

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

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
OAKLAND DIVISION

SUNBELT RENTALS, INC.,

Plaintiff,

vs.

SANTIAGO VICTOR,

Defendant.

Case No: C 13-4240 SBA

**ORDER GRANTING PLAINTIFF'S  
MOTION TO DISMISS  
DEFENDANT'S  
COUNTERCLAIMS**

Dkt. 39

Sunbelt Rentals, Inc. ("Plaintiff" or "Sunbelt") filed the instant action against its former employee, Santiago Victor ("Defendant" or "Victor"), alleging that he misappropriated trade secrets upon his termination. Victor has filed five counterclaims against Sunbelt, accusing it, inter alia, of violating the federal Wiretap Act and the Stored Communications Act ("SCA") by reviewing his text messages on the iPhone which Sunbelt had previously issued to him. The parties are presently before the Court on Plaintiff's Motion to Dismiss Defendants Counterclaims. Having read and considered the papers filed in connection with this matter and being fully informed, the Court hereby GRANTS the motion and dismisses Victor's counterclaims, with leave to amend. The Court, in its discretion, finds this matter suitable for resolution without oral argument. Fed. R. Civ. P. 78(b); N.D. Cal. Civ. L.R. 7-1(b).

1 **I. BACKGROUND**

2 **A. RELEVANT FACTS**

3 During the relevant time period, Victor worked as an outside sales representative for  
4 Sunbelt, an equipment rental company. Countercl. ¶ 11, Dkt. 34. In August 2013, Victor  
5 gave his two-week notice to Sunbelt, stating that he had taken a job with one of its  
6 competitors—Ahern Rentals (“Ahern”). Id. ¶ 16. Upon learning of Victor’s intent to leave  
7 the company, Sunbelt immediately dismissed him. Id.

8 During his time with Sunbelt, Victor was assigned a Sunbelt-owned iPhone  
9 (“Sunbelt iPhone”) and a Sunbelt-owned iPad for both work and personal purposes. Id.  
10 ¶¶ 12-14. Thereafter, Victor “created and paid for a personal ‘Apple account’ that was  
11 linked to both devices.” Id. ¶ 15. Victor returned the devices to Sunbelt after his  
12 separation. Id. ¶¶ 16, 18, 20.

13 Victor’s new employer, Ahern, provided him a new iPhone (“Ahern iPhone”). Id.  
14 ¶¶ 19-20. At some point thereafter, Victor registered or linked his Ahern iPhone to the same  
15 personal Apple account he had previously used while at Sunbelt. Id. ¶ 19. This process  
16 “synced” Victor’s Ahern iPhone with his personal Apple account. Id.

17 Several weeks later, when he received a new iPad from Ahern (“Ahern iPad”),  
18 Victor linked the new iPad to his personal Apple account. Id. ¶ 20. In the process of  
19 registering the Ahern iPad, Victor discovered the telephone number associated with the  
20 Sunbelt iPhone was still linked to his personal Apple account. Id. Because Victor had  
21 failed to unlink the Sunbelt iPhone from his account, his “private electronic data and  
22 electronic messages,” including text messages sent to and from his Ahern iPhone, also were  
23 transmitted to the Sunbelt iPhone which he had returned to Sunbelt. Id. ¶ 20, 21. Victor  
24 then deleted the Sunbelt number from his account “to ensure that his new Ahern issued  
25 Apple products were not in any way linked to Sunbelt.” Id.

26 Victor claims that after his departure, Sunbelt “began actively investigating Victor’s  
27 post-employment acts, conduct, and communications.” Id. ¶ 21. In the course of such  
28 investigation, Sunbelt allegedly “invaded Victor’s privacy rights by *accessing*,

1 *intercepting, monitoring, reviewing, storing and using* Victor’s post-employment private  
2 electronic data and electronic communications (including but not limited to *text messages*  
3 sent and received from Victor’s Ahern, Rentals Inc. issued iPhone) without authority,  
4 permission, or consent.” *Id.* (emphasis added). Victor further accuses Sunbelt of  
5 “*intentionally accessing* Victor’s private electronic communications and data, without  
6 authorization, from facilities through which Victor’s electronic communications were  
7 provided and stored (i.e., Victor’s cellular phone provider’s network which stores Victor’s  
8 electronic communications, and or Apple’s cloud based network where Victor’s electronic  
9 communication pertaining to his Apple Account are processed and stored) and where such  
10 services and communications were restricted to access by Victor, which Sunbelt obtained  
11 through improper means.” *Id.* ¶ 23 (emphasis added). No particular facts are alleged to  
12 support these assertions.

