FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE: ZYNGA PRIVACY LITIGATION, NANCY WALTHER GRAF; RICHARD BEILES; HOWARD L. SCHREIBER; JOHN SWANSON; LELLANIAH ADAMS; VALERIE GUDAC; WILLIAM J. O'HARA; IRIS PHEE; ZENA CARMEL-JESSUP; SHELLEY ALBANI; CHRISTOPHER BROCK; KAREN BRYANT; BARBARA MOSKOWITZ, *Plaintiffs-Appellants*, v. ZYNGA GAME NETWORK, INC., a Delaware corporation, *Defendant-Appellee*.	No. 11-18044 D.C. No. 5:10-cv-04680-JW

IN RE: FACEBOOK PRIVACY LITIGATION,

MIKE ROBERTSON, as representative of the class,
Plaintiff-Appellant,

v.

FACEBOOK, INC., a Delaware corporation,
Defendant-Appellee.

No. 12-15619

D.C. No. 5:10-cv-02389-JW

OPINION

Appeals from the United States District Court
for the Northern District of California
James Ware, District Judge, Presiding

Argued and Submitted
January 17, 2014—San Francisco, California

Filed May 8, 2014

Before: Arthur L. Alarcón, Richard C. Tallman, and Sandra S. Ikuta, Circuit Judges.

Opinion by Judge Ikuta

SUMMARY*

Electronic Communications Privacy Act

In consolidated cases, the panel affirmed the district court's dismissal of claims for violations of the Wiretap Act and the Stored Communications Act, two chapters within the Electronic Communications Privacy Act, when Facebook, Inc., a social networking company, and Zynga Game Network, Inc., a social gaming company, allegedly disclosed confidential user information to third parties.

The panel held that the plaintiffs in both cases failed to state a claim because they did not allege that either Facebook or Zynga disclosed the "contents" of a communication, a necessary element of their ECPA claims.

COUNSEL

Adam J. Levitt (argued), Grant & Eisenhofer P.A., Chicago, Illinois; Francis M. Gregorek, Betsy C. Manifold, Rachele R. Rickert, and Patrick H. Moran, Wolf Haldenstein Adler Freeman & Herz LLP, San Diego, California; Jonathan Shub, Seeger Weiss LLP, Los Angeles, California; Michael J. Aschenbrener, Aschenbrener Law, PC, San Francisco, California, for Plaintiffs-Appellants Nancy Walther Graf, John Swanson, Richard Beiles, Howard L. Schreiber, Lellaniah Adams, Valerie Gudac, William J. O'Hara, Iris

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

Phee, Zena Carmel-Jessup, Shelley Albani, Christopher Brock, Karen Bryant, and Barbara Moskowitz.

Kassra Nassiri (argued), Nassiri & Jung LLP, San Francisco, California; John Joseph Manier, Nassiri & Jung LLP, Los Angeles, California, for Plaintiff-Appellant Mike Robertson.

Richard L. Seabolt (argued), Oliver E. Benn, Suzanne R. Fogarty, Duane Morris LLP, San Francisco, California, for Defendant-Appellee Zynga Game Network, Inc.

Aaron Martin Panner (argued), Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C., Washington, D.C.; Matthew D. Brown, Cooley LLP, San Francisco, California; James M. Penning, Cooley LLP, Palo Alto, California, for Defendant-Appellee Facebook, Inc.

OPINION

IKUTA, Circuit Judge:

The plaintiffs in these cases appeal the district court's dismissal with prejudice of their claims for violations of the Wiretap Act and the Stored Communications Act, two chapters within the Electronic Communications Privacy Act of 1986 (ECPA). The plaintiffs allege that Facebook, Inc., a social networking company, and Zynga Game Network, Inc., a social gaming company, disclosed confidential user information to third parties. We have consolidated these cases for this opinion and conclude that the plaintiffs in both cases have failed to state a claim because they did not allege that either Facebook or Zynga disclosed the "contents" of a

communication, a necessary element of their ECPA claims. We therefore affirm the district court.[1]

I

Facebook operates Facebook.com, a social networking website. Zynga is an independent online game company that designs, develops, and provides social gaming applications that are accessible to users of Facebook. To understand the claims at issue, some background on Facebook and internet communication is necessary.

A

Social networking and gaming websites provide an internet forum where users can interact with each other and share information. Anyone may register to use Facebook's social networking site, but registrants must provide their real names, email addresses, gender, and birth dates. Facebook does not charge any fees to sign up for its social networking service. Upon registration, Facebook assigns each user a unique Facebook User ID. The User ID is a string of numbers, but a user can modify the ID to be the user's actual name or invented screen name. Facebook considers the IDs to be personally identifiable information.

