

United States District Court
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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ADAM BACKHAUT and KENNETH MORRIS,

Plaintiffs,

v.

APPLE INC.,

Defendant.

Case No.14-CV-02285-LHK

ORDER GRANTING MOTION FOR SUMMARY JUDGMENT

Re: Dkt. No. 85

Plaintiffs Adam Backhaut and Kenneth Morris (collectively, "Plaintiffs") bring this putative class action on behalf of themselves and others similarly situated against Defendant Apple, Inc. ("Defendant") for violations of the Wiretap Act, 18 U.S.C. § 2510 and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. First Am. Compl. ("FAC"), ECF No. 29. The gravamen of Plaintiffs' FAC is that Apple wrongfully intercepts, stores, and otherwise prevents former Apple device users from receiving text messages sent to them from current Apple device users. Before the Court is Defendant's motion for summary judgment. ("Mot."), ECF No. 86. The Court finds this matter appropriate for determination without oral argument and VACATES the hearing and the Case Management Conference set for December 3, 2015. See Civil L.R. 7-1(b). Having considered the submissions of the parties, the relevant law, and the

United States District Court
Northern District of California

1 record in this case, the Court hereby GRANTS Defendant’s motion for summary judgment.

2 **I. BACKGROUND**

3 **A. Facts**

4 Defendant Apple, Inc., a California corporation headquartered in Cupertino, California is
5 the “designer and seller” of the iPhone and other mobile devices that run “Apple’s proprietary
6 mobile operating system.” FAC ¶¶ 7, 35. Apple’s mobile operating system is known as “iOS”
7 and its first iteration was released on June 29, 2007. *Id.* ¶ 7. On October 12, 2011, Apple released
8 iOS 5, which included a “proprietary messaging service known as ‘iMessage’” that runs on a
9 client application called “Messages.” *Id.* ¶¶ 8–9. Plaintiff Adam Backhaut is a resident of
10 Michigan who purchased an iPhone in December 2012. *Id.* ¶¶ 33, 39, 40. Plaintiff Morris is a
11 resident of California who purchased his last iPhone in October 2012. *Id.* ¶¶ 34, 47. Plaintiffs
12 both used Apple’s iMessage and Messages application on their iPhones. Plaintiffs Backhaut and
13 Morris switched from Apple iPhones to non-Apple phones in December 2013 and December 2012
14 respectively. *Id.* ¶¶ 41, 47.

15 Plaintiffs allege that Apple “intentionally intercepted the electronic communications of
16 Plaintiffs” and “intercepts the text messages immediately after they are sent by current
17 iPhone/iMessage Users.” *Id.* ¶¶ 62–63. Plaintiffs contend that Apple wrongfully “receives and
18 stores these messages through the employment of a . . . device under” the Wiretap Act. *Id.* ¶ 64.
19 Plaintiffs further allege that these unlawful business practices support claims under California’s
20 Unfair Competition Law (“UCL”). *Id.* ¶ 68. Plaintiffs also allege that these business practices
21 constitute “unfair” business practices under the UCL for violation of “established legislative goals
22 and policies.” *Id.* ¶ 72.

23 **1. Text Messages, iMessages, and Messages**

24 “Text messages” or “texts” are “brief, electronic messages between two or more mobile
25 devices.” *Id.* ¶ 3. There are “multiple technologies” for sending text messages, but the
26 “traditional” or standard technology is the Short Message Service and Multimedia Messaging
27 Service (“SMS/MMS”) protocols. *Id.* ¶¶ 3, 5. As an alternative to this standard protocol, Apple’s

United States District Court
Northern District of California

1 proprietary text messages are known as “iMessages” and are sent using the “Messages” client
2 application. *Id.* ¶¶ 8–10. Instead of the SMS/MMS protocol for sending and receiving messages,
3 iMessages use Wi-Fi and cellular data networks to send messages and other content between two
4 Apple devices. *Id.* ¶¶ 9–10.