### 13 **B. PROCEDURAL HISTORY**

14 On September 12, 2013, Sunbelt filed a complaint against Victor in this Court  
15 alleging four state law causes of action: (1) breach of contract; (2) misappropriation of trade  
16 secrets; (3) unfair competition; and (4) breach of duty of loyalty. Dkt. 1. Victor then filed  
17 an Answer, and later amended an Answer and Counterclaim. The gist of the Counterclaim  
18 is that Sunbelt improperly read the text messages that were inadvertently transmitted to his  
19 Sunbelt iPhone. He alleges claims for violations of: (1) the Wiretap Act; (2) the SCA; (3)  
20 California Penal Code § 502 et seq.; (4) California Penal Code § 630 et seq.; and (5) his  
21 right to privacy. *See* Countercl. ¶ 24. Each of these claims is based on the same set of  
22 facts—Sunbelt’s purported interception, acquisition and use of Victor’s electronic  
23 communications (i.e., text messages) sent to and from his Ahern iPhone. Sunbelt now  
24 moves to dismiss all counterclaims. This matter has been fully briefed and is ripe for  
25 adjudication.

### 26 **II. LEGAL STANDARD**

27 Pleadings in federal court actions are governed by Federal Rule of Civil Procedure  
28 8(a)(2), which requires only “a short and plain statement of the claim showing that the

1 pleader is entitled to relief.” Rule 12(b)(6) “tests the legal sufficiency of a claim.” Navarro  
2 v. Block, 250 F.3d 729, 732 (9th Cir. 2001). A complaint may be dismissed under Rule  
3 12(b)(6) for either failure to state a cognizable legal theory or insufficient facts to support a  
4 cognizable legal theory. Mendondo v. Centinela Hosp. Med. Ctr., 521 F.3d 1097, 1104  
5 (9th Cir. 2008). “[C]ourts must consider the complaint in its entirety, as well as other  
6 sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in  
7 particular, documents incorporated into the complaint by reference, and matters of which a  
8 court may take judicial notice.” Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308,  
9 322 (2007). The court is to “accept all factual allegations in the complaint as true and  
10 construe the pleadings in the light most favorable to the nonmoving party.” Outdoor Media  
11 Group, Inc. v. City of Beaumont, 506 F.3d 895, 899-900 (9th Cir. 2007).

12 To survive a motion to dismiss, “a complaint must contain sufficient factual matter,  
13 accepted as true, to ‘state a claim to relief that is plausible on its face.’” Ashcroft v. Iqbal,  
14 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)).  
15 The complaint must afford the defendants with “fair notice” of the claims against them, and  
16 the grounds upon which the claims are based. Swierkiewicz v. Sorema N.A., 534 U.S. 506,  
17 512 (2002). “Threadbare recitals of the elements of a cause of action, supported by mere  
18 conclusory statements, do not suffice.” Iqbal, 556 U.S. at 678. When a complaint or claim  
19 is dismissed, “[l]eave to amend should be granted unless the district court determines that  
20 the pleading could not possibly be cured by the allegation of other facts.” Knappenberger  
21 v. City of Phoenix, 566 F.3d 936, 942 (9th Cir. 2009).

### 22 **III. DISCUSSION**

#### 23 **A. WIRETAP ACT**

24 The Wiretap Act imposes civil liability against any person who “*intentionally*  
25 *intercepts*, endeavors to intercept, or procures any other person to intercept or endeavor to  
26 intercept, any wire, oral, or electronic communication.” 18 U.S.C §§ 2511(1)(a) (emphasis  
27 added); *id.* § 2520(a). The Act defines “intercept” as “the aural or other acquisition of the  
28 contents of any wire, electronic, or oral communication through the use of any electronic,

1 mechanical, or other device.” 18 U.S.C. § 2510(4). “Such acquisition occurs ‘when the  
2 contents of a wire communication are captured or redirected in any way.’” Noel v. Hall,  
3 568 F.3d 743, 749 (9th Cir. 2009). The inception must be intentional, as opposed to  
4 inadvertent. See Sanders v. Robert Bosch Corp., 38 F.3d 736, 742-43 (4th Cir. 1994).

