GIBSON, DUNN & CRUTCHER LLP
JOSHUA A. JESSEN, SBN 222831
JJessen@gibsondunn.com
JEANA BISNAR MAUTE, SBN 290573
JBisnarMaute@gibsondunn.com
JESSICA S. OU, SBN 280534
JOu@gibsondunn.com
1881 Page Mill Road
Palo Alto, California 94304
Telephone: (650) 849-5300
Facsimile: (650) 849-5333

GIBSON, DUNN & CRUTCHER LLP
GAIL E. LEES, SBN 90363
GLees@gibsondunn.com
CHRISTOPHER CHORBA, SBN 216692
CChorba@gibsondunn.com
333 South Grand Avenue
Los Angeles, California 90071
Telephone: (213) 229-7000
Facsimile: (213) 229-7520

Attorneys for Defendant
FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISON

MATTHEW CAMPBELL, MICHAEL HURLEY, and DAVID SHADPOUR,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

Case No. C 13-05996 PJH

CONSOLIDATED CLASS ACTION

DEFENDANT FACEBOOK, INC.'S STATEMENT OF RECENT DECISION

HEARING:
Date: October 1, 2014
Time: 9:00 a.m.
Place: Courtroom 3, 3rd Floor
The Honorable Phyllis J. Hamilton

Pursuant to Civil Local Rule 7-3(d)(2), Defendant Facebook, Inc. respectfully submits this Statement of Recent Decision to bring to the Court's attention the Northern District of California's recent decision in *Sunbelt Rentals, Inc. v. Victor*, 4:13-cv-04240-SBA, 2014 WL 4274313 (N.D. Cal. Aug. 28, 2014), a true and correct copy of which is attached hereto as Exhibit A. The decision was filed the same day Facebook filed its Reply in Support of its Motion to Dismiss Plaintiffs' Consolidated Amended Complaint on August 28, 2014 (*see* Dkt. No. 35), and Facebook understands that the decision was published by Westlaw in early September. The decision is therefore appropriate for consideration by the Court. *See* Civil L.R. 7-3(d)(2) ("Before the noticed hearing date, counsel may bring to the Court's attention a relevant judicial opinion published after the date the opposition or reply was filed by filing and serving a Statement of Recent Decision, containing a citation to and providing a copy of the new opinion—without argument."). The *Sunbelt Rentals* decision is relevant to Plaintiffs' claim for alleged violation of the Wiretap Act (18 U.S.C. § 2511), specifically relating to the Act's requirement that a communication "must be acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-79 (9th Cir. 2002).

Dated: September 22, 2014

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: /s/
Joshua A. Jessen

Attorneys for Defendant FACEBOOK, INC.

Exhibit A

--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.)
(Cite as: 2014 WL 4274313 (N.D.Cal.))

H

Only the Westlaw citation is currently available.

United States District Court,
Oakland Division.
Oakland Division
Sunbelt Rentals, Inc., Plaintiff,
v.
Santiago Victor, Defendant.

Case No: C 13–4240 SBA
4:13–cv–04240Signed August 28, 2014

Joseph C. Wilson, Michelle Therese Duval, Richard James Curiale, Curiale Wilson LLP, Allison Marie Dibley, Esq., Joseph C. Wilson, V, Nossaman LLP, San Francisco, CA, Patricia Jeanne Hill, Yash B. Dave, Smith, Gambrell & Russell, LLP, Jacksonville, FL, Veronica Meryl Gray, Nossaman LLP, Irvine, CA, for Plaintiff.

Beth Ann Kahn, Kevin M. Pollack, Kurt Alan Dreibholz, Morris Polich Purdy, Los Angeles, CA, for Defendant.