5 “Once an iPhone user activates iMessage,” the interface for sending iMessages and
6 SMS/MMS text messages on the Messages client application is the same. *Id.* ¶ 11. The Messages
7 application “automatically checks if the contact to whom the text message is being sent is also
8 registered as an iMessage user.” *Id.* ¶ 13. [REDACTED]

9 [REDACTED]
10 [REDACTED] ECF No. 85-11 at 59:23-60:1; ECF No.
11 85-37 ¶ 6. If the intended recipient is listed as an iMessage user, [REDACTED]

12 [REDACTED] and the text message is sent as an iMessage, “bypassing the SMS/MMS
13 system of the sender’s cellular carrier.” FAC ¶ 13; ECF No. 85-37 ¶ 6. If the contact is not
14 registered as an iMessage user, [REDACTED]

15 [REDACTED] and the message is sent as an SMS/MMS. FAC ¶ 13; ECF No. 85-37 ¶ 6. [REDACTED]

16 [REDACTED]
17 [REDACTED]
18 ECF No. 85-11 at 59:23-60:1; ECF No. 85-37 ¶ 6.

19 The Messages application “does not allow the user to select whether a text message will be
20 sent using iMessage or SMS/MMS.” FAC ¶ 12. However, the sender may enable the “send as
21 SMS” option on the sender’s iPhone. ECF No. 85-37 ¶ 11; ECF No. 85-35 ¶ 23. If the “send as
22 SMS” option is selected, a message initially sent as an iMessage will be resent as an SMS/MMS
23 message if the message has not been successfully delivered after five minutes. ECF No. 85-37
24 ¶ 11; ECF No. 85-35 ¶ 23. A sender can see whether a message was sent using iMessage or
25 SMS/MMS based on the background color of the message: blue for iMessage and green for
26 SMS/MMS. FAC ¶ 14. When an iMessage is “received, the word ‘delivered’ will appear under
27 the text message on the sender’s phone.” *Id.* ¶ 15.

United States District Court
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

When a text message is sent as an iMessage, it is initially encrypted such that only the sender and the receiver can access the substance of the message. ECF No. 85-37 ¶ 8. Apple has no ability to decrypt messages that are in transit between phones [REDACTED] [REDACTED] *Id.*; ECF No. 85-11 at 71:1-15. [REDACTED] [REDACTED] ECF No 85-37 ¶ 9. [REDACTED] [REDACTED] ECF No. 85-37 ¶ 9; ECF No. 101-7, Exh. Q at 12:16-17; ECF No. 101-7, Exh. P at 44:12-15; ECF No. 101-8, Exh. S ¶ 19. [REDACTED] [REDACTED] ECF No. 101-7, Exh. P at 158:7-9; ECF No. 85-37 ¶ 11. [REDACTED] ECF No. 85-11 at 28:21; ECF No. 85-37 ¶ 9. [REDACTED] ECF No. 85-11 at 33:9-12; ECF No. 85-37 ¶ 9.

2. Plaintiffs’ Experiences

a. Plaintiff Backhaut

In December 2012, Plaintiff Backhaut and his spouse, Joy Backhaut,¹ purchased iPhone 5s in Michigan. FAC ¶ 39–40. “At the time of purchase,” a Best Buy employee set up their iPhones, including iMessage. *Id.* In December 2013, Plaintiff Backhaut purchased a “HTC One,” a non-Apple mobile device that runs on an Android operating system. *Id.* ¶ 41. Following Plaintiff Backhaut’s switch, his spouse Joy continued to send Plaintiff Backhaut text messages from her iPhone. *Id.* ¶ 43. On Joy Backhaut’s phone, the word “delivered” appeared under her messages to her spouse, but Plaintiff Backhaut never received those messages. *Id.* Upon realizing that he was

¹ Joy Backhaut was a named plaintiff in this action. On August 7, 2015, Joy Backhaut filed a motion to voluntarily dismiss with prejudice her claims against Apple. ECF No. 84. On August 11, 2015, Defendant filed a response indicating that it did not oppose Joy Backhaut’s motion. ECF No. 88. The Court granted the motion to dismiss Joy Backhaut’s claims with prejudice on August 13, 2015. ECF No. 89.