Facebook users upload information to the site to share with others. Users frequently share a wide range of personal information, including their birth date, relationship status,

[1] In a memorandum disposition filed simultaneously with this opinion, we affirm in part and reverse in part the district court's dismissal of the state law claims in *Robertson v. Facebook*, ___ Fed. App'x ___ (9th Cir. 2014). The state law claims are not before us in *Graf v. Zynga*.

place of residence, religion, and interests, as well as pictures, videos, and news articles. Facebook arranges this information into a profile page for each user. Users can make their profiles available to the public generally, or limit access to specified categories of family, friends, and acquaintances.

To generate revenue, Facebook sells advertising to third parties who want to market their products to Facebook users. Facebook helps advertisers target their advertising to a specific demographic group by providing them with users' demographic information. For example, a purveyor of spring training baseball memorabilia can choose to display its ads to males between the ages of 18 and 49 who like baseball and live in Phoenix, Arizona, on the theory that the members of that particular demographic group will be more likely to click on the ad and view the offer. Nevertheless, Facebook's privacy policy states that it will not reveal a user's specific identity and that only anonymous information is provided to advertisers.

In addition to its social networking and advertising services, Facebook offers a platform service that allows developers to design applications that run on the Facebook webpage. Zynga is one such developer. It offers free social gaming applications through Facebook's platform that are used by millions of Facebook users. Until November 30, 2010, Zynga's privacy policy stated that it did "not sell or rent your 'Personally Identifiable Information' to any third party."

B

A brief review of how computers communicate on the internet is helpful to understand what happens when a

Facebook user clicks on a link or icon. The hypertext transfer protocol, or HTTP, is the language of data transfer on the internet and facilitates the exchange of information between computers. R. Fielding, et al., *Hypertext Transfer Protocol —HTTP/1.1*, § 1.1 (1999), http://www.w3.org/Protocols/HTTP/1.1/rfc2616.pdf.[2] The protocol governs how communications occur between "clients" and "servers." A "client" is often a software application, such as a web browser, that sends requests to connect with a server. A server responds to the requests by, for instance, providing a "resource," which is the requested information or content. *Id.* §§ 1.3, 1.4. Uniform Resource Locators, or URLs, both identify a resource and describe its location or address. *Id.* §§ 3.2, 3.2.2. And so when users enter URL addresses into their web browser using the "http" web address format, or click on hyperlinks, they are actually telling their web browsers (the client) which resources to request and where to find them. *Id.* § 3.2.2.

The "basic unit of HTTP communication" is the message, which can be either a request from a client to a server or a response from a server to a client. *Id.* §§ 1.3, 4.1. A request message has several components, including a request line, the resource identified by the request, and request header fields. *Id.* § 5. The request line specifies the action to be performed on the identified resource. *Id.* § 5.1. Often, the request line includes "GET," which means "retrieve whatever information . . . is identified by the" indicated resource, or "POST," which

[2] We take judicial notice of the current version of the publicly-available HTTP specification, RFC 2616, because it is referenced and relied on in the body of the complaint in *Robertson v. Facebook*, and no party has questioned the authenticity of this document. *See Marder v. Lopez*, 450 F.3d 445, 448 (9th Cir. 2006).

requests that the server accept a body of information enclosed in the request, such as an email message. *Id.* §§ 9.3, 9.5. For example, if a web user clicked a link on the Ninth Circuit website to access recently published opinions (URL: http://www.ca9.uscourts.gov/opinions/), the client request line would state "GET /opinions/ HTTP/1.1," which is the resource, followed by "Host: www.ca9.uscourts.gov," a location header that specifies the website that hosts the resource. *Id.* § 5.1.2.

Other request headers follow the request line and "allow the client to pass additional information about the request, and about the client itself, to the server." *Id.* § 5.3. A request header known as the "referer"[3] provides the address of the webpage from which the request was sent. *Id.* § 14.36. For example, if a web user accessed the Ninth Circuit's website from the Northern District of California's webpage, the GET request would include the following header: "Referer: http://www.cand.uscourts.gov/home." A client can be programmed to avoid sending a referer header. *Id.* § 15.1.2.