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

Dkt. 39

SAUNDRA BROWN ARMSTRONG, United States District Judge

***1** 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).

I. *BACKGROUND*

A. RELEVANT FACTS

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

During his time with Sunbelt, Victor was assigned a Sunbelt-owned iPhone ("Sunbelt iPhone") and a Sunbelt-owned iPad for both work and personal purposes. *Id.* ¶¶ 12–14. Thereafter, Victor "created and paid for a personal 'Apple account' that was linked to both devices." *Id.* ¶ 15. Victor returned the devices to Sunbelt after his separation. *Id.* ¶¶ 16, 18, 20.

Victor's new employer, Ahern, provided him a new iPhone ("Ahern iPhone"). *Id.* ¶ 19–20. At some point thereafter, Victor registered or linked his Ahern iPhone to the same personal Apple account he had previously used while at Sunbelt. *Id.* ¶ 19. This process "synced" Victor's Ahern iPhone with his personal Apple account. *Id.*

Several weeks later, when he received a new iPad from Ahern ("Ahern iPad"), Victor linked the new iPad to his personal Apple account. *Id.* ¶ 20. In the process of registering the Ahern iPad, Victor discovered the telephone number associated with the Sunbelt iPhone was still linked to his personal Apple account. *Id.* Because Victor had failed to un-

link the Sunbelt iPhone from his account, his "private electronic data and electronic messages," including text messages sent to and from his Ahern iPhone, also were transmitted to the Sunbelt iPhone which he had returned to Sunbelt. *Id.* ¶ 20, 21. Victor then deleted the Sunbelt number from his account "to ensure that his new Ahern issued Apple products were not in any way linked to Sunbelt." *Id.*

Victor claims that after his departure, Sunbelt "began actively investigating Victor's post-employment acts, conduct, and communications." *Id.* ¶ 21. In the course of such investigation, Sunbelt allegedly "invaded Victor's privacy rights by ***accessing, intercepting, monitoring, reviewing, storing and using*** Victor's post-employment private electronic data and electronic communications (including but not limited to ***text messages*** sent and received from Victor's Ahern, Rentals Inc. issued iPhone) without authority, permission, or consent." *Id.* (emphasis added). Victor further accuses Sunbelt of " ***intentionally accessing*** Victor's private electronic communications and data, without authorization, from facilities through which 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." *Id.* ¶ 23 (emphasis added). No particular facts are alleged to support these assertions.

B. PROCEDURAL HISTORY

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

II. *LEGAL STANDARD*

Pleadings in federal court actions are governed by Federal Rule of Civil Procedure 8(a)(2), which requires only "a short and plain statement of the claim showing that the pleader is entitled to relief." Rule 12(b)(6) "tests the legal sufficiency of a claim." *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir.2001). A complaint may be dismissed under Rule 12(b)(6) for either failure to state a cognizable legal theory or insufficient facts to support a cognizable legal theory. *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir.2008). "[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322, 127 S.Ct. 2499, 168 L.Ed.2d 179 (2007). The court is to "accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Outdoor Media Group, Inc. v. City of Beaumont*, 506 F.3d 895, 899–900 (9th Cir.2007).

To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell*

Atl. Corp. v. Twombly, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). The complaint must afford the defendants with "fair notice" of the claims against them, and the grounds upon which the claims are based. *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 512, 122 S.Ct. 992, 152 L.Ed.2d 1 (2002). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. When a complaint or claim is dismissed, "[l]eave to amend should be granted unless the district court determines that the pleading could not possibly be cured by the allegation of other facts." *Knappenberger v. City of Phoenix*, 566 F.3d 936, 942 (9th Cir.2009).

III. *DISCUSSION*

A. WIRETAP ACT

The Wiretap Act imposes civil liability against any person who " ***intentionally intercepts,*** endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C §§ 2511(1)(a) (emphasis added); *id.* § 2520(a). The Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). "Such 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). The inception must be intentional, as opposed to inadvertent. *See Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742–43 (4th Cir.1994).

