11-10-2015

In Re: Google Inc Cookie Place

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 13-4300

IN RE: GOOGLE INC. COOKIE PLACEMENT
CONSUMER PRIVACY LITIGATION

William Gourley; Jose M. Bermudez; Nicholas Todd Heinrich; Lynne Krause,

Appellants

On Appeal from the United States District Court
for the District of Delaware
(No. 1-12-md-02358)
District Judge: Honorable Sue L. Robinson

Argued December 11, 2014

Before: FUENTES, FISHER, and KRAUSE, *Circuit Judges*

(Opinion Filed: November 10, 2015)

Jason O. Barnes, Esq. **[ARGUED]**
Barnes & Associates
219 East Dunklin Street, Suite A
Jefferson City, MO 65101

James P. Frickleton, Esq.
Bartimus Frickleton Robertson & Gorny
11150 Overbrook Road, Suite 250
Leawood, KS 66211

Edward D. Robertson, Jr., Esq.
Bartimus Frickleton Robertson & Gorny
715 Swifts Highway
Jefferson City, MO 65109

Brian R. Strange, Esq.
Strange & Carpenter
12100 Wilshire Boulevard
Suite 1900
Los Angeles, CA 90025

Attorneys for Plaintiff-Appellants

Colleen Bal, Esq.
Michael H. Rubin, Esq. **[ARGUED]**
Wilson, Sonsini, Goodrich & Rosati
One Market Street
Spear Tower, Suite 3300
San Francisco, CA 94105

Michael H. Rubin, Esq.
Wilson, Sonsini, Goodrich & Rosati
One Market Street
Spear Tower, Suite 3300
San Francisco, CA 94105

Anthony J. Weibell, Esq.
Wilson, Sonsini, Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94304

Attorneys for Defendant-Appellee Google Inc.

Edward P. Boyle, Esq.
David N. Cinotti, Esq.
Venable
1270 Avenue of the Americas
24th Floor, Rockefeller Center
New York, NY 10020

Travis S. Hunter, Esq.
Rudolf Koch, Esq.
Richards, Layton & Finger
920 North King Street
One Rodney Square
Wilmington, DE 19801

Attorneys for Defendant-Appellee Vibrant Media Inc.

Lisa M. Coyle, Esq.
Ropes & Gray
1211 Avenue of the Americas
New York, NY 10036

Douglas H. Meal, Esq.
Ropes & Gray
800 Boylston Street
Prudential Tower
Boston, MA 02199

Attorneys for Defendant-Appellees Media Innovation Group LLC and WPP PLC

OPINION OF THE COURT

FUENTES, *Circuit Judge*:

This class action arises from allegations that the defendants, who run internet advertising businesses, placed tracking cookies on the plaintiffs' web browsers in contravention of their browsers' cookie blockers and defendant Google's own public statements. At issue in this appeal is the District Court's dismissal of each of the nine claims brought by the plaintiffs. As follows, we will affirm in part, vacate in part, and remand to the District Court for additional proceedings.

I. Background

A. Internet Advertising and Cookie-Based Tracking

In most users' experience, webpages appear on browsers as integrated collages of text and images. As a technical matter, this content is delivered and aggregated from multiple independent servers. This includes advertising content, which is typically drawn from "third-party" servers owned by the advertisers themselves. The defendants in this case are internet advertising companies, and this suit concerns their practices in serving advertisements to the browsers of webpage visitors.

The delivery of advertising content from third party servers to webpage visitors' browsers is a highly technical process involving a series of communications between the visitor's browser, the server of the visited website, and the server of the advertising company. In its specifics:

> The host website leaves part of its webpage blank where the third-party advertisements will appear. Upon receiving a "GET" request from a user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, instructing the browser to send a "GET" request to the third-party company charged with serving the advertisements for that particular webpage. . . . The third-party server responds to the GET request by sending the advertisement to the user's browser, which then displays it on the user's device. The entire process occurs within milliseconds and the third-party content appears to arrive simultaneously with the first-party

> content so that the user does not discern any separate GET requests from the third-parties.[1]

As the defendants deliver their advertisements directly to users from their own servers, the defendants have the capacity to vary how they populate their rented webpage space. This capacity permits targeting by which the defendants may serve different advertisements to different visitors. The general principle is that the more that an advertisement is tailored to its audience—sneakers for runners, legal pads for lawyers—the greater the advertisement's expected value. Here, the value of customization, combined with the capacity for individuated advertisement service, impels internet advertisers to surmise whatever they can about each particular person requesting webpage content.

As pled in the complaint:

> To inject the most targeted ads possible, and therefore charge higher rates to buyers of the ad space, these third-party companies . . . compile the [i]nternet histories of users. The third-party advertising companies use "third-party cookies" to accomplish this goal. In the process of injecting the advertisements into the first-party websites, the third-party advertising companies also place third-party cookies on user's computing devices. Since the advertising companies place advertisements on multiple sites, these cookies allow these companies to

---

[1] Compl. ¶ 41.