During the period at issue in this case, when a user clicked on an ad or icon that appeared on a Facebook webpage, the web browser sent an HTTP request to access the resource identified by the link. The HTTP request included a referer header that provided both the user's Facebook ID and the address of the Facebook webpage the user was viewing when the user clicked the link. Accordingly, if the Facebook user clicked on an ad, the web browser would send the referer header information to the third party advertiser.

[3] Referer, although a misspelling of "referrer," is the term of art in the industry. *Id.* § 14.36.

To play a Zynga game through Facebook, a registered Facebook user would log into the user's Facebook account and then click on the Zynga game icon within the Facebook interface. For example, if a user wanted to access Zynga's popular FarmVille game, the user would click the FarmVille icon, and the user's web browser would send an HTTP request to retrieve the resource located at http://apps.facebook.com/onthefarm. Like the HTTP request to view an ad on Facebook, the HTTP request to launch a Zynga game contained a referer header that displayed the user's Facebook ID and the address of the Facebook webpage the user was viewing before clicking on the game icon. In response to the user's HTTP request, the Zynga server would load the game in an inline frame[4] on the Facebook website. The inline frame allows a user to view one webpage embedded within another; consequently, a user who is playing a Zynga game is viewing both the Facebook page from which the user launched the game and, within that page, the Zynga game.

According to the relevant complaint, Zynga programmed its gaming applications to collect the information contained in the referer header, and then transmit this information to advertisers and other third parties. As a result, both Facebook and Zynga allegedly disclosed the information provided in the referer headers (i.e., the user's Facebook IDs and the address of the Facebook webpage the user was viewing when the user clicked the link) to third parties.

[4] An inline frame is an element of HyperText Markup Language (HTML), which is the standard language of displaying internet content in a web browser.

C

In the separate proceedings before us here, the plaintiffs filed consolidated class action complaints against Facebook and Zynga, alleging violations of ECPA based on Facebook and Zynga's disclosure of the information contained in referer headers to third parties. In *Robertson v. Facebook*, the plaintiffs alleged that Facebook violated the Stored Communications Act, 18 U.S.C. § 2702(a)(2). In *Graf v. Zynga*, the plaintiffs alleged violations of both the Stored Communications Act and the Wiretap Act, 18 U.S.C. § 2511(3)(a). In both cases, the district court determined that the plaintiffs had standing because they alleged a violation of their statutory rights, but nevertheless granted Facebook and Zynga's motions to dismiss the plaintiffs' claims under both the Wiretap Act and the Stored Communications Act for failure to state a claim. The district court read the complaints as alleging that the plaintiffs intended for Facebook, Zygna, or the third parties to receive the communications. Because both the Wiretap Act and the Stored Communications Act allow disclosures to intended recipients, 18 U.S.C. §§ 2511(3)(a), 2702(b)(1), the district court concluded that the complaints did not state a claim for violation of the Wiretap Act or Stored Communications Act. These appeals followed.

II

We review de novo the district court's dismissal for failure to state a claim and we "must construe the complaint in favor of the complaining party." *Arakaki v. Lingle*, 477 F.3d 1048, 1056 (9th Cir. 2007). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on

its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* We may affirm the district court's judgment on any ground supported by the record. *Classic Media, Inc. v. Mewborn*, 532 F.3d 978, 990 (9th Cir. 2008).

Before ECPA, the chief statutory protection for communications was the Wiretap Act, enacted in 1968, which regulated only the "aural acquisition of the contents of any wire or oral communication," 18 U.S.C. § 2510(4) (1970). In 1986, Congress enacted ECPA to update statutory privacy protections that had failed to keep pace with the technological developments in the 17 years since the Wiretap Act was enacted. S. Rep. 99-541, at 1–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556–57; *see generally* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 378–82 (2014).

ECPA focused on two types of computer services that were prominent in the late 1980s: electronic communications services (e.g., the transfer of electronic messages, such as email, between computer users) and remote computing services (e.g., the provision of offsite computer storage or processing of data and files). *See generally Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895, 900–02 (9th Cir. 2008), *rev'd in nonrelevant part sub nom. City of Ontario v. Quon*, 560 U.S. 746 (2010); Office of Tech. Assessment, U.S. Cong., *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 45–48 (1985). Title I of ECPA amended the existing Wiretap Act. As relevant here, the amended Wiretap Act provides that (with

certain exceptions), "a person or entity" (1) "providing an electronic communication service to the public" (2) "shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof)" (3) "while in transmission on that service" (4) "to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a). The "contents" of a communication are defined as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). Even if a disclosure is otherwise prohibited by § 2511(3)(a), an electronic communications service provider can reveal the contents of communications transmitted on its service "with the lawful consent of the originator or any addressee or intended recipient of such communication." *Id.* § 2511(3)(b)(ii).

