'seized' or 'redirected' any communications themselves." Id.

Here, Plaintiff alleges that Yinzcam integrated Signal 360's source code into the App and "programmed" the App to ask for permission use a device's microphone and to "instantly initiate" the Bug once the App was installed and opened." (FAC ¶ 31, & Fig. 3, 41, 67.) Plaintiff also alleges that Yinzcam "conducted testing to ensure the Bug would cause user's microphones to turn on and begin listening," and that it "could have conducted 'alpha and beta tests' of the Warriors App with the Bug to conduct testing." (FAC ¶ 67.) The Court concludes these allegations are not sufficient to show Yinzcam intercepted one of Plaintiff's oral communications.

The Rackemann court denied the motion to dismiss as to Yinzcam's counterpart, Adept Mobile. Rackemann, 2017 WL 4340349, at *8. The plaintiff in Rackemann provided more details

Because the Court finds Plaintiff states a claim against the Warriors based on interception, it does not reach Plaintiff's alternative theory that the Warriors could be liable for procuring an interception.

Northern District of California

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

about how the Indianapolis Colts' app functions and alleged that Adept Mobile provided the rules that dictated when microphones should be activated. (*Rackemann* Complaint ¶¶ 31-32.) In contrast, in this case, the Warriors and Signal360 are alleged to have created the applicable rules. (FAC ¶¶ 41-42.) Therefore, the Court finds the allegations against Yinzcam are distinguishable from the allegations against Adept Mobile, and it declines to follow Rackemann for that reason as well.

In sum, the Court finds the allegations in Yinzcam in this case are analogous to the allegations relating to the mobile device manufacturers in *In re Carrier IQ*: the allegations are not sufficient to show Yinzcam itself "acquired the contents of any communications, as opposed to merely providing an avenue through which" Signal 360 and the Warriors "were able to effectuate such an interception." In re Carrier IQ, 78 F. Supp. 3d at 1089. Accordingly, the Court GRANTS, IN PART, Yinzcam's motion on this basis.

Plaintiff also alleges that the Yinzcam is liable for procuring an interception. (FAC ¶¶ 78-79.) Yinzcam argues that Section 2520 does not provide a private right of action for claims based on procurement. The Court need not reach that issue, because the Court agrees with Yinzcam that the facts alleged are insufficient to state a claim for procuring an interception. The term "procure" is commonly understood to mean "to obtain (something) ... by special effort or means" or "[t]o achieve or bring about (a result)." Black's Law Dictionary at 1401 (10th ed. 2014); see also Flowers v. Tandy Corp., 773 F.2d 585, 590 (4th Cir. 1985) ("'Procure' is generally understood to mean actively bringing about, causing or instigating something to be done."). A "procurer" is understood to mean "[s]omeone who induces or prevails on another to do something[.]" Black's Law Dictionary at 1401 (emphasis added).

Here, Plaintiff alleges that Yinzcam "procured Signal360 to implement and use the Bug as part of the scheme to implement beacon technology (which [it] knew would necessarily involve the recording of consumers' conversations)" and "procured the Bug from Signal360 as part of the scheme to implement beacon technology[.]" (FAC ¶¶ 78-79.) In support, Plaintiff "incorporates by reference" all prior allegations (id. \P 72), including allegations that Yinzcam acted at the direction of Signal360 and/or the Warriors. (FAC ¶¶ 8, 41). Those specific allegations directly

contradict the general allegations that Yinzcam procured the alleged violations. *See*, *e.g.*, *Valentine v. Wide Open West Finance*, *LLC*, 288 F.R.D. 407, 412 n.3 (N.D. Ill. 2012) ("[T]he procurer of a violation – the one who brings about the violation – is not secondarily liable as that term is usually understood; the procurer is the *principal*, not merely the secondary actor.").

Accordingly, the Court GRANTS Yinzcam's motion to dismiss on this basis as well.

C. Amendment.

At the hearing, the Court asked Plaintiff what facts she could allege to show that Yinzcam actually procured one of the other Defendants to intercept her communications and what additional facts she might be able to allege if the Court were to find the allegations in the FAC insufficient to state a claim. Plaintiff acknowledged that most of the facts were in the record but stated that it might be possible to allege that Yinzcam could have enlisted Signal360 to create the Bug. (See Dkt. No. 85, Transcript of Hearing at 37:4-23, 39:2-5, 39:11-40:11.) Having considered Plaintiff's representations at the hearing, and her theory of the case, the Court concludes that any further amendments relating to Yinzcam would be futile. Accordingly, the Court dismisses the claims asserted against Yinzcam with prejudice.

CONCLUSION

For the foregoing reasons, the Court GRANTS, IN PART, AND DENIES, IN PART, the motion to dismiss. The claims shall proceed as to Signal360 and the Warriors. Signal360 and the Warriors shall file their answer by no later than December 8, 2017, and the parties shall appear on January 12, 2018 at 11:00 a.m. for the initial case management conference. The parties shall file a joint case management conference statement by no later than January 5, 2018.

IT IS SO ORDERED.

Dated: November 20, 2017

JEFFREY S. WHITE United States District Judge