> keep track of and monitor an individual user's web activity over every website on which these companies inject ads.[2]
>
> These third-party cookies are used by advertising companies to help create detailed profiles on individuals . . . by recording every communication request by that browser to sites that are participating in the ad network, including all search terms the user has entered. The information is sent to the companies and associated with unique cookies—that is how the tracking takes place. The cookie lets the tracker associate the web activity with a unique person using a unique browser on a device. Once the third-party cookie is placed in the browser, the next time the user goes to a website with the same [d]efendant's advertisements, a copy of that request can be associated with the unique third-party cookie previously placed. Thus the tracker can track the behavior of the user . . . .[3]

B. Cookie Blocking, Circumvention, Deceit, and Discovery

Individually tailored webpage advertisements are now ubiquitous. But, where cookie-based tracking is concerned, leading web browsers have designed built-in features to prevent the installation of cookies by third-party servers. The

---

[2] Compl. ¶ 45.

[3] Compl. ¶ 46.

complaint calls them "cookie blockers." The cookie blockers of two browsers are at issue in this case. One is Microsoft's Internet Explorer, which featured an "opt-in" cookie blocker that a user could elect to activate. The other is Apple's Safari browser, which featured an "opt-out" cookie blocker that was activated by default. The complaint notes that the main Apple website page dedicated to Safari advertised its opt-out cookie blocker as a unique feature, stating that, "to better protect[] your privacy[,] Safari accepts cookies only from the websites you visit."[4] Likewise, the Safari browser labeled its default cookie setting as "Block cookies: From third parties and advertisers."[5]

According to the complaint, the Safari and Internet Explorer cookie blockers were well-known to industry participants, including as to their existence, functionality, and purpose. More is alleged about Google in particular. Google's Privacy Policy explained that "most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent."[6] Google provided further assurances about the Safari cookie blocker specifically. Google offered a proprietary cookie blocker, a so-called "opt-out cookie" that, when downloaded, would prevent the installation of tracking cookies. On the public webpage Google maintained to describe its opt-out cookie, Google assured visitors that "Safari is set by default

---

[4] Compl. ¶ 69.

[5] Compl. ¶ 71.

[6] Compl. ¶ 80.

to block all third party cookies. If you have not changed those settings, this option essentially accomplishes the same thing as setting the opt-out cookie."[7]

In February 2012, Stanford graduate student Jonathan Mayer published an online report revealing that Google and the other defendants had discovered, and were surreptitiously exploiting, loopholes in both the Safari cookie blocker and the Internet Explorer cookie blocker.[8] Safari's cookie blocker turns out to have had a few exceptions, one of which was that it permitted third-party cookies if the browser submitted a certain form to the third-party. Because advertisement delivery does not, in the ordinary course, involve such forms, the exception ought not have provided a pathway to installing advertiser tracking cookies. But according to Mayer's report, Google used code to command users' web browsers to automatically submit a hidden form to Google when users visited websites embedded with Google advertisements. This covert form triggered the exception to the cookie blocker, and, used widely, enabled the broad placement of cookies on Safari browsers notwithstanding that the blocker—as Google publicly acknowledged—was designed to prevent just that. The other defendants, meanwhile, accomplished similar circumventions. As a result, the defendants could—and did—place third-party cookies on browsers with activated blockers.

---

[7] Compl. ¶ 79.

[8] Compl. ¶ 75; Jonathan Mayer, Web Policy Blog, *Safari Trackers* (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/.

Mayer's findings were concurrently published in the Wall Street Journal[9] and drew the attention of the Federal Trade Commission and a consortium of state attorneys general. The Department of Justice filed suit under the Federal Trade Commission's authorizing statute in the Northern District of California, and the action resolved by way of a stipulated order providing for a $22.5 million civil penalty.[10] Google further agreed to certain forward-looking conditions related to internet privacy, but admitted no past acts or wrongdoing.[11] Google similarly reached a $17 million

---

[9] Compl. ¶ 74; Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall Street Journal (Feb. 17, 2012), *http://www.wsj.com/article_email/SB10001424052970204880404577225380456599176*.

[10] Compl. ¶¶ 166-68; *United States v. Google, Inc.*, N.D. Cal. No. 12-cv-4177, Docs. 1, 30; *see also* Press Release, Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser: Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order* (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[11] Compl. ¶ 169; *Google*, N.D. Cal. No. 12-cv-4177, Docs. 30, 32.

settlement with 38 state attorneys general, including the California Attorney General.[12]

C. The Instant Suit

Following Mayer's report, a series of lawsuits were filed in federal district courts around the country. Those

---

[12] *See* Settlement Agreement between Google, Inc. & the Attorneys General of the States of Alabama, Arizona, Arkansas, California, Connecticut, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, and Wisconsin, as well as the District of Columbia, *available at* http://www.ncdoj.gov/News-and-Alerts/News-Releases-and-Advisories/Related-Information/Google-Safari-Settlement-Agreement.aspx; *see also* Claire Cain Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. Times (Nov. 18, 2013), *http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html*. The settlement with the state attorneys general post-dated the District Court's dismissal order, and thus the filing of the complaint. Because the fact of this settlement is well-documented and officially recognized by the many governmental parties to it, and because the public policy implications of imposing liability on defendant Google are highly relevant to the disposition of two of the plaintiffs' claims, we will take judicial notice of Google's settlement with the state attorneys general.

lawsuits were consolidated by the Multi-District Litigation panel and assigned to Judge Sue Robinson of the District of Delaware. This appeal is from the District Court's dismissal of that consolidated case.