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

3** Nor has Victor alleged facts sufficient to establish that Sunbelt acted to "intercept" the text messages or any other electronic communications. The Ninth Circuit applies a "narrow definition of 'intercept.' " *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir.2002). For a communication to be intercepted, "it must be acquired during transmission, not while it is in electronic storage." *Id.* Though Victor vaguely alleges that Sunbelt intercepted his electronic communications, i.e., his text messages, he provides no facts to support this otherwise conclusory assertion.[FN1] If anything, the pleadings suggest that Sunbelt read Victor's text messages ***after they were sent and received on the Sunbelt iPhone, which is insufficient to demonstrate intentional interception under the Wiretap Act. *See NovelPoster v. Javitch Canfield Group*, No. C 13–5186 WHO, 2014 WL 3845148, *10 (N.D.Cal. Aug. 14, 2014) (reading emails that have already been received in an email account's inbox does not constitute interception under the Wiretap Act because the transmission had already occurred).

> FN1. Victor's Counterclaim repeatedly makes vague and formulaic references to "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.

Although it is clear that Victor's Wiretap Act claim must be dismissed, what is less clear is whether leave to amend should be granted. Given the almost instantaneous transmission of text mes-

sages, the window during which an interception may occur is exceedingly narrow. *NovelPoster*, 2014 WL 3845148, *10 (citing *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir.2003)). Thus, "unless some type of automatic routing software is used" to divert the text message, interception of [a text message] within the prohibition of the Wiretap Act is virtually impossible." *Id.* (internal quotations and citation omitted). Given these constraints, it is doubtful that Victor will be able to allege facts, consistent with Federal Rule of Civil Procedure 11, to state a claim for violation of the Wiretap Act. Nonetheless, the Court will afford Victor an opportunity to amend this claim and therefore DISMISSES his claim under the Wiretap Act, with leave to amend.[FN2]

FN2. Sunbelt also contends that Victor has failed to allege any facts showing that it 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.

B. STORED COMMUNICATIONS ACT

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

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

> Intentionally accessed, without authorization, facilities through which 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.

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

C. CALIFORNIA PENAL CODE § 502

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

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

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, 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.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services.
>
> (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
>
> ...
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

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

In his third Counterclaim, Victor alleges as follows:

> On information and belief, Sunbelt violated California Penal Code section 502 when it improperly began accessing, intercepting, monitoring, reviewing and using Victor's post-employment private electronic data and electronic communications without Victor's knowledge, authorization or consent. On information and belief, Sunbelt additionally, or in the alternative, violated of Penal Code § 502 ***by intentionally accessing, without authorization,*** facilities through which 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.

Countercl. ¶ 56 (emphasis added). These fact-barren and vague allegations are precisely the type of "threadbare recitals" proscribed by *Twombly* and *Iqbal.* Moreover, to the extent that Victor is claiming that Sunbelt accessed his unspecified "private electronic data and electronic communications" through the Apple account or his cellular telephone provider's computer network, such a claim fails on the ground that no facts are alleged showing that Sunbelt did so by circumventing technical or code-based barriers intended to restrict such access. *Facebook,* 844 F.Supp.2d at 1036. To the contrary, Victor simply avers that Sunbelt reviewed his text messages that he caused, albeit inadvertently, to be sent to the Sunbelt iPhone. The Court therefore concludes that Victor has failed to state a claim under Section 502 and DISMISSES said claim with leave to amend.

D. CALIFORNIA PENAL CODE § 630

***5** The California Invasion of Privacy Act ("CIPA") is intended to prevent privacy invasions facilitated by modern technology and devices.

Cal.Penal Code § 630. "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *NovelPoster*, 2014 WL 3845148, *12 (granting judgment on pleadings on CIPA claim for same reasons underlying the dismissal of the plaintiff's Wiretap Act claim, i.e., the lack of intentional interception). As discussed, Victor has failed to plausibly allege a violation of the Wiretap Act; *a fortiori*, he is also unable to allege a violation of CIPA. This claim is DISMISSED with leave to amend.

