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 DIVISION

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 NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED AMENDED COMPLAINT; SUPPORTING MEMORANDUM OF POINTS AND AUTHORITIES

HEARING:
Date: September 17, 2014
Time: 9:00 a.m.
Place: Courtroom 3, 3rd Floor
The Honorable Phyllis J. Hamilton

NOTICE OF MOTION AND MOTION TO DISMISS CONSOLIDATED AMENDED COMPLAINT

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that at 9:00 a.m. on September 17, 2014, or as soon thereafter as the matter may be heard by the above-entitled Court, in the courtroom of the Honorable Phyllis J. Hamilton, 1301 Clay Street, Oakland, CA 94612, Defendant Facebook, Inc. ("Facebook") will and hereby does move for an order dismissing Plaintiffs' Consolidated Amended Complaint (the "CAC" or "Complaint") with prejudice under Rule 12(b)(6) of the Federal Rules of Civil Procedure. This Motion is based on this Notice of Motion and Motion, the supporting Memorandum of Points and Authorities, the Declaration of Jeremy Jordan, the Request for Judicial Notice, the Court's files in this action, the arguments of counsel, and any other matter that the Court may properly consider.

ISSUES TO BE DECIDED

1. Do any of Plaintiffs' claims against Facebook state a claim upon which relief can be granted?

2. Do Plaintiffs have statutory standing to assert a claim under California's Unfair Competition Law?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION AND SUMMARY OF ARGUMENT

In the wake of similar lawsuits filed against other companies, Plaintiffs filed this copycat suit alleging that Facebook was intercepting its users' messages in order to build user profiles and serve targeted advertisements. Plaintiffs have now abandoned their inaccurate, advertising-related allegations (except for some lingering amorphous allegations made on "information and belief" about Facebook's purported "future objective[s]") and reframed their Consolidated Amended Complaint ("CAC") to focus on an unrelated, routine practice involving Facebook's "Like" button that does not support any viable legal theory.

Plaintiffs allege that for an unspecified period of time before October 2012, when a Facebook user sent a "private message" to another user that included a link to a website (a Uniform Resource Locator, or "URL"), Facebook "scanned" or "intercepted" the URL and then increased the aggregate "Like" count displayed on that webpage by one (or two, due to a bug). In other words, and by way of example, Plaintiffs contend that, before October 2012, if 15,000 Facebook users previously had clicked the "Like" button on a particular webpage (such as a travel article on the *New York Times*), and a single Facebook user also shared the URL for that article in a message to a friend, the aggregate "Like" count displayed on that webpage would have increased to 15,001 or 15,002. Plaintiffs' sole basis for their putative nationwide class action lawsuit is that by simply displaying an aggregate—and anonymous—count of the number of times Facebook users liked or shared content, Facebook allegedly violated *criminal* "wiretapping" and "eavesdropping" statutes under federal and state law.

Plaintiffs do not contend—nor could they—that anyone other than the recipient of the message learned that a particular user had shared a URL. And indeed, the count indicating the total number of Likes is *anonymous and aggregate*. Similarly, Plaintiffs cannot plausibly contend that they suffered any injury as a result of this conduct. Nor do Plaintiffs dispute that Facebook must process and analyze content shared on its service, including in messages, for a host of reasons, including the operation of the service itself and for security reasons such as protecting users from spam and malicious links.

Plaintiffs do not challenge any of these routine and necessary practices, but they still seek to press forward on their "increased 'Like' count" theory. The theory fails, and each of Plaintiffs' claims fails as a matter of law:

Wiretap Act. Plaintiffs' first claim for alleged violations of the criminal Wiretap Act (18 U.S.C. §§ 2510, *et seq*.) fails for three reasons. First, Plaintiffs have not alleged—nor can they—an actionable "interception" because the statute expressly *excludes* the receipt of electronic communications by a provider of an electronic communication service (like Facebook) "in the ordinary course of its business." Plaintiffs acknowledge that Facebook receives its users' communications in the ordinary course of its business, and for this reason there can be no "interception." Plaintiffs' real complaint is not that Facebook receives and processes their messages (obviously it does, and it must), but that Facebook used those messages in a manner that they challenge (i.e., by increasing the "Like" count). But there can be no violation of the "use" provision of the Wiretap Act unless the original "interception" was unlawful—and here it was not. Moreover, the CAC admits that the alleged conduct here (which Plaintiffs describe as "systematic[]," "as a matter of course," and relevant to Facebook's business) was in the ordinary course of Facebook's business. This concession bars Plaintiffs' Wiretap Act claim as a matter of law.

Second, Plaintiffs consented—both expressly and impliedly—to any alleged "interception" of their messages. Facebook's Data Use Policy—to which all users consent and which Plaintiffs admit they read—informed Plaintiffs that Facebook "receive[s] data about you ***whenever you use or are running Facebook***, such as when you . . . ***send or receive a message***[.]" The Data Use Policy also informed Plaintiffs of the many ways in which their data could be used, and further explained that Facebook could share data with website developers if Facebook "removed your name and any other personally identifying information from it" (as with an anonymous, aggregate count). These provisions in Facebook's Data Use Policy give rise to express consent as a matter of law. At a minimum, Plaintiffs impliedly consented to the alleged interceptions because they admit that whenever they included a URL in a message, Facebook generated a thumbnail preview of the content at the destination website and displayed it for the user's review *before* the message was sent. A user

who saw the URL preview and proceeded to send the message impliedly consented to the alleged "interception."

Third, Plaintiffs' Wiretap Act claim fails because "to be 'intercepted' in violation of the Wiretap Act, [a communication] must be acquired *during transmission*, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 878, 878-79 (9th Cir. 2002) (emphasis added). Here, the CAC alleges that the use of Plaintiffs' messages to increase the "Like" count occurred not while those messages were in "transmission," but rather after they were sent and stored on Facebook's servers. Such conduct is governed by another statute, the Stored Communications Act ("SCA"), rather than the Wiretap Act. And Plaintiffs have not asserted (nor could they assert) an SCA claim.

California Invasion of Privacy Act ("CIPA") (Penal Code Sections 631(a) and 632). Plaintiffs' claims for alleged violations of CIPA fail largely for the same reasons as the Wiretap Act claim. All Facebook users consented to the alleged interception of their messages, and the use of the messages is not an interception "in transit" in any event. Further, the Section 632 claim fails for the additional reasons that (i) California courts uniformly have held that Internet communications—which are recorded and can be re-shared by the recipient—are not "confidential communications" within the meaning of Section 632, and (ii) there was no "eavesdropping" here as a matter of law.

UCL. Plaintiffs lack standing to maintain a UCL claim because they have not "lost" any "money or property." Facebook is a free service, and courts—including the Ninth Circuit—have held that the acquisition of a person's personal information does not constitute "lost money or property."

Plaintiffs' entire lawsuit, which was launched on a faulty premise, remains fundamentally misguided. Its defects are not defects of pleading but defects of theory. Accordingly, they cannot be cured by amendment, and the Court should dismiss this action with prejudice.