1 not receiving certain text messages, Plaintiff Backhaut “attempted to remove his phone number
2 from the iMessage system but was unsuccessful.” *Id.* ¶ 45.

3 **b. Plaintiff Morris**

4 Plaintiff Morris was an iPhone user from November 2007 to December 2012. *Id.* ¶ 46. He
5 purchased his last iPhone, an iPhone 5, in October 2012. *Id.* ¶ 47. In December 2012, Plaintiff
6 Morris purchased a non-Apple phone. *Id.* Morris “attempted to remove his phone number from
7 the iMessage system” but was unable to do so. *Id.* ¶ 49. Morris also asked his contacts to
8 manually change the settings in their iPhones to send him SMS/MMS messages rather than
9 iMessages. *Id.* This resolved the problem until Apple released iOS 7.1.1, at which point even
10 contacts that had manually changed their settings had difficulties sending Morris text messages.
11 *Id.* ¶ 50.

12 **B. Procedural History**

13 Plaintiffs filed their original complaint on May 16, 2014. ECF No. 1. Defendant filed its
14 motion to dismiss on August 18, 2014. ECF No. 12. As part of its motion to dismiss, Defendant
15 also filed a request for judicial notice, which Plaintiffs did not oppose. ECF No. 12. Plaintiffs
16 filed their opposition on September 22, 2014. ECF No. 16. Defendant filed its reply on October
17 21, 2014. ECF No. 17. On November 19, 2014, the Court granted in part and denied in part
18 Defendant’s motion to dismiss. ECF No. 27. The Court granted without prejudice Defendant’s
19 motion to dismiss Plaintiffs’ Stored Communications Act claim; UCL claims based on violations
20 of the Stored Communications Act claim; California Consumer Legal Remedies Act claim; and
21 UCL claims based on fraudulent conduct. *Id.* at 22–23. The Court denied Defendant’s motion to
22 dismiss Plaintiffs’ Wiretap Act claim and UCL claims based on violations of the Wiretap Act. *Id.*

23 On December 10, 2014, Plaintiffs filed their FAC. ECF No. 29. Defendant filed an
24 answer on January 7, 2015. ECF No. 31.

25 Plaintiffs filed a motion for class certification on May 28, 2015. ECF No. 59. Defendant
26 filed its opposition on June 26, 2015. ECF No. 75. Plaintiffs filed their reply on July 16, 2015.
27 ECF No. 78. The Court denied Plaintiffs’ motion on August 13, 2015. ECF No. 89. Plaintiffs

1 filed a motion for leave to file a motion for reconsideration of the Court’s August 13 order
2 denying class certification (“Motion for Leave”) on August 27, 2015. ECF No. 99. Defendant
3 filed an opposition to Plaintiffs’ Motion for Leave on September 11, 2015. ECF No. 102.

4 Defendant filed the instant motion for summary judgment on August 8, 2015. (“Mot.”),
5 ECF No. 86. Plaintiffs opposed Defendant’s motion on September 9, 2015 (“Opp.”), ECF No.
6 101. Defendant filed a reply on September 28, 2015. (“Reply”), ECF No. 107.

7 **I. LEGAL STANDARD**

8 Summary judgment is appropriate if, viewing the evidence and drawing all reasonable
9 inferences in the light most favorable to the nonmoving party, there are no genuine issues of
10 material fact, and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a);
11 *Celotex Corp. v. Catrett*, 477 U.S. 317, 321 (1986). At the summary judgment stage, the Court
12 “does not assess credibility or weigh the evidence, but simply determines whether there is a
13 genuine factual issue for trial.” *House v. Bell*, 547 U.S. 518, 559-60 (2006). A fact is “material”
14 if it “might affect the outcome of the suit under the governing law,” *Anderson v. Liberty Lobby,*
15 *Inc.*, 477 U.S. 242, 248 (1986), and a dispute as to a material fact is “genuine” if there is sufficient
16 evidence for a reasonable trier of fact to decide in favor of the nonmoving party, *id.* “If the
17 evidence is merely colorable, or is not significantly probative, summary judgment may be
18 granted.” *Id.* (citations omitted).