E. INVASION OF PRIVACY

California recognizes four categories of the tort of invasion of privacy: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light in the public eye; and (4) appropriation of name or likeness. *Shulman v. Group W Prods., Inc.*, 18 Cal.4th 200, 214 n. 4, 74 Cal.Rptr.2d 843, 955 P.2d 469 (1998). Victor fails to indicate which type of invasion of privacy claim he is alleging. Nonetheless, based on the sparse allegations presented, it appears that he is attempting to state a claim for intrusion upon seclusion.

"A privacy violation based on the common law tort of intrusion has two elements. First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must occur in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 285, 97 Cal.Rptr.3d 274, 211 P.3d 1063 (2009). "The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *Shulman v. Grp. W Prods., Inc.*, 18 Cal.4th 200, 232, 74 Cal.Rptr.2d 843, 955 P.2d 469 (1998). A plaintiff pursuing an invasion of privacy action must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have engaged in conduct which manifests a voluntary consent to the invasive actions of defendant. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 26, 26 Cal.Rptr.2d 834, 865 P.2d 633 (1994).

Victor contends that, as a matter of law, an employee has a reasonable expectation of privacy with respect to text messages contained on employer-owned mobile telephones. The decisional authorities cited by Victor, however, are inapposite. In *City of Ontario v. Quon*, 560 U.S. 746, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010), a police officer was issued a pager by his police department which was subject to a limit on the number of characters that could be sent and received each month. *Id.* at 750, 130 S.Ct. 2619. After becoming concerned that the officer was repeatedly exceeding his character limit, the police department obtained transcripts of the text messages from the wireless carrier to ascertain whether the texts were work-related or personal. *Id.* at 750–51, 130 S.Ct. 2619. After finding that most of the text messages were not work-related, the police department took disciplinary action against the officer. *Id.* at 753, 130 S.Ct. 2619. The police officer then brought an action under 42 U.S.C. § 1983 against the city, police department and police chief, alleging that the police department's review of his text messages violated the Fourth Amendment.

In the addressing the plaintiff's Fourth Amendment claim, the United States Supreme Court ***assumed, without deciding,*** that the plaintiff had a reasonable expectation of privacy in text messages sent to him on an employer-provided pager; however, the Court ultimately upheld the police department's review of those messages as reasonable under the Fourth Amendment. *Id.* at 760, 130 S.Ct. 2619. Despite Victor's suggestion to the contrary, the Supreme Court did not hold that an employee automatically has an expectation of privacy in electronic messages stored on a device provided by his employer. *Quon* also is distinguishable on its facts. Unlike the police officer in *Quon*, Victor was no longer an employee of the company that owned the electronic device at issue at the time the invasion of privacy allegedly occurred. Moreover, unlike the police department, which requested transcripts of the text messages from the wireless carrier, Sunbelt

is not alleged to have affirmatively undertaken any action to obtain and review the text messages or any other electronic data. Rather, the electronic communications appeared on Sunbelt's iPhone because of actions taken by Victor.

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

Victor's privacy claim also fails on the ground that he has failed to show an intrusion into a "place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy." *Hernandez,* 47 Cal.4th at 285, 97 Cal.Rptr.3d 274, 211 P.3d 1063. As noted, Victor cannot legitimately claim an expectation of privacy in a "place," i.e., the Sunbelt iPhone, which belongs to his former employer and to which he has no right to access. Nor can Victor claim a reasonable expectation of privacy with respect to his text messages, in general. The pleadings do not identify the contents of any particular text messages, and instead, refer generally to "private electronic data and electronic communications." Countercl. ¶ 79. This and other courts have concluded that there is no "legally protected privacy interest and reasonable expectation of privacy" in electronic messages, "in general." *In re Yahoo Mail Litig.,* —— F.Supp.2d ——, ——,2014 WL 3962824, *16 (N.D.Cal. Aug. 12, 2014) (citing cases).[FN3] Rather, a privacy interest can exist, if at all, only with respect to the ***content*** of those communications. In any event, even if Victor were claiming an expectation of privacy with respect to the specific content of his text messages (which he has not specified), the facts alleged demonstrate that he failed to comport himself in a manner consistent with an objectively reasonable expectation of privacy. By his own admission, Victor personally caused the transmission of his text messages to the ***Sunbelt*** iPhone by syncing his new devices to his Apple account without first unlinking his Sunbelt iPhone.[FN4] As such, even if he ***subjectively*** harbored an expectation of privacy in his text messages, such expectation cannot be characterized as ***objectively*** reasonable, since it was ***Victor's*** conduct that directly caused the transmission of his text messages to Sunbelt in the first instance. *See Hill,* 7 Cal.4th at 26, 26 Cal.Rptr.2d 834, 865 P.2d 633.