II. FACTUAL BACKGROUND

A. Plaintiffs' Claims and The Proposed Class

The three named Plaintiffs—Matthew Campbell, Michael Hurley, and David Shadpour—are Facebook users residing in Arkansas, Oregon, and California, respectively, who allege that they "used Facebook's private messaging function throughout the class period for, *inter alia*, purposes of

conveying messages whose content [includes] URL links." (CAC ¶¶ 5-7.) Plaintiffs bring claims on behalf of a putative nationwide class of "[a]ll natural-person Facebook users . . . who have sent or received private messages that included URLs in their content, from within two years before the filing of this action up through and including the date when Facebook ceased its practice." (*Id.* ¶ 59.) They assert claims against Facebook for alleged violations of the Electronic Communications Privacy Act (18 U.S.C. §§ 2510, *et seq.*), the California Invasion of Privacy Act (Cal. Penal Code §§ 630, *et seq.*), and California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*). They seek declaratory and injunctive relief, restitution, actual and statutory damages, and attorneys' fees.

B. Facebook's Services and Practices

1. *Facebook's Platform for Content Sharing and Discovery*. Facebook is the world's largest social networking platform, "with approximately 1.2 billion users, representing approximately 51% of all internet users worldwide, accessing its services monthly." (CAC ¶ 15.) The platform aims to "give people the power to share" and make the world "more open and connected," and "[p]eople use Facebook to stay connected with their friends and family, to discover what is going on in the world around them, and to share and express what matters to them[.]" (Dkt. No. 1, ¶ 37.) Facebook's services—which are free—enable users to post and share text, photography, video, and other Internet content with one another. (*Id.*; CAC ¶ 20.) As Plaintiffs acknowledge, Facebook hosts this content for users so they are able to keep an accessible repository of the content they have shared and received. (CAC ¶¶ 23, 48.)

There are "different ways to share content on Facebook[.]" (CAC ¶ 21.) For example, users may post content of interest on their personal profile page (a "Timeline"), which is then viewable by the specific audience that the Facebook user has selected (such as the public or Friends,[1] depending on the privacy settings the user configures). (*Id.* ¶ 20.) If they are within the selected audience for posted content, other users may view that content in a variety of places, including in their "News Feed,"[2] and they may in turn comment on, "Like," or re-share the content. (*Id.* ¶¶ 20, 21.) Users

[1] Users may connect as "Friends" on Facebook, mutually agreeing to share posted content (although exact audience settings may be adjusted on a content-specific basis).

[2] A Facebook user's "News Feed" is a constantly updating list of stories (e.g., posts, links, app activity, and "Likes") from other users that the user has elected to follow on Facebook (i.e., their

[Footnote continued on next page]

alternatively may share content by sending a Facebook message to one or more selected Facebook users, which can be viewed in the recipient user's Messages folder (instead of being shared on users' Timelines or in News Feeds). (*Id.*) To send and receive Facebook messages, an individual must have created a Facebook account (which, as discussed below, requires the individual to agree to Facebook's terms and Data Use Policy). All shared content is by definition received by Facebook and stored on Facebook servers, regardless of whether it is a post or a message.

2. *Facebook's "Messages" Product*. Plaintiffs' CAC is focused on this latter way of sharing content on Facebook's platform—i.e., Facebook's Messages product. Plaintiffs observe that Facebook states that such messages are "private": "If you'd like to share something privately, you can always send someone a private message." (CAC ¶ 23 (emphasis omitted).) This is true: A message sent from one Facebook user to another Facebook user does not appear on either users' Timelines or in their News Feeds and is not accessible by any Facebook users or third parties who are not recipients of the message (unless the recipient chooses to disclose it). But "private" does not mean that Facebook itself—the provider of the communication service—does not receive the message. Facebook by definition must receive and host *all content* shared on the site (regardless of the medium), without which it could not provide its service. (*Id.* (only with hosting can users "view the contents and history of [their] conversation").) Indeed, Facebook makes this clear in its Data Use Policy, which provides both that "[w]e receive data about you whenever you use or are running Facebook, such as when you . . . send or receive a message," and "[w]e store data for as long as it is necessary to provide products and services to you and others[.]" Ex. D at 2, 5.[3]

Facebook users are aware that Facebook is receiving, processing, and storing their messages. For example, Messages—like the other sharing options on Facebook—includes a "URL preview" function, which helps users verify the content they are sharing *before sending*. (CAC ¶ 36 (screenshot illustrating preview functionality).) Specifically, when a user composes a message

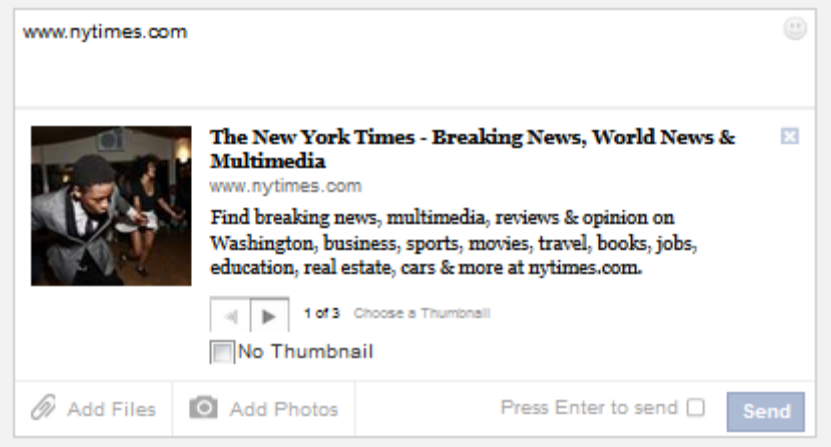
---

[Footnote continued from previous page]

Friends). A user's News Feed will only display content for which she has been designated as an audience member (by the content poster).

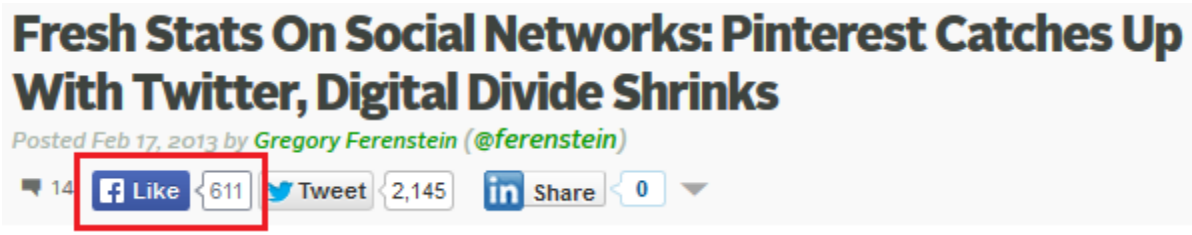
[3] All references to exhibits ("Ex."), unless otherwise indicated, are to the supporting Declaration of Jeremy Jordan.

containing a URL, Facebook's servers will generate a thumbnail preview of the content at the destination website and display it for the user's review—including a brief description of the content and, if available, a relevant image pulled from the website (*id.*), as illustrated by the example below:



When the URL preview is generated, it is displayed for the message sender ***before sending the message***, so the sender may first verify and gain a sense of the content located at the URL. (*Id.*) Message recipients also receive a preview (if available) of any transmitted URL that is valid. (*Id.*)