5 Here, Victor has failed to allege facts sufficient to establish that Sunbelt  
6 “intentionally intercepted” any of his text messages. By Victor’s own account, the text  
7 messages appeared on his Sunbelt iPhone as a result of Victor’s act of syncing his new  
8 iPhone to his Apple account without first un-linking his Sunbelt iPhone. Countercl. ¶¶ 19,  
9 20. In other words, Sunbelt did not intentionally capture or redirect Victor’s text messages  
10 to the Sunbelt iPhone—the transmission of those messages was entirely Victor’s doing.  
11 Given these circumstances, the requisite intentional conduct is lacking. Sanders, 38 F.3d at  
12 742-43; Shubert v. Metrophone, Inc., 898 F.2d 401, 405 (3rd Cir. 1990) (noting that  
13 Congress specifically intended that “inadvertent interceptions are not crimes under [the  
14 Wiretap Act]”).

15 Nor has Victor alleged facts sufficient to establish that Sunbelt acted to “intercept”  
16 the text messages or any other electronic communications. The Ninth Circuit applies a  
17 “narrow definition of ‘intercept.’” Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878  
18 (9th Cir. 2002). For a communication to be intercepted, “it must be acquired during  
19 transmission, not while it is in electronic storage.” Id. Though Victor vaguely alleges that  
20 Sunbelt intercepted his electronic communications, i.e., his text messages, he provides no  
21 facts to support this otherwise conclusory assertion.<sup>1</sup> If anything, the pleadings suggest that  
22 Sunbelt read Victor’s text messages *after* they were sent and received on the Sunbelt  
23 iPhone, which is insufficient to demonstrate intentional interception under the Wiretap Act.  
24 See NovelPoster v. Javitch Canfield Group, No. C 13-5186 WHO, 2014 WL 3845148, \*10  
25 (N.D. Cal. Aug. 14, 2014) (reading emails that have already been received in an email

26 \_\_\_\_\_  
27 <sup>1</sup> Victor’s Counterclaim repeatedly makes vague and formulaic references to  
28 “private and electronic communications,” but only specifically identifies “text messages” as  
having been allegedly intercepted. See Countercl. ¶ 22. Victor never specifies how the  
alleged interception transpired.

1 account's inbox does not constitute interception under the Wiretap Act because the  
2 transmission had already occurred).

3         Although it is clear that Victor's Wiretap Act claim must be dismissed, what is less  
4 clear is whether leave to amend should be granted. Given the almost instantaneous  
5 transmission of text messages, the window during which an interception may occur is  
6 exceedingly narrow. NovelPoster, 2014 WL 3845148, \*10 (citing United States v. Steiger,  
7 318 F.3d 1039, 1050 (11th Cir. 2003)). Thus, "unless some type of automatic routing  
8 software is used" to divert the text message, interception of [a text message] within the  
9 prohibition of the Wiretap Act is virtually impossible." Id. (internal quotations and citation  
10 omitted). Given these constraints, it is doubtful that Victor will be able to allege facts,  
11 consistent with Federal Rule of Civil Procedure 11, to state a claim for violation of the  
12 Wiretap Act. Nonetheless, the Court will afford Victor an opportunity to amend this claim  
13 and therefore DISMISSES his claim under the Wiretap Act, with leave to amend.<sup>2</sup>

#### 14         **B.         STORED COMMUNICATIONS ACT**

15         The SCA creates "a cause of action against anyone who "intentionally accesses  
16 without authorization a facility through which an electronic communication service is  
17 provided . . . and thereby obtains, alters, or prevents authorized access to a wire or  
18 electronic communication while it is in electronic storage.'" Theofel v. Farey-Jones, 359  
19 F.3d 1066, 1072 (9th Cir. 2004) (quoting 18 U.S.C. §§ 2701(a)(1), 2707(a)). "[E]lectronic  
20 storage" is defined as either "temporary, intermediate storage . . . incidental to . . .  
21 electronic transmission," or "storage . . . for purposes of backup protection." 28 U.S.C.  
22 § 2510(17).