The consolidated case was presented to the District Court as a putative class action, and four named plaintiffs—our appellants here—filed a consolidated class action complaint. The putative class consists of:

> all persons in the United States of America who used the Apple Safari or Microsoft Internet Explorer web browsers and who visited a website from which doubleclick.net (Google's advertising serving service), PointRoll, Vibrant Media, Media Innovation Group, or WPP cookies were deployed as part of a scheme to circumvent the users' browsers' settings to block such cookies and which were thereby used to enable tracking of the class members['] [i]nternet communications without consent.[13]

The complaint asserts three federal law claims against all defendants. Count I claims violation of the federal Wiretap Act, 18 U.S.C. § 2510 et seq. Count II claims violation of the Stored Communications Act, 18 U.S.C § 2701. And Count III claims violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

---

[13] Compl. ¶ 191.

The complaint also asserts six California state law claims against Google only. Count IV claims violation of the privacy right conferred by the California Constitution. Count V claims intrusion upon seclusion under California tort law. Count VI claims violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. Count VII claims violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502. Count VIII claims violation of the California Invasion of Privacy Act, Cal. Penal Code § 630 et seq. And Count IX claims violation of the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750 et seq.

The defendants moved to dismiss the entire complaint for lack of Article III standing and for failure to state any claim. Without definitively resolving the standing challenge, the District Court agreed with the defendants that the allegations in the complaint did not give rise to any action, and on that basis dismissed the complaint under Rule 12(b)(6).[14] On appeal, the plaintiffs challenge the dismissal of each of their nine claims, and the defendants renew their contention that the plaintiffs lack Article III standing.

II. Injury in Fact

Before we reach the merits, we address the defendants' argument that the plaintiffs lack standing. "[T]he question of standing is whether the litigant is entitled to have the court

---

[14] *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 988 F. Supp. 2d 434 (D. Del. 2013).

decide the merits of the dispute or of particular issues."[15] A core requirement of standing is that the plaintiff have suffered an injury in fact. The defendants contend that the plaintiffs fail to demonstrate injury in fact because they make insufficient allegations of pecuniary harm.

For purposes of injury in fact, the defendants' emphasis on economic loss is misplaced. In assessing injury in fact, we look for an "invasion . . . which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical."[16] Though the "injury must affect the plaintiff in a personal and individual way,"[17] this standard does not demand that a plaintiff suffer any particular type of harm to have standing. Consequently, and contrary to the contentions of the defendants, a plaintiff need not show actual monetary loss for purposes of injury in fact. Rather, "the actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing."[18] Sure enough, the Supreme Court itself

---

[15] *Storino v. Borough of Point Pleasant Beach*, 322 F.3d 293, 296 (3d Cir. 2003) (internal quotation marks omitted). "If [the] plaintiffs do not possess Article III standing, both the District Court and this Court lack subject matter jurisdiction to address the merits of [the] plaintiffs' case." *Id*. (internal quotation marks omitted).

[16] *Pichler v. UNITE*, 542 F.3d 380, 390 (3d Cir. 2008) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)).

[17] *Lujan*, 504 U.S. at 560 n.1.

has permitted a plaintiff to bring suit for violations of federal privacy law absent any indication of pecuniary harm.[19]

The plaintiffs here base their claims on highly specific allegations that the defendants, in the course of serving advertisements to their *personal* web browsers, implanted tracking cookies on their *personal* computers. Irrespective of whether these allegations state a claim, the events that the complaint describes are concrete, particularized, and actual as to the plaintiffs. To the extent that the defendants believe that the alleged conduct implicates interests that are not legally protected, this is an issue of the merits rather than of standing.

The plaintiffs show injury in fact, and we have jurisdiction to address the merits of their claims.[20]

---

[18] *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982) (alteration in original) (internal quotation marks omitted); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 183 (2000) ("[E]nvironmental plaintiffs adequately allege injury in fact when they aver that they use the affected area and are persons for whom the aesthetic and recreational values of the area will be lessened by the challenged activity.") (internal quotation marks omitted).

[19] *See Doe v. Chao*, 540 U.S. 614, 641 (2004) (Ginsburg, J., dissenting) ("Doe has standing to sue, the Court agrees, based on 'allegations that he was "torn . . . all to pieces" and "greatly concerned and worried" because of the disclosure of his Social Security number and its potentially "devastating" consequences.'").

[20] The District Court had subject matter jurisdiction over the plaintiffs' federal law claims under 28 U.S.C. § 1331. It had

III. Federal Claims Against All Defendants

We first address the three federal law claims brought against all defendants. For the following reasons, we will vacate the dismissal of the plaintiffs' Wiretap Act claim but affirm the dismissal of the plaintiffs' claims under the Stored Communications Act and Computer Fraud and Abuse Act.