3. *Facebook's Social Plugins and the Aggregated, Anonymous "Like" Count*. Facebook further enhances users' ability to share and discover relevant content by making its platform available on the Internet at large. Specifically, Facebook offers websites "social plugins," or units of embeddable code that allow people to share content using Facebook directly from third-party websites. (CAC ¶ 26.) For example, a third-party website may embed code for the Facebook "Like" button plugin on its website, enabling Facebook users to directly "Like" the content on the page and to share that action with their Facebook connections (without having to return to https://www.facebook.com or the Facebook mobile app to share the content). (*Id.*) The "Like" button plugin also may display an aggregate count of all "Likes" for that particular website (as shown in the example below):



This aggregate count of "Likes" presently includes (i) clicks on the "Like" button on Facebook, (ii) clicks on the "Like" button on the third-party website, (iii) the act of commenting on a link to that website, and (iv) any instance of non-message sharing of a link to that website. (*Id.* ¶ 36 (images of "Like" button plugin, including count).)[4] These aggregated "Likes" may help users discover content that matters to them. (*Id.* ¶ 32.)

C. The Alleged Basis for Plaintiffs' Lawsuit

The crux of the CAC alleges that, for some unspecified period of time before October 2012, whenever a Facebook user sent another Facebook user a message that included a URL, the aggregate "Like" count for that URL displayed on a social plugin increased by one (or two, due to a bug). (CAC ¶¶ 27, 35-37.) This is the basis for Plaintiffs' class action allegations of "wiretapping" and "eavesdropping"—i.e., that Facebook, which by definition already had their messages, "scanned [their] messages and then analyzed the URL in the link. If the website contained a Facebook 'Like' button, Facebook treated the content of Plaintiffs' private messages as an endorsement of the website . . . ." (*Id.* ¶ 2.) While they use the word "endorsement," Plaintiffs do not allege—nor could they—that any other person using Facebook (or anyone at all, other than the intended recipient of the message) was alerted to the fact that the message sender had shared the URL. (*Id.*) Nor do they allege that the particular user's sharing of the URL was ever disclosed to anyone else. They merely allege that an anonymous, aggregate number (*e.g.*, 45,273) was incrementally increased by one or two (*e.g.*, to 45,274 or 45,275). (*Id.* ¶¶ 27, 35-37.) They further allege, on "information and belief," and without any factual basis whatsoever, that "Facebook further retained these data for the current or future objective of accumulating and analyzing user data and thereafter refining user profiles and/or enhancing its targeted advertising efforts," thereby "increas[ing] its own value to—and revenue from—third-party advertisers." (*Id.* ¶¶ 30, 42.) Plaintiffs do not explain how anyone was harmed by these alleged practices, and indeed no one was harmed.

[4] CAC ¶¶ 35-37, citing Valentino-DeVries & Soltani, *How Private Are Your Private Facebook Messages?*, Wall St. J., Oct 3, 2012 (referencing developer guidance explaining the composition of global "Like" count).

D. Facebook's Clear Disclosures Regarding Message Information

Plaintiffs allege that "Facebook acted without [the] consent of its users" (*id*. ¶ 2), but their own pleadings establish the opposite. As detailed below, Facebook fully disclosed the practices challenged in the CAC and obtained consent to these practices from all users. Recognizing that these disclosures undermine their claims, Plaintiffs ***deleted*** the pertinent language when they amended their complaint. (*Compare* Dkt. No. 1 ¶ 83 (quoting Data Use Policy) *with* CAC ¶¶ 17-19 (referencing the Data Use Policy but not quoting relevant provision).)

By creating a free Facebook account—a necessary prerequisite to sending or receiving a Facebook message—every user agrees to Facebook's terms of service (i.e., Facebook's Statement of Rights and Responsibilities) and further affirms that she has reviewed the disclosures in Facebook's Data Use Policy.[5] (CAC ¶ 17; Ex. A at 1 (current Statement of Rights and Responsibilities, operative on December 30, 2013) and Ex. D (current Data Use Policy, operative on December 30, 2013).)[6] The Data Use Policy provides "important disclosures about how [a user] can use Facebook to share with others and how [Facebook] collect[s] and can use [user] content and information." (Ex. A at 1.) The three named Plaintiffs here—Matthew Campbell, Michael Hurley, and David Shadpour—each admit they established a Facebook account and reviewed and agreed to these policies before electing to use Facebook's free services. (*Id*. ¶¶ 69-71.)

---

[5] Specifically, "Facebook's main page states, 'By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy . . . Within this sentence, the word 'Terms' contains a hyperlink to Facebook's 'Statement of Rights and Responsibilities' . . . and the words 'Data Use Policy' contain a hyperlink, leading to Facebook's 'Data Use Policy.'" (CAC ¶ 17 (citations omitted).)

[6] The CAC relies on Facebook's terms and disclosures in effect on December 30, 2013. (CAC ¶ 17 n.2 ("Unless otherwise noted, a citation to any Facebook web page is to the version of that page in effect on December 30, 2013, the date on which the initial complaint was filed in this action.").) As explained in Facebook's Request for Judicial Notice, this Court may consider these documents because their contents are alleged in the CAC. *See, e.g.*, *In re Stac Elecs. Sec. Litig.*, 89 F.3d 1399, 1405 n.4 (9th Cir. 1996) ("[D]ocuments whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleading, may be considered in ruling on a Rule 12(b)(6) motion to dismiss.") (citation and quotation marks omitted); *In re iPhone 4S Consumer Litig.*, No. C 12-1127 CW, 2013 WL 3829653, at *6 (N.D. Cal. July 23, 2013) (holding the Court may take judicial notice of "webpages or documents . . . specifically referred to in the [complaint]"). Additionally, because Plaintiffs are alleging a class period that runs from December 2011 through October 2012 (CAC ¶ 59), Facebook also is attaching the versions of its Statement of Rights and Responsibilities and Data Use Policy that were in effect during this period. As explained in the Request for Judicial Notice, the Court also may properly consider these documents in deciding Facebook's Motion. *See* Request for Judicial Notice; *see also* Exs. B, C, E, and F.

The Data Use Policy informs users that Facebook receives and processes information, including when users send private messages:

> ***We receive data about you whenever you use or are running Facebook, such as when you*** look at another person's timeline, ***send or receive a message***, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or make purchases through Facebook.

(Ex. D at 2 (emphasis added).) Facebook also fully discloses how it will "use" the information it receives from Facebook users: "We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use." (*Id.* at 4.) The Data Use Policy also states that "in addition to helping people see and find things that you do and share, we may use the information we receive about you:

- as part of our efforts to keep Facebook products, services and integrations safe and secure;
- to protect Facebook's or others' rights or property; [. . .]
- to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you; [. . .]
- for internal operations, including troubleshooting, data analysis, testing, research and service improvement."