19 The moving party bears the initial burden of identifying those portions of the pleadings,
20 discovery, and affidavits that demonstrate the absence of a genuine issue of material fact. *Celotex*
21 *Corp.*, 477 U.S. at 323. Where the moving party will have the burden of proof on an issue at trial,
22 it must affirmatively demonstrate that no reasonable trier of fact could find other than for the
23 moving party, but on an issue for which the opposing party will have the burden of proof at trial,
24 the party moving for summary judgment need only point out “that there is an absence of evidence
25 to support the nonmoving party’s case.” *Id.* at 325; accord *Soremekun v. Thrifty Payless, Inc.*, 509
26 F.3d 978, 984 (9th Cir. 2007). Once the moving party meets its initial burden, the nonmoving
27 party must set forth, by affidavit or as otherwise provided in Rule 56, “specific facts showing that

United States District Court
Northern District of California

1 there is a genuine issue for trial.” *Anderson*, 477 U.S. at 250.

2 **II. DISCUSSION**

3 Defendant advances several bases on which the Court may grant summary judgment.
4 First, Defendant argues that there is no evidence that Plaintiffs failed to receive any specific text
5 messages. Mot. at 14-15. Second, Defendant argues that there is no evidence that Defendant’s
6 iMessage system “intercepted” any messages, as the term “intercepted” is defined within the Ninth
7 Circuit for purposes of the Wiretap Act. Mot. at 15-18. Third, Defendant argues that there is no
8 evidence that Defendant used a “device” to intercept any messages, as required by the Wiretap
9 Act. Mot. at 18-20. Fourth, Defendant argues that there is no evidence that any interception of
10 messages by Defendant was intentional. Mot. at 20-24. Fifth, Defendant argues that Plaintiffs’
11 UCL claim is dependent upon Plaintiffs’ Wiretap Act claim, so Plaintiffs cannot succeed on the
12 UCL claim if they cannot succeed on the Wiretap Act claim. Mot. at 24. Finally, Defendant
13 argues that Defendant’s terms of use contract for iMessage precludes Plaintiffs from succeeding
14 on their two claims. Mot. at 24-27.

15 For the reasons stated below, the Court concludes that there is insufficient evidence that
16 Defendant intercepted any messages within the meaning of the Wiretap Act and insufficient
17 evidence that Defendant used a device as defined by the Wiretap Act. Because Defendant has
18 shown an absence of genuine dispute of material fact on these points, the Court GRANTS
19 Defendant’s motion for summary judgment as to the Wiretap Act claim. Because Plaintiffs’ UCL
20 claim is dependent upon Plaintiffs’ Wiretap Act claim, the Court also GRANTS Defendant’s
21 motion for summary judgment as to the UCL claim. The Court need not address Defendant’s
22 other bases for summary judgment or Plaintiffs’ counterarguments thereto.

23 **A. Wiretap Act Claim**

24 The Wiretap Act, which was enacted as Title III of the Electronic Communications
25 Protection Act (“ECPA”), generally prohibits the “interception” of “wire, oral, or electronic
26 communications.” 18 U.S.C. § 2511(1). More specifically, the Wiretap Act provides a private
27 right of action against any person who “intentionally intercepts, endeavors to intercept, or procures

United States District Court
Northern District of California

1 any other person to intercept or endeavor to intercept, any wire, oral, or electronic
2 communication.” 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action).