23         According to Victor, Sunbelt violated the SCA by virtue of having,

24                 Intentionally accessed, without authorization, facilities through  
25                 which Victor's electronic communications were provided and  
26                 stored (i.e., Victor's cellular phone provider's network which  
                    stores Victor's electronic communications, and or Apple's

---

27         <sup>2</sup> Sunbelt also contends that Victor has failed to allege any facts showing that it  
28 intercepted his text messages "through the use of any . . . device." 18 U.S.C. § 2510(4)  
(emphasis added). Since it is clear that the Counterclaim fails to allege intentional  
interception, the Court need not reach that issue at this juncture.

1 cloud based network where Victor’s electronic communication  
2 pertaining to his Apple Account are processed and stored) and  
3 where such services and communications were restricted to  
access by Victor, which Sunbelt obtained through improper  
means.

4 Countercl. ¶ 45. No facts are presented, however, to support the conclusory assertion that  
5 Sunbelt *accessed* Victor’s text messages through his cellular telephone provider or Apple’s  
6 network. Moreover, in his opposition, Victor contradicts himself by stating that the text  
7 messages allegedly accessed by Sunbelt “were *not* accessed through, nor stored on a  
8 website.” Opp’n at 4 (emphasis added). To the extent that Victor is claiming that Sunbelt  
9 accessed his text messages by reviewing the messages on his Sunbelt iPhone—as he does  
10 elsewhere in his Counterclaim, such conduct does not violate the SCA. See Garcia v. City  
11 of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012) (holding that text messages and pictures  
12 stored on a cellular telephone do not constitute “electronic storage” for purposes of the  
13 SCA). This claim is DISMISSED with leave to amend.

14 **C. CALIFORNIA PENAL CODE § 502**

15 Section 502 of the California Penal Code prohibits unauthorized access to  
16 computers, computer systems, and computer networks, and provides for a civil remedy in  
17 the form of compensatory damages, injunctive relief, and other equitable relief. Cal. Penal  
18 Code § 502. Section 502 is an anti-hacking statute intended to prohibit the unauthorized  
19 use of any computer system for improper or illegitimate purpose. Yee v. Lin, No. C 12-  
20 02474 WHA, 2012 WL 4343778, \*2 (N.D. Cal. Sept. 20, 2012).

21 Victor alleges that Sunbelt violated subsections (c)(1), (2), (3), (4), (6), and (7) of  
22 Section 502, which provides that a person is liable if he:

23 (1) Knowingly accesses and without permission alters,  
24 damages, deletes, destroys, or otherwise uses any data,  
25 computer, computer system, or computer network in order to  
either (A) devise or execute any scheme or artifice to defraud,  
deceive, or extort, or (B) wrongfully control or obtain money,  
property, or data.

26 (2) Knowingly accesses and without permission takes, copies,  
27 or makes use of any data from a computer, computer system, or  
28 computer network, or takes or copies any supporting  
documentation, whether existing or residing internal or external  
to a computer, computer system, or computer network.

1 (3) Knowingly and without permission uses or causes to be  
used computer services.

2 (4) Knowingly accesses and without permission adds, alters,  
3 damages, deletes, or destroys any data, computer software, or  
4 computer programs which reside or exist internal or external to  
a computer, computer system, or computer network.

5 . . .

6 (6) Knowingly and without permission provides or assists in  
7 providing a means of accessing a computer, computer system,  
8 or computer network in violation of this section.

9 (7) Knowingly and without permission accesses or causes to be  
accessed any computer, computer system, or computer network.”

10 Id. § 502(c); Countercl. ¶ 54. For purposes of Section 502, parties act “without permission”  
11 when they “circumvent[ ] technical or code-based barriers in place to restrict or bar a user’s  
12 access.” Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1036 (N.D. Cal.  
2012).