(*Id.*) The Data Use Policy further explains that Facebook does not "share information we receive about you with others unless we have: [1] received your permission; [2] given you notice, such as by telling you about it in this policy; or [3] removed your name and any other personally identifying information from it." (*Id.*)

Accordingly, by joining Facebook, all users acknowledge that they understand and agree that Facebook will receive and employ user data—***including information Facebook receives whenever a user sends or receives a message***—for a variety of routine business purposes, including, among other things, "efforts to keep Facebook products, services and integrations safe and secure," "to measure or understand the effectiveness of ads [users] and others see, including to deliver relevant ads to [the user]," and "for internal operations" such as "data analysis" or "service improvement." (Ex. D at 4.) Users also acknowledge that Facebook may share information, including with "developers that build the . . . websites [users] use," where Facebook "has removed your name and any other personally identifying information from it." (*Id.*) Stated differently, these disclosures—which Plaintiffs

strategically deleted from the CAC—expressly permit Facebook to aggregate instances of URLs shared across its service (including in messages) and provide that number (e.g., 45,273) in an anonymous, aggregate format to website developers. Facebook's policies *explicitly* disclose that Facebook will use the information it receives from user messages to serve routine business functions.[7]

E. Facebook's Access to Message Information

As the Data Use Policy makes clear, Facebook requires access to message information (as it does to all of the other information on its site) for myriad features crucial to providing its services. For example, as the sources cited in the CAC note, Facebook "analyze[s] messages to filter spam and to detect conversations that could be related to criminal behavior." (*See, e.g.*, Valentino-DeVries & Soltani*, How Private Are Your Private Facebook Messages?*, Wall St. J., Oct 3, 2012 (relied upon at CAC ¶ 35).)

Facebook also must process messages to render the basic features of the Messages product (such as language and format) and to facilitate content sharing. For example, as Plaintiffs admit, Facebook requires access to URLs contained within messages to generate the above-described URL preview functionality. (CAC ¶ 36.) This feature—which shows a thumbnail of the URL before the user sends the message—reduces the transmission of unintended content, as senders can preview the content of the destination website before transmitting, and recipients can preview a transmitted URL before visiting the destination website. (*Supra* pp. 5-6.)

Likewise, Facebook must process and store messages so that users have an accessible repository of their message content—a vital component of its Messages product. (CAC ¶ 23 (persons using Facebook Messages "can view the contents and history of your conversation"); *id*. ¶ 24, citing Seligstein, J., *See the Messages that Matter* ("All of your messages with someone will be together in one place, whether they are sent over chat, email or SMS. You can see everything you've discussed with each friend as a single conversation.").) Processing URLs in messages enables Facebook to

[7] Plaintiffs assert that "the definition of the 'Information We [Facebook] Receive About You' contained in the Data Use Policy excludes the content of users' private messages, including the content of users' private messages which include an embedded link to a URL" (CAC ¶ 19), but the Data Use Policy in fact explicitly *includes* messages. It states that "[w]e receive data about you whenever you use or are running Facebook, such as when you . . . send or receive a message . . . ." (Ex. D at 2.)

protect users, the product, and the site from threats and abusive behavior, and to offer services and features that enhance content sharing.

III. THE LEGAL STANDARDS GOVERNING THIS MOTION

Under Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss a complaint for failure to state a claim upon which relief can be granted. To survive a motion to dismiss for failure to state a claim, a complaint must state "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009) (Rule 8(a) "does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions"). This "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp.*, 550 U.S. at 555; *Iqbal*, 556 U.S. at 678 (a complaint that merely "tenders 'naked assertion[s]' devoid of 'further factual enhancement'" requires dismissal) (citing *Bell Atl. Corp.*, 550 U.S. at 557). A court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (citation omitted).

In ruling on a Rule 12(b)(6) motion, the Court may consider documents referenced in the complaint, *see, e.g.*, *No. 84 Emp'r-Teamster Joint Council Pension Trust Fund v. Amer. W. Holding Corp.*, 320 F.3d 920, 925 n.2 (9th Cir. 2003), and it need not accept allegations contradicted by judicially noticeable facts, *see, e.g.*, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000).

IV. ARGUMENT

A. Plaintiffs Fail to State a Claim Under the Wiretap Act

The Wiretap Act—enacted in 1968 and amended by the Electronic Communications Privacy Act ("ECPA") in 1986—provides for criminal penalties and a private right of action 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). A "specific Congressional goal[]" of the Wiretap Act was to "prevent[] wiretapping for criminal or tortious purposes." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001). The Act also prohibits the intentional "use" of unlawfully intercepted communications; where, as

here, the initial "interception" was not unlawful, this Section is inapplicable. 18 U.S.C. § 2511(1)(d) (unlawful to knowingly "use" the contents of a communication only when "the information was obtained through [an] interception . . . *in violation of this subsection*") (emphasis added).

The Wiretap Act is a penal statute, and "[i]t has long been settled that penal statutes are to be construed strictly . . . and that one is not to be subjected to a penalty unless the words of the statute plainly impose it." *United States v. Napier*, 861 F.2d 547, 548-49 (9th Cir. 1988) (citation and quotation marks omitted). Any ambiguity in the statute must be resolved in the defendant's favor by application of the rule of lenity. *See Skilling v. United States*, 561 U.S. 358, 410-11 (2010) ("[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.") (citation omitted); *United States v. Goyal*, 629 F.3d 912, 922 (9th Cir. 2010) (Kozinski, C.J., concurring) (noting that while "[c]ivil law often covers conduct that falls in a gray area of arguable legality[,] . . . criminal law should clearly separate conduct that is criminal from conduct that is legal"); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011) (stating that a "penal statute[] is to be strictly construed").

Plaintiffs' Wiretap Act claim fails as a matter of law for three separate reasons: (1) Plaintiffs have not alleged (and cannot allege) an actionable "interception;" (2) they consented to the alleged interceptions; and (3) the challenged conduct does not involve communications acquired "during transmission," but instead involves "stored communications" not governed by the Wiretap Act.

1. Plaintiffs Have Not Pled and Cannot Plead an Unlawful "Interception" Because the Complaint Acknowledges That Facebook's Acquisition of Plaintiffs' Messages Was "In the Ordinary Course of Its Business"

Plaintiffs have not pled—and cannot amend to plead—that any electronic communication was "intercept[ed]" by Facebook within the meaning of the Wiretap Act. Under the statute, "'intercept' means 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) (emphasis added). "[E]lectronic, mechanical, or other device," in turn, "means any device or apparatus which can be used to intercept a wire, oral, or electronic communication *other than*—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof . . . (ii) *being used by a provider of wire or electronic communication service* ***in the ordinary course of its business*** . . . ." 18

U.S.C. § 2510(5)(a)(ii) (emphasis added). In other words, if an alleged interception involves equipment used by the service provider in the ordinary course of its business, that equipment is not a "device" under the Act, and its use to receive the contents of a communication is not an unlawful "interception" as a matter of law. *See In re Google, Inc. Privacy Policy Litig.* ("*Google*"), No. 12-01382 PSG, 2013 WL 6248499, at *10 (N.D. Cal. Dec. 3, 2013) (holding that "as a provider of electronic communication services, [defendant] is immune from claims alleging interception by a 'device' based on equipment used 'by a provider of wire and electronic communication service in the ordinary course of business'"). Here, because (i) Plaintiffs acknowledge that Facebook is a provider of an electronic communication service and (ii) the very nature of Facebook's Messages product *requires* it to "acqui[re] . . . the contents" of electronic communications, there is no "interception" as a matter of law. Receiving users' content (including their messages) is necessary for the operation of Facebook's service, as Facebook specifically discloses in its Data Use Policy. On this basis alone, Plaintiffs' claim fails.