A. The Federal Wiretap Act

The federal Wiretap Act is codified at 18 U.S.C. § 2510 et seq. A plaintiff pleads a prima facie case under the Act by showing that the defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device."[21] Of

---

subject matter jurisdiction over the plaintiffs' state law claims for two independent reasons: supplemental jurisdiction under 28 U.S.C. § 1367, and diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). We have jurisdiction over the District Court's final dismissal under 28 U.S.C. § 1291.

[21] *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003) (citing 18 U.S.C. § 2511(1)(a)); *see also* §§ 2510(4) (providing that "'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"), 2520 (providing a private right of action)).

several statutory exceptions, one is the exception of § 2511(2)(d). Section 2511(2)(d) provides that, ordinarily, no cause of action will lie against a private person "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."[22]

1. Acquisition of "Content"

The District Court dismissed the plaintiffs' Wiretap Act claim on the basis that the defendants' alleged conduct did not involve the acquisition of communications "content." While the plaintiffs allege that the defendants acquired and tracked the URLs they visited, the Act defines "contents" as "any information concerning the substance, purport, or meaning of th[e] communication [at issue]."[23] The District Court held that, "[a]s described by their name, 'Universal Resource Locators,' . . . . a URL is a location identifier and does not 'concern [ ] the substance, purport, or meaning' of an electronic communication.'"[24]

---

[22] The exception does not apply if "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).

[23] 18 U.S.C. § 2510(8).

[24] *In re: Google*, 988 F. Supp. 2d at 444 (final alteration in original) (quoting 18 U.S.C. § 2510(8)).

In *Smith v. Maryland*, the Supreme Court made clear the important difference between extrinsic information used to route a communication and the communicated content itself.[25] In *Smith*, the Supreme Court found no Fourth Amendment violation from the government's warrantless use of a pen register.[26] Distinguishing its holding in *Katz v. United States*[27] that warrantless wiretapping violated the Fourth Amendment, the Supreme Court explained that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[28] Rather, the Court explained, pen registers "disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[29]

Smith's differentiation between the "means of establishing communication" and the "purport of a[] communication"[30] looms large in federal surveillance law.

---

[25] 442 U.S. 735 (1979).

[26] *Id*. at 745-46.

[27] 389 U.S. 347 (1967).

[28] *Id.* at 741 (emphasis in original).

[29] *Id*. (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)).

[30] *Id.*

Whereas the Wiretap Act governs the interception of communications "content[],"[31] the separate federal Pen Register Act governs the acquisition of non-content "dialing, routing, addressing, [or] signaling information."[32] As the House of Representatives noted in its Report regarding the enactment of the PATRIOT Act, "the statutorily prescribed line between a communication's contents and non-content information[] [is] a line identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*."[33]

Since *Smith*, location identifiers have classically been associated with non-content "means of establishing communication."[34] Nevertheless, the District Court's

---

[31] 18 U.S.C. § 2510(4); *see also id.* § 2511(1)(a).

[32] 18 U.S.C. §§ 3121(c), 3127(3)-(4). Where surveillance by law enforcement is concerned, "[t]he difference in the standards for court approval of content-capturing wiretaps and non-content-capturing pen registers is dramatic—content information is protected by a 'super-warrant,' non-content information by a rubber stamp." Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105, 2120 (2009).

[33] Report of the House of Representatives Judiciary Committee, H. Rep. No. 107-236, at 53, *available at* http://www.gpo.gov/fdsys/pkg/CRPT-107hrpt236/pdf/CRPT-107hrpt236-pt1.pdf.

[34] *Smith*, 442 U.S. at 741 (quoting *New York Tel. Co.*, 434 U.S. at 167).

categorical assessment that location identifiers *never* "concern[] the substance, purport, or meaning" of a communication misses the mark.[35] Often, a location identifier serves no routing function, but instead comprises part of a communication's substance.[36] As a leading treatise on criminal procedure explains:

> [T]he line between content and non-content information is inherently relative. If A sends a letter to B, asking him to deliver a package to C at a particular address, the contents of that letter are contents from A to B but mere non-content addressing information with respect to the delivery of the package to C. In the case of e-mail, for example, a list of e-mail addresses sent as an attachment to an e-mail communication from one person to another are contents rather than addressing information. In short, whether an e-mail address is content or non-content information depends entirely on the circumstances.[37]

In essence, addresses, phone numbers, and URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function. If an address,

---

[35] 18 U.S.C. § 2510(8).

[36] *See generally* Orin Kerr, *Websurfing and the Wiretap Act*, Wash. Post. (June 4, 2015), *https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/*.

[37] Wayne R. LaFave, et al., 2 Crim. Proc. § 4.4(d) (3d ed.).

phone number, or URL is instead part of the substantive information conveyed to the recipient, then by definition it is "content."

The different ways that an address can be used means, as Professor Orin Kerr puts it, that "the line between contents and metadata is not abstract but contextual with respect to each communication."[38] Thus, there is no general answer to the question of whether locational information is content. Rather, a "content" inquiry is a case-specific one turning on the role the location identifier played in the "intercepted" communication.

Here, the complaint does not make clear whether the tracked URLs were acquired by the defendants from communications in which those URLs played a routing function. This is not, however, fatal to the plaintiffs' claim.