Title II of ECPA, termed the Stored Communications Act, covers access to electronic information stored in third party computers. *Id.* §§ 2701–12. The relevant provision here imposes requirements on providers of remote computing services that are similar to the requirements of the Wiretap Act discussed above. Under the Stored Communications Act, "a person or entity" (1) "providing remote computing service to the public" (2) "shall not knowingly divulge to any person or entity the contents of any communication" (3) "which is carried or maintained on that service . . . on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service" (4) "solely for the purpose of providing storage or computer processing services to such subscriber or customer," unless the provider is authorized to access the contents of any such communications

to provide other services. *Id.* § 2702(a)(2). Also, like the Wiretap Act, the Stored Communications Act allows a provider of covered services to "divulge the contents of a communication" to "an addressee or intended recipient of such communication," or "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." *Id.* § 2702(b)(1), (3).

The Stored Communications Act incorporates the Wiretap Act's definition of "contents." *See id.* § 2711(1). It also differentiates between contents and record information. Section 2702(c)(6) permits an electronic communications service or remote computing service to "divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by [§ 2702](a)(1) or (a)(2)) . . . to any person other than a governmental entity." Although there is no specific statutory definition for "record," the Stored Communications Act provides examples of record information in a different provision that governs the government's power to require a provider of electronic communications service or remote computing service to disclose such information. *Id.* § 2703(c). According to § 2703(c), record information includes, among other things, the "name," "address," and "subscriber number or identity" of "a subscriber to or customer of such service," but not "the contents of communications." *Id.* § 2703(c)(2)(A), (B), (E). In other words, the Stored Communications Act generally precludes a covered entity from disclosing the contents of a communication, but permits disclosure of record information like the name, address, or client ID number of the entity's customers in certain circumstances.

ECPA provides a cause of action to third parties for violations of the Wiretap Act and the Stored Communications Act. Under the Wiretap Act, "any person whose wire, oral, or electronic communication is . . . disclosed . . . may in a civil action recover from the person or entity . . . such relief as may be appropriate," including damages and attorney's fees, *id.* § 2520(a), and under the Stored Communications Act, "any . . . person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity . . . which engaged in that violation such relief as may be appropriate," *id.* § 2707(a).

III

On appeal, the plaintiffs argue that the district court erred in holding that Facebook, Zynga, and the third parties were the intended recipients of the referer headers containing the user's Facebook IDs and the URLs. According to the plaintiffs, because their complaints allege that Facebook and Zynga had privacy policies which precluded them from providing personally identifiable information to third parties, the exceptions in §§ 2511(3) and 2702(b) for intended recipients are inapplicable. Facebook and Zynga, in turn, raise a number of arguments as to why we should affirm the district court. Because the plaintiffs' complaints suffer from a common defect—they fail to allege that either Facebook or Zynga divulged the contents of a communication to a third party—we focus our analysis on this single ground.[5] In doing

[5] Facebook and Zynga argue that the plaintiffs lack standing because they have not suffered any concrete or particularized injury arising from the alleged disclosure of users' Facebook IDs and URL information to

so, we express no opinion on the other elements of an ECPA claim.

A

Because the plaintiffs alleged that Facebook and Zynga violated ECPA by disclosing the HTTP referer information to third parties, we must determine whether such information is the "contents" of a communication for purposes of 18 U.S.C. §§ 2511(3)(a) and 2702(a)(2).

To answer this question, we first must determine Congress's intended meaning of the word "contents." "In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole." *K-Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988). We start with the plain language of the statutes. *See Gwaltney of Smithfield, Ltd. v. Chesapeake Bay Found., Inc.*, 484 U.S. 49, 56 (1987). For purposes of §§ 2511(3)(a) and 2702(a), the word "contents" is defined as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. §§ 2510(8), 2711(a). Because the words "substance, purport, or meaning" are not further defined, we consider the ordinary meaning of these terms, including their

---

third parties. This argument has been foreclosed by *Edwards v. First American Corp.*, which held that a plaintiff demonstrates an injury sufficient to satisfy Article III when bringing a claim under a statute that prohibits the defendant's conduct and grants "'persons in the plaintiff's position a right to judicial relief.'" 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)). Because the plaintiffs allege that Facebook and Zynga are violating statutes that grant persons in the plaintiffs' position the right to judicial relief, we conclude they have standing to bring this claim. *See* 18 U.S.C. §§ 2520, 2707.