Federal courts have interpreted "ordinary course of business" in Section 2510(5)(a) to mean "routine" or "undertaken normally," and "justified by a valid business purpose" or "legitimate business reasons." *See, e.g.*, *United States v. Jiau*, 734 F.3d 147, 151-52 (2d Cir. 2013) (citation omitted); *Arias v. Mutual Central Alarm Serv., Inc.*, 202 F.3d 553, 554, 558-59 (2d Cir. 2000) (citation omitted); *Google*, 2013 WL 6248499, at *10-11.[8] Here, Plaintiffs allege that "[t]he core purpose of Facebook is to facilitate communication among its users. Facebook facilitates public communications via Facebook pages, and private communications via personal messages and chats." (CAC ¶ 16.) To "facilitate communication among its users," Facebook *must* acquire and store the contents of those communications on its servers. (*Id.* ¶¶ 20-24.)[9] Such conduct is by definition

[8] *Cf. First v. Stark Cnty Bd. of Comm'rs*, 234 F.3d 1268, at *4 (6th Cir. 2000) (requiring "a legitimate business purpose" even for law enforcement agency); *Knight v. City of New Orleans*, Civ.A. No. 89-3409, 1991 WL 126387, at *5-6 (E.D. La. July 1, 1991) (taping of conversation as part of "routine" investigation within "ordinary course of business"), *aff'd*, 968 F.2d 17 (5th Cir. 1992).

[9] Plaintiffs devote several paragraphs of their CAC to explaining how users may share their messages and posts with others—i.e., provide others with access to the content that Facebook already has stored for the user. (CAC ¶¶ 20-24.) The legislative history of the ECPA acknowledged that facilitating electronic communications requires the hosting entity to acquire a copy of it. (*Id.* ¶ 53, citing S. Rep. No. 99-541); *see* Request for Judicial Notice, Ex. 1 at 2 (S. Rep. 99-541 at *3) (stating that, unlike telephone service providers, data processing services and email providers "create

[Footnote continued on next page]

"routine," "undertaken normally," and "justified by a valid business purpose." Indeed, courts routinely have held that alleged "interceptions" of electronic communications *by electronic communication services* ("ECS")—the very nature of which requires that they receive, process, and sometimes store electronic communications—are within those entities' ordinary course of business and thus immune from suit under the Wiretap Act. *See, e.g., Kirch v. Embarq Mgmt. Co*., 702 F.3d 1245, 1250 (10th Cir. 2012) (finding that if the flow of plaintiffs' communications through the ECS's network was an "acquisition," then it was in the "ordinary course" of ECS's business because it allowed the ECS "access to no more of its users' electronic communications than it had in the ordinary course of its business as an [internet service provider]"); *Hall v. EarthLink Network, Inc*., 396 F.3d 500, 505 (2d Cir. 2005) (explaining that "[i]f [internet service providers] were not covered by the ordinary course of business exception, [they] would constantly be intercepting communications under ECPA because their basic services involve the 'acquisition of the contents' of electronic communication"). Under this precedent, Facebook's alleged conduct falls squarely within the "ordinary course of business" exemption. As an ECS that receives and stores the content of Plaintiffs' messages, ***Facebook has no choice but to receive Plaintiffs' messages***. Accordingly, Plaintiffs fail to allege an actionable "interception" as a matter of law.

Plaintiffs' real complaint is not that their communications were "intercepted" by Facebook; rather, they take issue with the manner in which Facebook *used* those communications—by allegedly increasing the aggregate "Like" count when a user included a URL in a message. As noted above, however, there is no violation of the "use" provision in the Wiretap Act (18 U.S.C. § 2511(1)(d)) when there is no unlawful interception. *Noel v. Hall*, 568 F.3d 743, 751 (9th Cir. 2009) ("use" provision only "protects against the dissemination of private communications that have been *unlawfully* intercepted") (emphasis in original); *Marsh v. Zaazoom Solutions, LLC*, No. 11-05226-

---

[Footnote continued from previous page]

electronic copies of private correspondence for later reference" and "[t]his information is processed for the benefit of the user").)

Plaintiffs do not challenge Facebook's processing and analysis of users' messages to provide various features of its messaging service. They allege only that "interception" for the intended use of increasing the "Like" count is not required. As discussed below, this conflates two different concepts—(i) acquisition and (ii) use.

YGR, 2012 WL 952226, at *16-18 (N.D. Cal. Mar. 20, 2012) (dismissing Section 2511(1)(d) claim for failure to allege an "interception"). Here, because there was no unlawful interception in the first place, Plaintiffs' Wiretap Act claim—under either Section (1)(a) or (1)(d)—fails as a matter of law.

Additionally, even if Plaintiffs' factual contentions regarding the "Like" button are credited, the alleged "use" of this information was in the "ordinary course" of Facebook's business.[10] Specifically, Plaintiffs allege that the "'Like' button, one of Facebook's principal social plug-ins, is commonly found on internet web pages." (CAC ¶ 32.) Plaintiffs then allege that Facebook's core business model is to "primarily generate[] revenue from targeted advertising" and assert—incorrectly—that a "fundamental means" of doing this is through the "Like" function, including by "systematically" scanning URLs contained in messages "for the [alleged] purpose of increasing the collection of data which it [allegedly] does directly employ in its targeted advertising." (*Id.* ¶¶ 3, 19, 25; *see also id.* ¶ 37 (alleging practice is explained in developer documentation), ¶¶ 41-42 ("The 'Like' function is crucial . . . for Facebook to generate data on users, and increase its own value . . . ."), ¶¶ 45, 57 (alleging Facebook scans messages "as a matter of course").)

While Plaintiffs' allegations are factually incorrect for a number of reasons, even if they were true, they do not establish any claim because systematic conduct of the type alleged by Plaintiffs that generates revenue for a company is the very essence of a company acting "in the ordinary course of its business." *See Google*, 2013 WL 6248499, at *10-11 (dismissing ECPA claim because "customary and routine business practices" included alleged interception of emails for the "legitimate business purpose[]" of providing targeted advertising; "Plaintiffs' own allegations make clear that the activities at issue here, concerning Google's core targeted advertising, is within its business' ordinary course."). Thus, even if the "use" Facebook allegedly made of Plaintiffs' communications were relevant to the "interception" inquiry—and it is not—the "ordinary course of business" exemption would continue to bar Plaintiffs' Wiretap Act claim.

[10] The Court need not credit Plaintiffs' conclusory assertion that the challenged conduct is not "in the ordinary course of business as a provider of an electronic communication service" (CAC ¶ 85), because it is contradicted by the factual content alleged in the CAC. *See, e.g.*, *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011).