In a declassified opinion analyzing whether there was statutory authority for a National Security Agency surveillance program, the Foreign Intelligence Surveillance Court observed that the government possessed trap and trace authority over "dialing, routing, addressing, and signaling information . . . provided, however, that such information shall not include the contents of any information."[39] The

---

[38] Kerr, *Websurfing and the Wiretap Act*.

[39] *[Redacted]*, No. PR/TT [Redacted] (FISA Ct. 2010), *available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf* at 26 (quoting 18 U.S.C. § 3127(4)).

Surveillance Court read this to mean that, for purposes of federal surveillance law, information may well serve both a routing function and a content function. Noting the breadth of the statutory descriptions of routing information and "content," the Surveillance Court concluded that routing information and "content" are not mutually exclusive categories, but rather ones that Congress expressly contemplated to be occasionally coextensive.[40] Proceeding to identify exemplary areas where routing information and "content" overlap, the Surveillance Court pointed, "in particular," to URL queries that involve reproduction of a search phrase entered by a user into a search engine.[41] Quoting the District of Massachusetts, the Surveillance Court explained that, "if a user runs a search using an [i]nternet search engine, the 'search phrase would appear in the URL after the first forward slash' as part of the addressing information, but would also reveal contents, *i.e.*, the '"substance" and "meaning" of the communication . . . that the user is conducting a search for information on a particular topic.'"[42] For an example from another context, the court pointed to post-cut-through digits in the phone context "as

---

[40] *Id.* at 31.

[41] *Id.* at 32.

[42] *Id.* at 32 (final alteration in original) (quoting *In re Application of the U.S.*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005)).

dialing information, some of which also constitutes contents."[43]

The decision of the Surveillance Court is instructive in several ways relevant to our analysis here. The first of these is that, to the extent that the statutory definitions and conceptual categories of content and routing information overlap, Congress expressly contemplated the possibility of such an overlap. For the reasons stated by the Surveillance Court, we are persuaded that, under the surveillance laws, "dialing, routing, addressing, and signaling information" may also be "content."

Second, the Surveillance Court takes the position that queried URLs can be content as well as routing information, for instance in the case of URLs that reproduce search engine inquiries. Though some district courts have held that a URL is never content, the Surveillance Court decision is part of a growing chorus that some, if not most, queried URLs do contain content. In *In re Zynga Privacy Litigation*, the Ninth Circuit took the position that queried URLs are content if, but only if, they reproduce words from a search engine query.[44]

---

[43] *Id.* at 33. As the Southern District of Texas has explained, "'[p]ost-cut-through dialed digits' are any numbers dialed from a telephone after the call is initially setup or 'cut-through.'" *In re Application of the U.S.*, 441 F. Supp. 2d 816, 818 (S.D. Tex. 2006). "Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like." *Id*.

[44] 750 F.3d 1098, 1108-09 (9th Cir. 2014) ("[A] user's request to a search engine for specific information could

In *United States v. Forrester*, meanwhile, a different panel of the Ninth Circuit noted that warrantless capture of URLs generally "might be more constitutionally problematic" than warrantless capture of IP addresses.[45] The *Forrester* court explained that "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's [i]nternet activity."[46] Akin to *Forrester* is the stance taken by the House Judiciary Committee in its PATRIOT Act report, which stated that a pen register order "could not be used to collect information other than 'dialing, routing, addressing, and signaling' information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or

---

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 referrer 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.").

[45] 512 F.3d 500, 510 n.6 (9th Cir. 2008). An "IP address" is "[t]he 10-digit identification tag used by computers to locate specific websites." Black's Law Dictionary (10th ed. 2014) ("Internet-protocol address").

[46] 512 F.3d at 510 n.6; s*ee also* Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. at 2136 ("[S]tandard URLs . . . reveal every bit as much content as do URLs containing search terms.").

the name of a requested file or article."[47] Though none of these authorities offer detailed reasoning on why they draw the "content" line where they do, what they have in common is that they assess whether a URL involves "contents" based on how much information would be revealed by disclosure of the URL.

Third, the Surveillance Court's example of post-cut-through digits in the telephone context—i.e. numbers dialed from a telephone after a call is already setup or "cut-through"—hints at a different reason why queried URLs might be considered content. A number of courts apart from the Surveillance Court—most prominently the D.C. Circuit—have found such digits to comprise communications content beyond the permissible scope of a pen register.[48] URL queries

---

[47] *See* H. Rep. No. 107-36, at 53.