13 In his third Counterclaim, Victor alleges as follows:

14 On information and belief, Sunbelt violated California Penal  
15 Code section 502 when it improperly began accessing,  
16 intercepting, monitoring, reviewing and using Victor’s post-  
17 employment private electronic data and electronic  
18 communications without Victor’s knowledge, authorization or  
19 consent. On information and belief, Sunbelt additionally, or in  
20 the alternative, violated of Penal Code § 502 ***by intentionally***  
21 ***accessing, without authorization***, facilities through which  
22 Victor’s electronic communications were provided and stored  
(i.e., Victor’s cellular phone provider’s network which stores  
Victor’s electronic communications, and or Apple’s cloud  
based network where Victor’s electronic communication  
pertaining to his Apple Account are processed and stored)  
and where such services and communications were restricted to  
access by Victor, which Sunbelt obtained through improper  
means.

23 Countercl. ¶ 56 (emphasis added). These fact-barren and vague allegations are precisely  
24 the type of “threadbare recitals” proscribed by Twombly and Iqbal. Moreover, to the extent  
25 that Victor is claiming that Sunbelt accessed his unspecified “private electronic data and  
26 electronic communications” through the Apple account or his cellular telephone provider’s  
27 computer network, such a claim fails on the ground that no facts are alleged showing that  
28 Sunbelt did so by circumventing technical or code-based barriers intended to restrict such



1 access. Facebook, 844 F. Supp. 2d at 1036. To the contrary, Victor simply avers that  
2 Sunbelt reviewed his text messages that he caused, albeit inadvertently, to be sent to the  
3 Sunbelt iPhone. The Court therefore concludes that Victor has failed to state a claim under  
4 Section 502 and DISMISSES said claim with leave to amend.

5 **D. CALIFORNIA PENAL CODE § 630**

6 The California Invasion of Privacy Act (“CIPA”) is intended to prevent privacy  
7 invasions facilitated by modern technology and devices. Cal. Penal Code § 630. “The  
8 analysis for a violation of CIPA is the same as that under the federal Wiretap Act.”  
9 NovelPoster, 2014 WL 3845148, \*12 (granting judgment on pleadings on CIPA claim for  
10 same reasons underlying the dismissal of the plaintiff’s Wiretap Act claim, i.e., the lack of  
11 intentional interception). As discussed, Victor has failed to plausibly allege a violation of  
12 the Wiretap Act; *a fortiori*, he is also unable to allege a violation of CIPA. This claim is  
13 DISMISSED with leave to amend.

14 **E. INVASION OF PRIVACY**

15 California recognizes four categories of the tort of invasion of privacy: (1) intrusion  
16 upon seclusion; (2) public disclosure of private facts; (3) false light in the public eye; and  
17 (4) appropriation of name or likeness. Shulman v. Group W Prods., Inc., 18 Cal.4th 200,  
18 214 n. 4 (1998). Victor fails to indicate which type of invasion of privacy claim he is  
19 alleging. Nonetheless, based on the sparse allegations presented, it appears that he is  
20 attempting to state a claim for intrusion upon seclusion.

21 “A privacy violation based on the common law tort of intrusion has two elements.  
22 First, the defendant must intentionally intrude into a place, conversation, or matter as to  
23 which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must  
24 occur in a manner highly offensive to a reasonable person.” Hernandez v. Hillside, Inc.,  
25 47 Cal.4th 272, 285 (2009). “The tort is proven only if the plaintiff had an objectively  
26 reasonable expectation of seclusion or solitude in the place, conversation or data source.”  
27 Shulman v. Grp. W Prods., Inc., 18 Cal.4th 200, 232 (1998). A plaintiff pursuing an  
28 invasion of privacy action must have conducted himself or herself in a manner consistent

1 with an actual expectation of privacy, i.e., he or she must not have engaged in conduct  
2 which manifests a voluntary consent to the invasive actions of defendant. Hill v. Nat'l  
3 Collegiate Athletic Ass'n, 7 Cal.4th 1, 26 (1994).

4 Victor contends that, as a matter of law, an employee has a reasonable expectation of  
5 privacy with respect to text messages contained on employer-owned mobile telephones.  
6 The decisional authorities cited by Victor, however, are inapposite. In City of Ontario v.  
7 Quon, 560 U.S. 746 (2010), a police officer was issued a pager by his police department  
8 which was subject to a limit on the number of characters that could be sent and received  
9 each month. Id. at 750. After becoming concerned that the officer was repeatedly  
10 exceeding his character limit, the police department obtained transcripts of the text  
11 messages from the wireless carrier to ascertain whether the texts were work-related or  
12 personal. Id. at 750-51. After finding that most of the text messages were not work-  
13 related, the police department took disciplinary action against the officer. Id. at 753. The  
14 police officer then brought an action under 42 U.S.C. § 1983 against the city, police  
15 department and police chief, alleging that the police department's review of his text  
16 messages violated the Fourth Amendment.