3 The statute defines “intercept” as “the aural or other acquisition of the contents of any
4 wire, electronic, or oral communication through the use of any electronic, mechanical, or other
5 device.” *Id.* § 2510(4). “Such acquisition occurs ‘when the contents of a wire communication are
6 captured or redirected in any way.’” *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009). Defendant
7 contends that Plaintiffs have not identified evidence that Defendant’s conduct satisfies the
8 definition of “intercept” in the Wiretap Act. The Court agrees with Defendant on two grounds: (1)
9 that the undisputed evidence shows that any acquisition by Defendant did not occur at the time of
10 transmission as required by the Wiretap Act, and (2) that the undisputed evidence shows that the
11 “device” used by Defendant falls within the “ordinary course of business” exception to Wiretap
12 Act liability.

13 **1. No Acquisition at the Time of Transmission**

14 Defendant first contends that Plaintiffs have not shown that Defendant acquired any
15 misdirected messages at the time of transmission. The Ninth Circuit has held that for an electronic
16 communication to be “intercepted” in violation of the Wiretap Act, “it must be acquired during
17 transmission, not while it is in electronic storage.” *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d
18 868, 878 (9th Cir. 2002). There can be no interception for purposes of the Wiretap Act if the
19 acquisition of the message occurs while the message is in storage, even if it is in temporary
20 storage incidental to the transmission of the communication. *Id.* n.6. Thus, the Ninth Circuit held
21 that no interception occurs when an individual who lacks authorization to access a webpage uses
22 an authorized user’s credentials to gain access to the webpage, even though the unauthorized
23 individual acquired the contents of the webpage, because the webpage was not in transmission at
24 the time of acquisition. *Id.* at 879.

25 In the instant case, Plaintiffs argue that “the iMessage server caused [Plaintiffs’] messages
26 to be intercepted at the exact moment of transmission as a result of a structural defect,” resulting in
27 messages being sent as iMessages to users who cannot receive iMessages. *Opp.* at 14. However,

United States District Court
Northern District of California

1 Plaintiffs have not identified any structural defect that misclassifies or redirects messages as
2 iMessages “at the exact moment of transmission.” Instead, the undisputed evidence shows that a
3 prospective message is [REDACTED]

4 [REDACTED] ECF No. 85-11 at 59:23-60:1; ECF No. 85-37 ¶ 6. [REDACTED]

6 [REDACTED] When the sender first selects a recipient, the sender’s Messages
7 application and the iMessage system [REDACTED]

8 *Id.* [REDACTED]

9 [REDACTED] *Id.* [REDACTED]

10 [REDACTED] Defendant does
11 not “intercept” the message within the meaning of the Wiretap Act by erroneously classifying the
12 message as an iMessage. *See Konop*, 302 F.3d at 878 (holding that for an electronic
13 communication to be “intercepted” in violation of the Wiretap Act, “it must be acquired during
14 transmission”).

15 Moreover, Plaintiffs appear to concede that it is not an “interception” for messages to be
16 initially misclassified and sent as iMessages. Plaintiffs acknowledge that the sender can select the
17 “send as SMS text” option on the sender’s phone prior to transmitting the message. *Opp.* at 3 n.2;
18 ECF No. 85-37 ¶ 11; ECF No. 85-35 ¶ 23. If the sender selects this option, a message initially
19 misclassified as an iMessage will be sent as an iMessage initially but then will be resent as an
20 SMS/MMS after five minutes. ECF No. 85-37 ¶ 11; ECF No. 85-35 ¶ 23. Plaintiffs concede that
21 “if the message is sent as an SMS text there would be no unlawful interception,” *Opp.* at 3 n.2,
22 even though the message is first sent to the iMessage server prior to the determination that the
23 message cannot be delivered, *see* ECF No. 85-37 ¶ 11; ECF No. 85-35 ¶ 23.

24 To the extent Plaintiffs instead contend that the interception occurs when messages from a
25 sender who has not selected “send as SMS” are not resent as SMS/MMS when the messages prove
26 undeliverable as iMessages, this event also does not occur while the message is “in transmission.”

27 [REDACTED], ECF No. 85-11 at 60:22-25, [REDACTED]

United States District Court
Northern District of California

1 [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED] ECF No. 85-11 at 60:22-25; ECF No.