[48] *See U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 462 (D.C. Cir. 2000) ("Post-cut-through dialed digits can . . . represent call content. For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers."); *In re Applications of the U.S.*, 515 F. Supp. 2d 325, 339 (E.D.N.Y. 2007) ("[T]he "Government's request for access to all post-cut-through dialed digits is not clearly authorized by the Pen/Trap Statute, and . . . granting such a request would violate the Fourth Amendment . . . ."); *In re Application of the U.S.*, 441 F. Supp. 2d at 827 ("Post-cut-through dialed digits . . . are not available to law enforcement under the Pen/Trap Statute.").

bear functional analogues to this process, in that different portions of a queried URL may serve to convey different messages to different audiences. For instance, the domain name portion of the URL—everything before the ".com"—instructs a centralized web server to direct the user to a particular website, but post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user.[49]

As stated above, we agree with the Surveillance Court that routing information and content are not mutually exclusive categories. And between the information revealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that—at a minimum—some queried URLs qualify as content.[50] Indeed, the

---

[49] *See generally* Jonathan Mayer, *Web Browsing (Under the Pen Register Act and Wiretap Act*), (Nov. 28, 2014). https://www.youtube.com/watch?v=7vFha-af7GE

[50] We need not make a global determination as to what is content, and why, in the context of queried URLs. Lack of consensus, the complexity and rapid pace of change associated with the delivery of modern communications, and the facileness of direct analogy to mail and telephone cases counsel the utmost care in considering what is, and what is not, "content" in the context of web queries. Indeed, when it comes to differentiating content from non-content, Professor Kerr describes queried URLs as "the most difficult and discussed case." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1030 n. 93 (2010); *see also* Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't*, 97 Nw. U. L. Rev. 607, 644-48 (2003); *cf.* Tokson,

defendants' counsel acknowledged as much at argument.[51] Because the complaint pleads a broad scheme in which the defendants generally acquired and tracked the plaintiffs' internet usage, we are satisfied that this scheme, if it operated as alleged, involved the collection of at least some "content" within the meaning of the Wiretap Act.[52]

The Content/Envelope Distinction in Internet Law, 50 Wm. & Mary L. Rev. at 2136 ("Perhaps because it is so intuitive that search terms in a URL should be considered content, the treatment of content-revealing communications data is undertheorized in computer surveillance scholarship.").

[51] Oral Arg. Tr. at 44 ("We acknowledge that there may be URLs that could constitute content.").

[52] Because the URL information acquired and tracked by the defendants is "content" for purposes of the plaintiffs' Wiretap Act claim, we need not consider whether the defendants acquired and/or tracked other "content" from the electronic transmissions at issue. Our understanding of the factual position of the defendants is that their cookies operate by adding a unique sequence of letters and/or numbers to any GET request transmitted from the user browser hosting the cookie to the advertiser server that set the cookie. *See* Oral Arg. Tr. at 25 ("The cookie doesn't acquire anything. . . . The cookie doesn't look for anything. It just sits on the browser and gets sent along with information that would otherwise be sent."); *id.* at 26 ("Maybe it's sort of like a bookmark. Information gets sent anyway every day, all the time. And then a cookie is placed. And thereafter the same information is sent, except that the cookie is there, too. It's unique. It's not personally identifying. It has nothing to do with the actual

2. Section 2511(2)(d)

According to the defendants, even if we find that the plaintiffs adequately plead the acquisition of "content," we may affirm nevertheless under § 2511(2)(d). Section 2511(2)(d) sets forth that "[i]t shall not be unlawful . . . 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 . . . 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." The defendants contend that they were the intended recipients of—and thus "parties" to—any electronic transmissions that they acquired and tracked, and that, as they committed no secondary criminal or tortious act, their conduct cannot have been unlawful under the statute.

a. How the Information at Issue Was Acquired

Before we can assess whether the defendants were "parties" to the electronic transmissions at issue, we must first identify what, exactly, are the transmissions at issue.

In the portion of the complaint devoted to the plaintiffs' Wiretap Act claim, the complaint states that "the [d]efendants' third-party web tracking permitted them to

---

information that's being sent at that time."). This is consistent with our understanding of the allegations of the plaintiffs, as discussed in detail below.

record information that [c]lass [m]embers exchanged with first-party websites . . . which [the d]efendants intercepted while not a party to those communications (hence third-party tracking)[.]"[53] It continues to plead that "the defendants' third-party tracking intercepted the class members' communications while they were in transit from the class members' computing devices to the web servers of the first-party websites the class members used their browsers to visit."[54]

The highly specific allegations contained in the body of the complaint, however, give no credence to the complaint's later allegations that the defendants acquired their internet history information from transmissions between the plaintiffs' browsers and first-party websites. With respect to the mechanics of the defendants' acquisition of web browsing information, the interior of the complaint says that, "[u]pon receiving a []GET[] request from a user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, instructing the browser to send a []GET[] request to the third-party company charged with serving the advertisements for that particular webpage."[55] As to Google specifically, the complaint likewise pleads that "the server hosting the publisher's webpage . . . instructs the user's web browser to send a GET request to Google to display the relevant advertising information for the

---

[53] Compl. ¶ 206.

[54] Compl. ¶ 208.

[55] Compl. ¶ 41.

space on the page for which Google has agreed to sell display advertisements."[56]

If users' browsers directly communicate with the defendants about the webpages they are visiting—as the complaint pleads with particularity—then there is no need for the defendants to acquire that information from transmissions to which they are not a party. After all, the defendants would have the information at issue anyway. Underscoring that there are direct transmissions between the plaintiffs and the defendants, the complaint notes that the defendants place cookies on web browsers "in the process of injecting the advertisements,"[57] which are "serve[d] . . . directly from the third-party company's servers rather than going through the individual website's server."[58]

The complaint's descriptions of how tracking is accomplished, meanwhile, further supports that the information was captured from the plaintiffs' GET requests to the defendants. According to the complaint:

> The information is sent to the companies and associated with unique cookies -- that is how the tracking takes place. The cookie lets the tracker associate the web activity with a unique person using a unique browser on a device. Once the third-party cookie is placed in the

---

[56] Compl. ¶ 86.