dictionary definition. *See Wilderness Soc'y v. U.S. Fish & Wildlife Serv.*, 353 F.3d 1051, 1061 (9th Cir. 2003) (en banc), *amended by* 360 F.3d 1374 (9th Cir. 2004) (en banc). A dictionary in wide circulation during the relevant time frame provides the following definitions: (1) "substance" means "the characteristic and essential part," *Webster's Third New International Dictionary* 2279 (1981); (2) "purport" means the "meaning conveyed, professed or implied," *id.* at 1847; and (3) "meaning" refers to "the thing one intends to convey . . . by language," *id.* at 1399. These definitions indicate that Congress intended the word "contents" to mean a person's intended message to another (i.e., the "essential part" of the communication, the "meaning conveyed," and the "thing one intends to convey").

The "language and design of the statute as a whole," *K-Mart Corp.,* 486 U.S. at 291, sheds further light on the meaning of "contents" by indicating that "contents" does not include "record" information. Specifically, the Stored Communications Act provides that a covered service provider "may divulge a record or other information pertaining to a . . . customer" but may not divulge "the contents of communications." 18 U.S.C. §§ 2702(c), 2703(c)(1). Customer record information (which can be disclosed under certain circumstances) includes the "name," "address," and "subscriber number or identity" of a subscriber or customer. *Id.* § 2702(c)(2). Accordingly, we conclude that "contents" does not include such record information.

This conclusion is confirmed by ECPA's amendments to the Wiretap Act enacted in 1968. Before ECPA, the Wiretap Act defined "contents" as including "the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 18 U.S.C.

§ 2510(8) (1982). When it enacted ECPA, Congress amended the definition of "contents" to eliminate the words "identity of the parties to such communication," indicating its intent to exclude such record information from its definition of "contents." *See* Pub. L. 99-508 § 101(a)(5).

Accordingly, we hold that under ECPA, the term "contents" refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication. We have previously made this distinction between contents and record information. *See United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009) (holding that information about a telephone call's "origination, length, and time" was not "contents" for purposes of § 2510(8), because it contained no "information concerning the substance, purport or meaning of [the] communication"). And this conclusion is consistent with the reasoning of our sister circuits. *See Gilday v. Dubois*, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (holding that a device that "captures electronic signals relating to the [personal identification number] of the caller, the number called, and the date, time and length of the call" does not capture the contents of communications and therefore "is not within the ambit of the Wiretap Act"); *see also In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 305–06 (3d Cir. 2010) (holding that cell phone users' location data is not content information under the Stored Communications Act).

B

We must next determine whether the plaintiffs plausibly alleged that the referer header information at issue here

constituted the "contents of any communication," 18 U.S.C. §§ 2511(3)(a), 2702(a), that is, "any information concerning the substance, purport, or meaning of a communication," *id.* § 2510(8).

The referer header information that Facebook and Zynga transmitted to third parties included the user's Facebook ID and the address of the webpage from which the user's HTTP request to view another webpage was sent. This information does not meet the definition of "contents," because these pieces of information are not the "substance, purport, or meaning" of a communication. A Facebook ID identifies a Facebook user and so functions as a "name" or a "subscriber number or identity." *Id.* §§ 2702(c)(6), 2703(c)(2)(A), (E). Similarly, the webpage address identifies the location of a webpage a user is viewing on the internet, and therefore functions like an "address." *Id.* § 2703(c)(B). Congress excluded this sort of record information from the definition of "contents." *See id.* §§ 2702(c)(6), 2703(c)(2)(A), (B), (E).

The plaintiffs argue that the referer header discloses content information, because when the referer header provides the advertiser with a Facebook ID (which, at the election of the user, may have been changed to a user name) along with the address of the Facebook page the user was previously viewing, an enterprising advertiser could uncover the user's profile page and any personal information made available to the public on that page. But the statutes at issue in these cases do not preclude the disclosure of personally identifiable information; indeed, they expressly allow it. *See id.* §§ 2702(c)(6), 2703(c)(2) (allowing providers to disclose subscribers' names, addresses, telephone connection records, length of service, telephone numbers, subscriber numbers, credit card numbers, and bank account numbers under certain

circumstances). There is no language in ECPA equating "contents" with personally identifiable information. Thus, an allegation that Facebook and Zynga disclosed personally identifiable information is not equivalent to an allegation that they disclosed the contents of a communication.