Plaintiffs can be expected to argue in response that this Court cannot dismiss their claim because the phrase "ordinary course of business" is limited to interceptions that "facilitate[] the transmission of the communication at issue[.]" *In re Google Inc. Gmail Litig*. ("*Gmail*"), No.13–MD–02430–LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013). The argument fails for three reasons. First, as noted by another court in this District, such a requirement "does not square with the plain meaning of the statutory text[.]" *Google*, 2013 WL 6248499, at *10. As the court in *Google* explained, "[r]ather than narrowing the exemption to only the provision of electronic communications services itself, or some such narrower scope, Congress specifically chose the broader term 'business' that covers more far[-]ranging activity. For good measure, Congress also teamed the term 'business' with the terms 'ordinary course,' suggesting an interest in protecting a provider's customary and routine business practices." *Id.* The court went on to note that "[a]lthough the Ninth Circuit has yet to rule on the subject, other appellate courts [] have agreed that the 'ordinary course of business' exception is not limited to actions necessary to providing the electronic communication services ('ECS') at issue." *Id.* at *11 (discussing *Hall* and *Kirch*).

Second, in distinguishing the *Gmail* opinion, the court in *Google* observed that "the [*Gmail*] court's thorough analysis addressed allegations that Google's practices violated its own internal policies, further establishing that its actions [were] outside the course of its business. In this case, Plaintiffs allege no such violation of any internal policy, rendering Plaintiffs[']claim insufficiently stated to overcome the hurdle that Rule 12(b)(6) imposes." *Id*. at *11; *see also Gmail*, 2013 WL 5423918, at *11-12 (stating that defendant's conduct was found to be contrary to its own stated ordinary course of business in its Privacy Policy, precluding a finding that it fell within the exemption on a motion to dismiss). Here, Plaintiffs do not allege that Facebook violated its internal policies. In fact, it is precisely the opposite: they contend that Facebook engaged in the alleged conduct "as a matter of course" and publicly announced it to developers. (CAC ¶¶ 36-37, 45, 57.)

Third, as detailed above (*supra* pp. 13-15), Facebook's receipt of its users' electronic communications is in fact necessary to "facilitate the transmission of the communication at issue," and the ordinary course of business exemption therefore would apply even if the *Gmail* construction were correct.

2. Plaintiffs Consented to the Alleged Interceptions As a Matter of Law

Even if Plaintiffs could allege an actionable "interception" under the Wiretap Act, their ECPA claim still would fail because Plaintiffs consented—both expressly and impliedly—to the alleged interceptions. Consent is a complete defense to an ECPA claim:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or **where one of the parties to the communication has given prior consent to such interception** unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d) (emphasis added). Consent may be either "express" or "implied in fact from 'surrounding circumstances indicating that the [plaintiff] knowingly agreed'" to the interception of the communications at issue. *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (citations omitted). "[C]ourts have emphasized that 'consent' must be construed broadly under the Wiretap Act." *DoubleClick*, 154 F. Supp. 2d at 514 n.23 (citing cases); *see also United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) ("Congress intended the consent requirement to be construed broadly").

a. *Plaintiffs Expressly Consented to the Alleged "Interceptions."* Plaintiffs expressly consented to the challenged conduct when they accepted and consented to Facebook's Statement of Rights and Responsibilities and Data Use Policy. As discussed above, the Data Use Policy informs all Facebook users that:

- "***We receive data about you whenever you use or are running Facebook, such as when you*** look at another person's timeline, ***send or receive a message***, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or make purchases through Facebook."
- "We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and ***the developers that build the games, applications, and websites you use***."
- Facebook does not "share information we receive about you with others unless we have: [1] received your permission; [2] given you notice, such as by telling you about it in this policy; or [3] removed your name and any other personally identifying information from it."

(Ex. D at 2, 4 (all emphases added).)

In short, users consented to Facebook's receipt of data about them whenever they sent or received messages and authorized Facebook to use that data as specified, including disclosing—in an anonymous and aggregate format—the total number of users who had shared a URL, including in a message. These disclosures—which Plaintiffs admit they read and agreed to (*see* CAC ¶¶ 17, 69-71)—establish Plaintiffs' express consent as a matter of law.

Courts have dismissed similar Wiretap Act claims where express consent is apparent from the face of the complaint, from documents referenced in the complaint, or from documents of which courts may take judicial notice. *See, e.g.*, *Deering v. CenturyTel, Inc.*, No. CV–10–63–BLG–RFC, 2011 WL 1842859, at *2-3 (D. Mont. May 16, 2011) (granting motion to dismiss Wiretap Act claim upon finding that, "by using [defendant's] services despite the disclosures made in the Privacy Policy, [plaintiff] and the putative class members consented to the interception and use of their electronic communications"); *In re Vistaprint Corp. Mktg. & Sales Pracs. Litig.*, MDL No. 4:08–md–1994, 2009 WL 2884727, at *9 (S.D. Tex. Aug. 31, 2009) (granting motion to dismiss Wiretap Act claim as plaintiffs "'click[ed] Yes' in the designated spaces on the webpages, authoriz[ing] [defendant] to transfer that information").

b. *At a Minimum, Plaintiffs Impliedly Consented*. Even if Plaintiffs had not expressly consented to the alleged conduct—and they did—their Wiretap Act claim still would fail as a matter of law because Plaintiffs impliedly consented to the alleged practices. As noted above, consent may be implied from the overall circumstances of a particular communication. *See, e.g.*, *Van Poyck*, 77 F.3d at 292. "The critical question with respect to implied consent is whether the parties whose communications were intercepted had *adequate notice* of the alleged interception." *Gmail*, 2013 WL 5423918, at *12 (emphasis added); *see also Van Poyck*, 77 F.3d at 292 (surrounding context indicated that defendant had notice, and that the defendant had therefore "knowingly agree[d] to the surveillance") (internal quotations and citations omitted).

Given the features of the Messages product, Plaintiffs had full notice of, necessarily expected, and consented to Facebook's processing of message data. As discussed above, one feature of the Messages product is the helpful "URL preview" functionality, which processes a valid URL, generates a thumbnail preview of the URL content, and displays it for the user's review *before*

sending the message. (*Supra* pp. 5-6.) The CAC concedes that Plaintiffs sent messages *with full recognition* that Facebook processes their message content. (*Id.*; CAC ¶ 36 (acknowledging URL preview functionality).) Thus, Plaintiffs' Wiretap Act claim must be dismissed on this independent ground. *See, e.g.*, *Mortensen v. Bresnan Commc'n, L.L.C.*, No. CV 10–13–BLG–RFC, 2010 WL 5140454, at *4-5 (D. Mont. Dec. 13, 2010) (dismissing Wiretap Act claim after finding implied consent as a matter of law, where "circumstances 'indicate[d] that [the] party to the communication knew that the interception was likely and agreed to the monitoring'") (citation omitted); *cf. State v. Townsend*, 57 P.3d 255, 257, 260 (Wash. 2002) (interpreting Washington Privacy Act and explaining that an e-mail sender "impliedly consented to the recording of his email and [chat] communications" because "in order for e-mail to be useful it must be" processed and hosted).[11]