[57] Compl. ¶ 45.

[58] Compl. ¶ 41.

> browser, the next time the user goes to a webpage with the same [d]efendant's advertisements, a copy of that request can be associated with the unique third-party cookie previously placed. Thus the tracker can track the behavior of the user[.]"[59]

If the information at issue is sent to the defendants in the ordinary course, then this description of the cookies makes sense. This is because in such a scenario the defendants need only associate information to track it, which can be successfully accomplished by affixing an identifier to that information. This is precisely how the complaint describes the defendants' cookies' function. With respect to Google, the complaint pleads installation of Google's "id" cookie, "which is a unique and consistent identifier given to each user by Google for its use in tracking persons across the entire spectrum of websites on which Google places . . . cookies."[60] Google allegedly uses this cookie to "identif[y] users," such that "the placement of the third-party cookies, placed by circumventing Plaintiffs' and Class Members' privacy settings, allows this identification to take place."[61] Likewise, as to two of the other defendants, the complaint says that "[t]he spokesman [for Vibrant] admitted Vibrant used the

---

[59] Compl. ¶ 46.

[60] Compl. ¶ 95.

[61] Compl. ¶ 96.

trick 'for unique user identification,'"[62] and that "Media's 'id' cookie is just that—an 'ID' or 'identification' cookie."[63]

Just as the operative allegations in the complaint tend to support the inference that the cookies enabled the defendants to identify, and thus associate, information that the plaintiffs sent directly to them in the ordinary course, the operative allegations tend to negate any inference to the contrary. This is because, if the information at issue was not sent to the defendants in the ordinary course, mere identification cookies would not be sufficient for the defendants' scheme. To accomplish their tracking in that instance, the defendants would have needed not an associative device, but one capable of capturing communications sent by the plaintiffs and intended for first-party websites, and then transmitting them to the defendants.[64] There is no pleading of any such device, nor is

---

[62] Compl. ¶ 151

[63] Compl. ¶ 156

[64] *Cf. Pharmatrak*, 329 F.3d at 22 ("[Pharmatrak's code] automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak)."); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) ("The intended communication is between the users' iPhone and the Wi-fi and cell phone towers, and Plaintiffs appear to allege that Apple designed its operating system to intercept that communication and transmit the information to Apple's servers.").

that function the ordinary function of a tracking cookie. As stated above, in discussing the function of the defendants' cookies, the complaint describes them as having an associative function only.[65]

In view of our common sense reading of the operative allegations of the complaint, we note the factual position that the defendants advanced at argument: "The cookie doesn't acquire anything . . . The cookie doesn't look for anything. It just sits on the browser and gets sent along with information that would otherwise be sent."[66] The information at issue would be sent anyway because "the user's web browser send[s] a GET request to Google to display the relevant advertising information for the space on the page for which Google has agreed to sell display advertisements."[67] We note also that, at argument, the plaintiffs' counsel was directly asked on six separate occasions to clarify what transmissions they believed were improperly acquired and/or how the defendants' cookies functioned.[68] The plaintiffs' counsel did not provide a direct response on any of these occasions.

At the Rule 12(b)(6) stage "we accept the pleader's description of what happened to him or her along with any

---

[65] Compl. ¶¶ 46, 95, 96, 151, 156.

[66] Oral Arg. Tr. at 25.

[67] Compl. ¶ 86.

[68] Oral Arg. Tr. at 9-10, 11, 12, 13, 14, 15.

conclusions that can reasonably be drawn therefrom."[69] This standard permits the dismissal of a complaint "when [the] defendant's plausible alternative explanation is so convincing that plaintiff's explanation is *im* plausible."[70] Here, the operative allegations of the complaint support only the conclusion that the defendants acquired the plaintiffs' internet history information by way of GET requests that the plaintiffs sent directly to the defendants, and that the defendants deployed identifier cookies to make the information received from GET requests associable and thus trackable. And though the portion of the complaint pertaining to the Wiretap Act contains statements to the contrary, we need not give legal effect to "conclusory allegations" that are contradicted by the pleader's actual description of what happened.[71]

In short, our understanding of the plaintiffs' allegations is that the defendants acquired the plaintiffs' internet history information when, in the course of requesting webpage advertising content at the direction of the visited website, the plaintiffs' browsers sent that information directly to the defendants' servers.

---

[69] 5B Fed. Prac. & Proc. Civ. § 1357 (3d ed.) ("Motions to Dismiss—Practice Under Rule 12(b)(6)").

[70] *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011) (citing Fed. R. Civ. P. 8(a)(2); *Ashcroft v. Iqbal*, 556 U.S. 662 (2009); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007)).