The plaintiffs also argue that record information can become content if the record is the subject of a communication, as in an email message saying "here's my Facebook ID number," or "you have to check out this website." Such was the case in *In re Pharmatrak*, where the First Circuit recognized an ECPA violation when an entity intercepted the content of the sign-up information customers provided to pharmaceutical websites, which included their "names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website," and provided this information to third parties. 329 F.3d 9, 15, 18–19 (1st Cir. 2003). Because the users had communicated with the website by entering their personal medical information into a form provided by a website, the First Circuit correctly concluded that the defendant was disclosing the contents of a communication. But the complaints here do not plausibly allege that Facebook and Zynga divulged a user's communications to a website; rather, they allege that Facebook and Zynga divulged identification and address information contained in a referer header automatically generated by the web browser. Unlike the information disclosed in *Pharmatrak*, the information allegedly disclosed by Facebook and Zynga is record information about a user's communication, not the communication itself. ECPA does not apply to such disclosures.

Finally, the plaintiffs rely on cases analyzing when disclosure of a URL may provide the contents of a communication, rather than record information, for purposes of Fourth Amendment protections. The plaintiffs rely on a footnote in *United States v. Forrester*, where we noted that a "URL, unlike an IP address, identifies the particular document within a website that a person views," and therefore "might be more constitutionally problematic." 512 F.3d 500, 510 n.6 (9th Cir. 2008). *Forrester* quoted a district court case for the proposition that if a user entered a search phrase into a search engine, "'that search phrase would appear in the URL after the first forward slash,'" and disclosure of that URL "'would reveal content.'" *Id.* (quoting *In re Application of U.S. for an Order Authorizing Use of a Pen Register & Trap On (xxx) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005)). Based on this footnote, the plaintiffs argue that the webpage addresses contained in the referer headers in this case revealed the contents of a communication, because they disclose specific information regarding a webpage that a user previously viewed. For example, they allege that "if a Facebook user who was gay and struggling to come out of the closet was viewing the Facebook page of a gay support group, and then clicked on an ad, the advertiser would know . . . that s/he was viewing the Facebook page of a gay support group just before navigating to their site."

This argument fails. As a threshold matter, our task in interpreting ECPA is to discern Congress's intent, *see Gwaltney*, 484 U.S. at 56–58, and our Fourth Amendment jurisprudence is largely irrelevant to this enterprise of statutory interpretation. But even assuming that Congress considered the body of law regarding persons' reasonable expectation of privacy under the Fourth Amendment in

making the statutory distinction between content and record information at issue in ECPA, we disagree with the plaintiffs' claims. Under the Fourth Amendment, courts have long distinguished between the contents of a communication (in which a person may have a reasonable expectation of privacy) and record information about those communications (in which a person does not have a reasonable expectation of privacy). *Forrester*, 512 F.3d at 509–11. Thus the warrantless installation of pen registers, which capture only the telephone numbers that are dialed and not the calls themselves, does not violate the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 745–46 (1979). Courts have made a similar distinction between the outside of an envelope and its contents in mail cases. *See, e.g., United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *United States v. Hernandez*, 313 F.3d 1206, 1209–10 (9th Cir. 2002). And we have allowed the warrantless collection of email and IP addresses under the same reasoning because email and IP addresses "constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Forrester*, 512 F.3d at 510. So *Forrester* does not support the plaintiffs, but rather reinforces the distinction between contents and record information that we have discerned in ECPA.

Nor does *Forrester*'s dicta about URL information being "content" under some circumstances help the plaintiffs. Information about the address of the Facebook webpage the user was viewing is distinguishable from the sort of communication involving a search engine discussed in *Forrester*. As noted in the district court opinion cited by *Forrester*, a Google search URL not only shows that a user is using the Google search engine, but also shows the specific search terms the user had communicated to Google. *In re*

Application, 396 F. Supp. 2d at 49. Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication. But the referer header information at issue here includes only basic identification and address information, not a search term or similar communication made by the user, and therefore does not constitute the contents of a communication.

IV

In order for the plaintiffs to state a claim under the Wiretap Act and Stored Communications Act, they must plausibly allege that Facebook and Zynga divulged the "contents" of a communication. Because information disclosed in the referer headers at issue here is not the contents of a communication as defined in ECPA, the plaintiffs cannot state a claim under those statutes. Accordingly, we affirm the district court's dismissal with prejudice.

AFFIRMED.