3. The Alleged Conduct Does Not Concern "Intercepting" a Communication "In Transmission"

Third, "to be 'intercepted' in violation of the Wiretap Act, [a communication] must be acquired *during transmission*, not while it is in electronic storage," because "[Congress] created" another statute, the Stored Communications Act ("SCA"), "for the express purpose of addressing 'access to *stored* . . . electronic communications[.]'" *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 878, 878-79 (9th Cir. 2002) (emphasis added) (quoting S. Rep. No. 99-541). Here, the purportedly objectionable use of Plaintiffs' messages occurred not while those messages were in transmission, but

[11] Plaintiffs have not pled any facts to support their bald assertion that Facebook intercepted their communications for the purpose of some unidentified "criminal or tortious act." (CAC ¶ 92.) Thus, they cannot overcome their consent to Facebook's acquisition of messages. *See, e.g.*, *Sussman v. ABC, Inc.*, 186 F.3d 1200, 1202-03 (9th Cir. 1999) ("Where the purpose [of a legitimate acquisition] is not illegal or tortious . . . the victims must seek redress elsewhere."); *Council on Amer.-Islamic Relations Action Network, Inc. v. Gaubatz*, Civil Action No. 09-02030(CKK), 2014 WL 1289467, at *12 (D.D.C. Mar. 27, 2014) (in order for the consent exception to be inapplicable, Plaintiff must show "either (1) that the primary motivation, or (2) that a determinative factor in the actor's motivation in intercepting the conversation was to commit a criminal or tortious act") (citations and quotation marks omitted); *Chance v. Avenue A., Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) (the "requisite showing of tortious or criminal purpose" requires that "such purpose . . . be either the 'primary motivation' or the 'determinative factor in the actor's motivation for intercepting' the communication") (citation omitted); *DoubleClick*, 154 F. Supp. 2d at 517-18 ("[P]laintiffs overreach when they argue that Congress and the courts created a general rule that 'tortious purpose' exists wherever an intentional action is later determined to have constituted a tort;" plaintiffs must plead "facts that could support an inference that [defendant] accessed plaintiffs' electronic communications with the 'insidious' intent to harm plaintiffs or others," not the mere "pursuit of commercial gain."). In fact, Plaintiffs explicitly contend that the challenged conduct was undertaken for the purpose of non-tortious, commercial gain. (CAC ¶¶ 2-4, 38, 42, 45, 48, 98, 118, 127-28.)

rather after they were stored on Facebook's servers. (*Supra* pp. 10-11.) Plaintiffs allege that Facebook received and stored message content (*see, e.g.*, CAC ¶ 23 (users "can view the contents and history of [their Messages] conversation")), and "*then* analyzed the URL," and only if the website contained a Facebook "Like" button did Facebook then add to the "Like" count (*see, e.g.*, *id*. ¶ 2 (emphasis added)). The sequence of actions that Plaintiffs allege involves use of content already in storage. And the SCA—not the Wiretap Act—governs access to an "electronic communication while it is in electronic storage," including "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2701(a); *id.* § 2510(17)(A). Plaintiffs' Wiretap Act claim fails for this additional reason.

B. Plaintiffs Fail to State a Claim Under California Penal Code Section 631

Plaintiffs also assert that Facebook's alleged conduct violates another criminal statute—California Penal Code Section 631, the state law corollary to the Wiretap Act—which punishes:

> [any] person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state[.]

Cal. Penal Code § 631(a).

This claim fails for the same reason as Plaintiffs' Wiretap Act claim: all parties consented to Facebook's processing of the alleged communications. As explained above, Facebook never acted "without the consent of all parties to the communication" or in any "unauthorized manner" in processing Plaintiffs' messages. (CAC ¶¶ 106, 111, 112.) Plaintiffs consented—both expressly and impliedly—to the alleged interceptions, and this consent bars their Section 631 claim. *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, No. 12–2358–SLR, 2013 WL 5582866, at *5-6 (D. Del. Oct. 9, 2013) (granting motion to dismiss § 631 claim against Google because "Google would have received the inputted information, including the URL, regardless of [the purported interception]"); *Powell v. Union Pac. R. Co.*, 864 F. Supp. 2d 949, 954-55 (E.D. Cal. 2012) (dismissing § 631 claim because there was no "unauthorized connection" or lack of "consent of all

parties to the communication"); *Membrila v. Receivables Perf. Mgmt., LLC*, No. 09–CV–2790–IEG (RBB), 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010) (same).

Additionally, while Plaintiffs contend in an entirely conclusory manner that their messages were intercepted "in transit" (CAC ¶ 108), their concessions that messages were *entirely contained* within Facebook's network during the purported "interception" belie this assertion. (*Id.* ¶ 48 (alleging "Facebook mined any and all transmissions across *its network*) (emphasis added).) *See also Hernandez v. Path, Inc.*, No. 12–CV–01515 YGR, 2012 WL 5194120, at *3, *5 (N.D. Cal. Oct. 19, 2012) (dismissing ECPA and Section 631 claims for, *inter alia*, failing to show "intercep[tion] [of] a communication in transit"; "Although Path allegedly transmitted the Class Members' [contacts] from [their] mobile devices to Path's servers, Path did not 'intercept' a 'communication' to do so").

C. Plaintiffs Fail to State a Claim Under California Penal Code Section 632

California Penal Code Section 632 punishes any person who "intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication[.]" Cal. Penal Code § 632(a). This claim also fails for several reasons.

First, as detailed above, Plaintiffs consented to all access and processing of their message data. (*Supra* pp. 17-19.) Second, Plaintiffs do not and cannot allege any "confidential communication," which the Act defines to include "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made . . . in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c). This is not a subjective test; "[t]he California Supreme Court has concluded that a conversation is confidential within the meaning of Section 632 'if a party to that conversation has an *objectively* reasonable expectation that the conversation is not being overheard or recorded.'" *Faulkner v. ADT Security Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013) (quoting *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 117 n.7 (2006) (quoting *Flanagan v. Flanagan*, 27 Cal. 4th 766, 776-77 (2002))) (emphasis added).

California courts uniformly have held that Internet communications are, by their very nature, not "confidential" within the meaning of Section 632. *See, e.g.*, *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010) (finding that Internet chats were not confidential "[d]espite [a user's] desire to keep the communication confidential" because he was communicating "via writing" on the Internet, and the privacy policy of the service further "warn[ed] users that chat dialogues can be archived, printed, and saved") (internal quotations omitted); *People v. Cho*, No. E049243, 2010 WL 4380113, at *4-5 (Cal. Ct. App. Nov. 5, 2010) (affirming trial court holding that chat conversations are not "confidential" under Section 632); *People v. Griffitt*, No. E049004, 2010 WL 5006815, at *6 (Cal. Ct. App. Dec. 9, 2010) ("Everyone who uses a computer knows that the recipient of e-mails and participants in chat rooms can print the e-mails and chat logs and share them with whoever they please, forward them or otherwise send them to others.").[12] Courts in this District have agreed. *See, e.g.*, *Gmail*, 2013 WL 5423918, at *23 (holding that plaintiffs did not "plausibly allege[] that they had an objectively reasonable expectation that their email communications were 'confidential' under the terms of section 632," because e-mails "are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet or print the communications").