17 In the addressing the plaintiff's Fourth Amendment claim, the United States  
18 Supreme Court *assumed, without deciding*, that the plaintiff had a reasonable expectation  
19 of privacy in text messages sent to him on an employer-provided pager; however, the Court  
20 ultimately upheld the police department's review of those messages as reasonable under the  
21 Fourth Amendment. Id. at 760. Despite Victor's suggestion to the contrary, the Supreme  
22 Court did not hold that an employee automatically has an expectation of privacy in  
23 electronic messages stored on a device provided by his employer. Quon also is  
24 distinguishable on its facts. Unlike the police officer in Quon, Victor was no longer an  
25 employee of the company that owned the electronic device at issue at the time the invasion  
26 of privacy allegedly occurred. Moreover, unlike the police department, which requested  
27 transcripts of the text messages from the wireless carrier, Sunbelt is not alleged to have  
28 affirmatively undertaken any action to obtain and review the text messages or any other

1 electronic data. Rather, the electronic communications appeared on Sunbelt’s iPhone  
2 because of actions taken by Victor.

3 Victor’s citation to United States v. Finley, 477 F.3d 250 (5th Cir. 2007) fares no  
4 better. In that case, a criminal defendant challenged the denial of his motion to suppress  
5 text messages and call records which law enforcement officials had obtained through a  
6 warrantless search of his employer-issued cell phone. In addressing the threshold issue of  
7 whether the defendant had standing to raise a Fourth Amendment challenge, the Fifth  
8 Circuit held that the mere fact that the employer owned the phone and had access to its  
9 contents did not ipso facto demonstrate that defendant correspondingly had no expectation  
10 of privacy in his call records and text messages. Id. at 259. In reaching its decision, the  
11 court specifically noted that the defendant had undertaken precautions to maintain the  
12 privacy of data stored on his phone and that he “had a right to exclude others from using the  
13 phone.” Id. Unlike the defendant in Finley, Victor was no longer an employee of the  
14 company which owned the cell phone to which the subject text messages had been sent. In  
15 addition, Victor had no right to exclude others from accessing the Sunbelt iPhone—which  
16 he did not own or possess and no longer had any right to access. Moreover, rather than  
17 undertake precautions to maintain the privacy of his text messages, Victor did just the  
18 opposite by failing to unlink his Sunbelt iPhone from his Apple account, which, in turn,  
19 facilitated the transmission of those messages to an iPhone exclusively owned, controlled  
20 and possessed by his former employer.

21 Victor’s privacy claim also fails on the ground that he has failed to show an  
22 intrusion into a “place, conversation, or matter as to which the plaintiff has a reasonable  
23 expectation of privacy.” Hernandez, 47 Cal.4th at 285. As noted, Victor cannot  
24 legitimately claim an expectation of privacy in a “place,” i.e., the Sunbelt iPhone, which  
25 belongs to his former employer and to which he has no right to access. Nor can Victor  
26 claim a reasonable expectation of privacy with respect to his text messages, in general. The  
27 pleadings do not identify the contents of any particular text messages, and instead, refer  
28 generally to “private electronic data and electronic communications.” Countercl. ¶ 79.

1 This and other courts have concluded that there is no “legally protected privacy interest and  
2 reasonable expectation of privacy” in electronic messages, “in general.” In re Yahoo Mail  
3 Litig., -- F. Supp. 2d --, 2014 WL 3962824, \*16 (N.D. Cal. Aug. 12, 2014) (citing cases).<sup>3</sup>  
4 Rather, a privacy interest can exist, if at all, only with respect to the *content* of those  
5 communications. In any event, even if Victor were claiming an expectation of privacy with  
6 respect to the specific content of his text messages (which he has not specified), the facts  
7 alleged demonstrate that he failed to comport himself in a manner consistent with an  
8 objectively reasonable expectation of privacy. By his own admission, Victor personally  
9 caused the transmission of his text messages to the *Sunbelt* iPhone by syncing his new  
10 devices to his Apple account without first unlinking his Sunbelt iPhone.<sup>4</sup> As such, even if  
11 he *subjectively* harbored an expectation of privacy in his text messages, such expectation  
12 cannot be characterized as *objectively* reasonable, since it was *Victor’s* conduct that directly  
13 caused the transmission of his text messages to Sunbelt in the first instance. See Hill,  
14 7 Cal.4th at 26.