FN3. Victor also does not specify whether his claim is predicated upon text messages sent by him, received by him, or both. With respect to messages he transmitted, there is authority finding that a plaintiff has no reasonable expectation of privacy in messages sent to third parties. *See Fetsch v. City of Roseburg,* No. 6:11–cv–6343–TC, 2012 WL 6742665, *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).

FN4. Victor vaguely alleges that Sunbelt intercepted his electronic communications. He provides no factual support for this conclusory assertion. *See* Countercl. ¶ 77.

The above notwithstanding, the facts alleged in Victor's fifth counterclaim are insufficient to show that Sunbelt intruded into Victor's privacy in a manner highly offensive to a reasonable person. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill,* 7 Cal.4th at 37, 26 Cal.Rptr.2d 834, 865 P.2d 633. In addition, the plaintiff must show "that the ***use*** of plaintiff's information was highly offensive." *Folgelstrom v. Lamps Plus, Inc.,* 195 Cal.App.4th 986, 993, 125 Cal.Rptr.3d 260 (2011) (emphasis added) (upholding the demurrer to plaintiff's common law invasion of privacy claim where, finding that even if the customer addresses were obtained through "questionable" means, there was "no allegation that Lamps Plus used the address once obtained for an offensive or improper purpose.").

***7** Here, Victor alleges only that Sunbelt acted in a "highly offensive" manner by "accessing, intercepting, monitoring, reviewing, storing and using [his] post-employment private electronic data and electronic communications without [his] knowledge, authorization or consent as part of an unreasonably intrusive and unauthorized investigation into Victor's post-employment conduct." Countercl. ¶ 79. Victor offers no factual support for these conclusory assertions. In particular, he provides no details regarding the specific conduct by Sunbelt that amounts to "accessing, intercepting, monitoring, reviewing, storing and using [his] post-employment private electronic data and electronic communications." *Id.* He also fails to aver any facts to establish that Sunbelt's use of the intercepted communications was highly offensive. *See Folgelstrom,* 195 Cal.App.4th at 993, 125 Cal.Rptr.3d 260. The possibility that Sunbelt may have reviewed text messages sent to a cell phone which it owned and controlled—without more—is insufficient to establish an offensive use. As with his other claims, Victor's formulaic recitation of an invasion of privacy claim is inconsistent with the federal pleading requirements of Rule 8. This claim is DISMISSED with leave to amend.

IV. *CONCLUSION*

For the reasons stated above,

IT IS HEREBY ORDERED THAT:

1. Plaintiff's Motion to Dismiss Defendants Counterclaims is GRANTED.

2. Defendant shall have twenty-one (21) days from the date this Order is filed to amend his counterclaims, consistent with the Court's rulings. Defendant is warned that any factual allegations set forth in his amended pleading must be made in good faith and consistent with Rule 11. The failure to timely file the amended counterclaim and/or the failure to comply with this Order will result in the dismissal of all counterclaims with prejudice.

IT IS SO ORDERED.

N.D.Cal., 2014
Sunbelt Rentals, Inc. v. Victor
--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.)

END OF DOCUMENT