5 85-11 at 28:15-21; 33:9-12; ECF No. 85-37 ¶ 9. [REDACTED]

6 [REDACTED]

7 [REDACTED] ECF No. 85-37 ¶ 9; ECF No. 101-7, Exh. Q at 12:16-17; ECF No. 101-7, Exh. P at 44:12-

8 15; ECF No. 101-8, Exh. S ¶ 19. [REDACTED]

9 [REDACTED] There can be no

10 interception within the meaning of the Wiretap Act while the message is [REDACTED]

11 [REDACTED]

12 [REDACTED] See *Konop*, 302 F.3d at 878 n.6 (holding that there can be no

13 interception for purposes of the Wiretap Act if the acquisition of the message occurs while the

14 message is in storage, even if it is in temporary storage incidental to the transmission of the

15 communication).

16 Finally, to the extent Plaintiffs argue that the interception occurs when a message [REDACTED]

17 [REDACTED]

18 [REDACTED] Plaintiffs effectively concede that this

19 transmission on its own is insufficient to establish an interception. Plaintiffs concede that a

20 message initially transmitted as an iMessage may still be sent as an SMS if the sender has selected

21 “send as SMS,” and that there is no interception if the message is sent as an SMS. See *Opp.* at 3

22 n.2. Additionally, Plaintiffs in opposition to Defendant’s motion for summary judgment have not

23 identified any device, other than the iMessage server, [REDACTED]

24 [REDACTED] See *Opp.* at 16 (describing the iMessage server as the

25 “‘device’ for purposes of the interception”). As the Court explains below, the iMessage server

26 falls within the “ordinary course of business” exception to the Wiretap Act, [REDACTED]

27 [REDACTED]

United States District Court
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

2. The iMessage Server Falls within the “Ordinary Course of Business” Exception

Defendant further contends that any “device” identified by Plaintiffs falls within the “ordinary course of business” exception to Wiretap Act liability. Section 2510(5)(a), the definition of “device,” exempts “any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business” This exception is narrow in scope and requires that the electronic communication service provider demonstrate that “the interception facilitated the communication service or was incidental to the functioning of the provided communication service.” *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013).

In the instant case, the device Plaintiffs identify in their opposition to Defendant’s motion for summary judgment is the iMessage server. Opp. at 16. Plaintiffs do not dispute that Apple is “a provider of wire or electronic communication service.” See Opp. at 15-16. Instead, Plaintiffs argue that the “ordinary course of business” exception does not apply to [REDACTED] the iMessage server because “(1) the purposes [sic] of iMessage is to deliver messages, and (2) iMessage contains a structural defect that causes the messages to be intercepted.” Opp. at 15.

Defendant has produced evidence that in Defendant’s ordinary course of business, [REDACTED] ECF No. 85-37 ¶ 9. [REDACTED] ECF No. 85-11 at 60:22-25. [REDACTED] ECF No. 85-37 ¶ 9; [REDACTED] ECF No. 85-37 ¶ 9; ECF No. 101-7, Exh. Q at 12:16-17; ECF No. 101-7, Exh. P at 44:12-15; ECF No. 101-8, Exh. S ¶ 19; [REDACTED]

United States District Court
Northern District of California

1 [REDACTED] ECF No. 101-7, Exh. P
2 at 158:7-9; ECF No. 85-37 ¶ 11; [REDACTED]
3 [REDACTED] ECF No. 85-11 at 33:9-12; ECF No. 85-37 ¶ 9. All of these functions “facilitate[] the
4 communication service” provided by Apple or are “incidental to the functioning of the provided
5 communication service.” See *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *8. Plaintiff
6 has not identified any contrary evidence.