As in the above cases, Plaintiffs have not alleged—nor could they—that they had any objectively reasonable expectation that their message communications were "confidential" under Section 632. Their type-written messages were, by their very nature, recorded by Facebook and stored in the sender and recipient's message history. (CAC ¶ 23 (users "can view the contents and history of [their Messages] conversation").) And, in the unlikely event users were unaware that information they shared with other users could be re-shared by those users, Facebook's Data Use Policy reiterated this well-known fact: "Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share

[12] This Court may consider unpublished state appellate decisions in construing California law. *See, e.g.*, *Bao Yi Yang v. Shanghai Gourmet, LLC*, 471 F. App'x 784, 788 (9th Cir. 2012); *Emp'rs Ins. of Wausau v. Granite State Ins. Co.*, 330 F.3d 1214, 1220 n.8 (9th Cir. 2003).

something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use." (Ex. D at 9.)

Nor can Plaintiffs establish that the alleged conduct constituted "eavesdropping" under the Act. California courts interpret "eavesdrop" to refer to "a third party secretly listening to a conversation between two other parties." *Thomasson v. GC Servs. Ltd. P'ship.*, 321 F. App'x 557, 559 (9th Cir. 2008) (citing *Ribas v. Clark*, 38 Cal. 3d 355, 363 (1985); *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975)). Here, Plaintiffs' own allegations and referenced documents establish that Facebook stored Plaintiffs' messages in the course of providing the Messages product (CAC ¶ 23), and announced these practices in the disclosures that Plaintiffs read (CAC ¶¶ 17, 69-71). Users send their messages to Facebook for the very purpose of storing them and making them available to the recipient. (CAC ¶ 23.) Facebook is not a "third party secretly listening," and therefore Facebook's services "cannot constitute eavesdropping, and cannot violate CIPA as a matter of law." *Thomasson*, 321 F. App'x at 559.

D. Plaintiffs Lack Standing to Pursue a Claim Under California's Unfair Competition Law

Plaintiffs' final claim alleges a violation of California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*; the "UCL"), but Plaintiffs do not and cannot allege facts to establish their standing to bring this claim.

A private party has standing to bring an action under the UCL only if he or she "has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Here, Plaintiffs have not shown that they suffered any "injury in fact," nor have they identified any "lost money or property." Plaintiffs' sole, conclusory allegation reciting the statutory elements of the UCL (CAC ¶ 129 (alleging that "Plaintiffs have suffered injury in fact and lost money or property as a result of Facebook's business acts or practices")) is legally insufficient to carry their pleading burden. *See, e.g.*, *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754–55 (9th Cir. 1994) (courts need not accept "legal conclusions cast in the form of factual allegations if those conclusions cannot reasonably be drawn from the facts alleged").

As with Plaintiffs' other claims, this is no mere technical defect that Plaintiffs can remedy with further amendment. Because Facebook is a free service, Plaintiffs cannot allege that they "lost"

any "money or property." Even the most generous reading of Plaintiffs' allegations—that they somehow "lost" the content of their messages or their control over the content of those messages (they did not)—does not establish the requisite standing. Even if publicly-accessible URLs contained in private messages could plausibly be alleged to have some "value," the Ninth Circuit recently reaffirmed that the amorphous "loss" of personal information cannot constitute lost money or property under the UCL. *See In re Facebook Privacy Litig.*, No. 12-15619, 2014 WL 1815489, at *1 (9th Cir. May 8, 2014) (affirming dismissal of plaintiffs' UCL claim because plaintiffs failed to allege that they lost money or property, even where plaintiffs alleged the dissemination of personal information and the lost sales value of that information); *see also Opperman v. Path, Inc.*, No. 13-cv-00453-JST, 2014 WL 1973378, at *24 (N.D. Cal. May 14, 2014) (dismissing UCL claim premised on defendant app developers' alleged appropriation of plaintiffs' personal contact lists from their mobile devices, as plaintiffs "failed" to show they "lost money or property"); *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) (granting motion to dismiss UCL claim for unauthorized access to personal information for lack of standing, and noting that "[n]umerous courts have held that a plaintiff's 'personal information' does not constitute money or property under the UCL"); *RockYou, Inc.*, 785 F. Supp. 2d at 863 (rejecting the claim that a plaintiff's PII exposed as the result of a data breach constituted "lost money or property" under the UCL; "plaintiff has failed to plead the heightened degree of injury required under the UCL").

Plaintiffs cannot establish standing to support a UCL claim.[13]

[13] Even if Plaintiffs had standing, their UCL claim still would fail because they have failed to plausibly allege any "unlawful, unfair or fraudulent" business acts or practices. Cal. Bus. & Prof. Code § 17200; *Shroyer v. New Cingular Wireless Servs.*, 622 F.3d 1035, 1043-44 (9th Cir. 2010). Additionally, their request for "restitution" (CAC p. 28) should be stricken because Plaintiffs admit they did not pay any money to Facebook, and there is nothing to "restore" to them. Cal. Bus. & Prof. Code § 17203; *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1149 (2003) (explaining that "restore," as it is used in the UCL, is limited to the restitution of "money or property that defendants took directly from plaintiff" or "money or property in which [plaintiff] has a vested interest" such as earned wages that are due and payable); *Bradstreet v. Wong*, 161 Cal. App. 4th 1440, 1458 (2008) (affirming finding that restitution would be inappropriate where defendants "obtained no money or gains from which to disgorge or pay restitution").

E. This Court Should Strike Plaintiffs' Request for Injunctive Relief Because the Challenged Conduct Ceased in October 2012

Finally, even if any of Plaintiffs' claims could survive this Motion—and Facebook respectfully submits they cannot—at a minimum, this Court should strike Plaintiffs' request for injunctive relief because, by Plaintiffs' own admission, the conduct of including instances of URLs sent in user messages in the anonymous, aggregate "Like" count ended almost two years ago. (CAC ¶ 59 n.3.) Plaintiffs may not "enjoin" conduct that already ceased. *See, e.g.*, *City of Los Angeles v. Lyons*, 461 U.S. 95, 109 (1983) ("requirements for seeking an injunction in a federal court" include "showing that [plaintiff] is realistically threatened by a repetition of his experience"); *Ice Cream Distribs. of Evansville, LLC v. Dreyer's Grand Ice Cream, Inc.*, 487 F. App'x 362, 363 (9th Cir. 2012) (injunctive relief inappropriate where "alleged misconduct ended [5 years prior] and [plaintiff] [did] not allege a threat of continuing misconduct"); *Sun Microsystems, Inc. v. Microsoft Corp.*, 188 F.3d 1115, 1123 (9th Cir. 1999) (vacating district court's entry of injunction because defendant had discontinued the challenged practices).

V. CONCLUSION

Because the shortcomings in the CAC go to Plaintiffs' theory, and are not mere technical pleading defects, allowing further amendment would be futile. The CAC therefore should be dismissed with prejudice. *See, e.g.*, *Sisseton-Wahpeton Sioux Tribe v. United States*, 90 F.3d 351, 356 (9th Cir. 1996) (affirming denial of leave to amend as further amendment "would be redundant and futile").

Dated: June 17, 2014

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: /s/
Joshua A. Jessen

Attorneys for Defendant FACEBOOK, INC.