15 The above notwithstanding, the facts alleged in Victor’s fifth counterclaim are  
16 insufficient to show that Sunbelt intruded into Victor’s privacy in a manner highly  
17 offensive to a reasonable person. “Actionable invasions of privacy must be sufficiently  
18 serious in their nature, scope, and actual or potential impact to constitute an egregious  
19 breach of the social norms underlying the privacy right.” Hill, 7 Cal. 4th at 37. In addition,  
20 the plaintiff must show “that the *use* of plaintiff’s information was highly offensive.”  
21 Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 993 (2011) (emphasis added)  
22 (upholding the demurrer to plaintiff’s common law invasion of privacy claim where,  
23

---

24 <sup>3</sup> Victor also does not specify whether his claim is predicated upon text messages  
25 sent by him, received by him, or both. With respect to messages he transmitted, there is  
26 authority finding that a plaintiff has no reasonable expectation of privacy in messages sent  
27 to third parties. See Fetsch v. City of Roseburg, No. 6:11-cv-6343-TC, 2012 WL 6742665,  
28 \*10 \*(D.Or. Dec. 31, 2012) (plaintiff had no expectation of privacy in text messages sent  
from his phone because relinquished control of them once they were transmitted).

<sup>4</sup> Victor vaguely alleges that Sunbelt intercepted his electronic communications. He  
provides no factual support for this conclusory assertion. See Countercl. ¶ 77.

1 finding that even if the customer addresses were obtained through “questionable” means,  
2 there was “no allegation that Lamps Plus used the address once obtained for an offensive or  
3 improper purpose.”).

4 Here, Victor alleges only that Sunbelt acted in a “highly offensive” manner by  
5 “accessing, intercepting, monitoring, reviewing, storing and using [his] post-employment  
6 private electronic data and electronic communications without [his] knowledge,  
7 authorization or consent as part of an unreasonably intrusive and unauthorized investigation  
8 into Victor’s post-employment conduct.” Countercl. ¶ 79. Victor offers no factual support  
9 for these conclusory assertions. In particular, he provides no details regarding the specific  
10 conduct by Sunbelt that amounts to “accessing, intercepting, monitoring, reviewing, storing  
11 and using [his] post-employment private electronic data and electronic communications.”

12 Id. He also fails to aver any facts to establish that Sunbelt’s use of the intercepted  
13 communications was highly offensive. See Folgelstrom, 195 Cal. App. 4th at 993. The  
14 possibility that Sunbelt may have reviewed text messages sent to a cell phone which it  
15 owned and controlled—without more—is insufficient to establish an offensive use. As  
16 with his other claims, Victor’s formulaic recitation of an invasion of privacy claim is  
17 inconsistent with the federal pleading requirements of Rule 8. This claim is DISMISSED  
18 with leave to amend.

19 **IV. CONCLUSION**

20 For the reasons stated above,

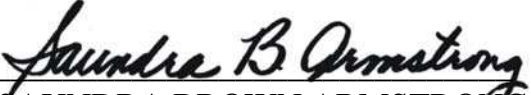
21 IT IS HEREBY ORDERED THAT:

- 22 1. Plaintiff’s Motion to Dismiss Defendants Counterclaims is GRANTED.
- 23 2. Defendant shall have twenty-one (21) days from the date this Order is filed to  
24 amend his counterclaims, consistent with the Court’s rulings. Defendant is warned that any  
25 factual allegations set forth in his amended pleading must be made in good faith and  
26 consistent with Rule 11. The failure to timely file the amended counterclaim and/or the  
27 failure to comply with this Order will result in the dismissal of all counterclaims with  
28 prejudice.

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

IT IS SO ORDERED.

Dated: August 28, 2014

  
SAUNDRA BROWN ARMSTRONG  
United States District Judge