7 Moreover, Plaintiffs point to no evidence that the iMessage server ever operated outside its
8 ordinary functions. The undisputed evidence shows that by the time any misclassified messages to
9 former iPhone users [REDACTED]
10 [REDACTED] ECF No. 85-11 at
11 59:23-60:1; ECF No. 85-37 ¶¶ 6, 14. [REDACTED]

12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED] ECF No. 85-11 at 59:23-60:1, 60:22-25; ECF No. 85-37 ¶¶ 6, 14.

16 [REDACTED]
17 [REDACTED]
18 [REDACTED] ECF No. 85-11 at 60. [REDACTED]

19 [REDACTED]
20 [REDACTED] ECF No. 85-11 at 28:15-21; 33:9-12; ECF
21 No. 85-37 ¶ 9. This evidence, undisputed by Plaintiffs, is sufficient to establish that the iMessage
22 server was operating within the ordinary course of business [REDACTED]

23 [REDACTED] An acquisition of a communication by a device
24 “being used by a provider of wire or electronic communication service in the ordinary course of its
25 business” cannot form the basis of a Wiretap Act claim. 18 U.S.C. § 2510(5)(a). Thus, the
26 iMessage server does not qualify as a “device” within the meaning of the Wiretap Act, and
27 Defendant is entitled to summary judgment on the Wiretap Act claim.

1 The evidence in this case is similar to *Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 502
 2 (2d Cir. 2005). In *Hall*, the plaintiff alleged Earthlink had wrongfully intercepted emails sent to
 3 his cancelled email address because Earthlink had stored those emails rather than “bouncing back”
 4 the emails to the senders. In a motion for summary judgment, Earthlink offered evidence that it
 5 lacked the technical ability to “bounce back” emails and that storing such emails was an ordinary
 6 business practice. *Id.* The *Hall* plaintiff offered no evidence to the contrary, and the Second
 7 Circuit affirmed the district court’s grant of summary judgment. *Id.* Likewise, in this case,
 8 Defendant has offered undisputed evidence that the iMessage server [REDACTED]

9 [REDACTED]
 10 [REDACTED] Defendant has also offered undisputed evidence that [REDACTED]
 11 [REDACTED] is an ordinary business practice. As in *Hall*, summary judgment
 12 for Defendant is appropriate because the device identified by Plaintiffs was used within the
 13 ordinary course of business by a provider of wire or electronic communication services and thus
 14 cannot form the basis of a Wiretap Act claim. *See* 18 U.S.C. § 2510(5)(a) (exempting from the
 15 Wiretap Act devices used by providers of wire or electronic communication services in the
 16 ordinary course of business).

17 Therefore, the Court GRANTS Defendant’s motion for summary judgment on the Wiretap
 18 Act claim.

19 **B. UCL Claim**

20 Defendant additionally argues that the Court should grant summary judgment in favor of
 21 Defendant on Plaintiffs’ UCL claim because the UCL claim is predicated upon the Wiretap Act
 22 claim. Defendant argues that summary judgment should accordingly be entered on the UCL claim
 23 for the same reasons as for the Wiretap Act claim. Mot. at 24.

24 Plaintiffs concede that the UCL claim is predicated upon the Wiretap Act claim and make
 25 no separate arguments for why the UCL claim should survive summary judgment. Opp. at 18.
 26 Because the Court concludes that Defendant is entitled to summary judgment on Plaintiffs’
 27 Wiretap Act claim, Defendant is also entitled to summary judgment on Plaintiff’s UCL claim.

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

Therefore, the Court GRANTS Defendant’s motion for summary judgment on the UCL claim.

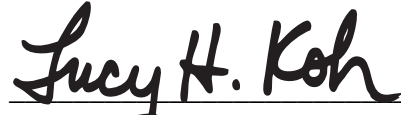
III. CONCLUSION

For the foregoing reasons, the Court GRANTS Defendant’s motion for summary judgment. The Court DENIES as moot Plaintiffs’ Motion for Leave.

The Clerk shall enter judgment in favor of Defendant and close the file.

IT IS SO ORDERED.

Dated: November 30, 2015



LUCY H. KOH
United States District Judge

United States District Court
Northern District of California