[71] 5B Fed. Prac. & Proc. Civ. § 1357.

b. Application of § 2511(2)(d)

Because the defendants were the intended recipients of the transmissions at issue—i.e. GET requests that the plaintiffs' browsers sent directly to the defendants' servers—we agree that § 2511(2)(d) means the defendants have done nothing unlawful under the Wiretap Act. Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient. As the intended recipient of a communication is necessarily one of its parties, and the defendants were the intended recipients of the GET requests they acquired here, the defendants were parties to the transmissions at issue in this case. And under § 2511(2)(d), it is not unlawful for a private person "to intercept a wire, oral, or electronic communication where such person is a party to the communication."[72]

In their reply brief, the plaintiffs raise three objections in response to the argument that their Wiretap Act claim must fail because the defendants were the intended recipients of the relevant communications. None are persuasive.

First, the plaintiffs argue that we should not consider the defendants' argument because the issue was not addressed by the District Court and because the defendants failed to raise the issue in the form of a cross-appeal. This is inapposite, for even if the defendants had never raised the issue at all, whether the plaintiffs have stated a claim is a matter of law to be determined from the face of their complaint. As always, we may affirm a district court's

---

[72] 18 U.S.C. § 2511(2)(d).

judgment on grounds other than those considered by the district court itself.[73]

Second, the plaintiffs argue that the party exception should not apply for equitable reasons, in that the transmitted GET requests included cookie information that the communications included only because of the defendants' surreptitious circumvention of the cookie blockers. The point here is that, though the plaintiffs sent the GET requests to the defendants voluntarily, they were induced to do so by deceit. Though we are no doubt troubled by the various deceits alleged in the complaint, we do not agree that a deceit upon the sender affects the presumptive non-liability of parties under § 2511(2)(d). "In the context of the statute, a party to the conversation is one who takes part in the conversation."[74] There is no statutory language indicating this excludes intended recipients who procured their entrance to a conversation through a fraud in the inducement, such as, here,

---

[73] *See Jones v. Se. Pa. Transp. Auth.*, __ F.3d __, 2015 WL 4746391, at *8 (3d Cir. Aug. 12, 2015).

[74] *Caro v. Weintraub*, 618 F.3d 94, 97 (2d Cir. 2010) *United States v. Pasha*, 332 F.2d 193 (7th Cir. 1964) ("[I]mpersonation of the intended receiver is not an interception within the meaning of the statute."); *Clemons v. Waller*, 82 Fed. App'x 436, 442 (6th Cir. 2003) ("By citing *Pasha*, Congress strongly intimated that one who impersonates the intended receiver of a communication may still be a party to that communication for the purposes of the federal wiretap statute and that such conduct is not proscribed by the statute.").

by deceiving the plaintiffs' browsers into thinking the cookie-setting entity was a first-party website.

It is not unimaginable that the Wiretap Act would give legal effect to the fraudulent participation of a party to a conversation.[75] It is, after all, a *wiretapping* statute.[76] Indeed, it appears the absence of an equitable exception to § 2511(2)(d) is no accident. In *United States v. Pasha*, the Seventh Circuit held that a police officer who impersonated the intended recipient of a phone call did not violate the Wiretap Act.[77] And, as the Sixth Circuit has explained:

> When amending the federal [W]iretap [A]ct in 1968 to its current state, Congress specifically mentioned *Pasha* in its discussions of the "party to the communication" provision. In discussing § 2511(2)(c), which is in pari materia with § 2511(2)(d) and differs from that provision only in that § 2511(2)(c) applies to persons acting under color of law, the Senate Judiciary Committee stated:

---

[75] *Cf. Desnick v. Am. Broad. Companies, Inc.*, 44 F.3d 1345, 1352 (7th Cir. 1995) ("The law's willingness to give effect to consent procured by fraud is not limited to the tort of trespass.").

[76] *See* Black's Law Dictionary (10th ed. 2014) (defining "wiretapping" as "electronic or mechanical eavesdropping").

[77] 333 F.2d 193, 198 (7th Cir. 1964).

> Paragraph 2(c) provides that it shall not be unlawful for a party to any wire or oral communication . . . to intercept such communication. It largely reflects existing law. Where one of the parties consents, it is not unlawful. . . . "[P]arty" would mean the person actually participating in the communication. (*United States v. Pasha,* 332 F.2d 193 (7th Cir. 1964)).[78]

We agree with the Sixth Circuit and the Fifth Circuit that, "[b]y citing *Pasha*, Congress strongly intimated that one who impersonates the intended receiver of a communication may still be a party to that communication for the purposes of the federal wiretap statute and that such conduct is not proscribed by the statute."[79] Likewise, we conclude it was by design that there is no statutory language by which the defendants' various alleged deceits would vitiate their claims to be parties

---

[78] *Clemons v. Waller*, 82 Fed. App'x 436, 442 (6th Cir. 2003) (quoting S. Rep. No. 90-1097, at 93-94 (1968)); *see also United States v. Campagnuolo*, 592 F.2d 852, 863 (5th Cir. 1979) ("It is clear from this passage that Congress intended to reaffirm the result in *Pasha* and make admissible communications to which a police officer is a party.").

[79] *Clemons*, 82 Fed. App'x at 442; *accord Campagnuolo*, 592 F.2d at 863.

to the relevant communications. The Wiretap Act is a wiretapping statute, and just because a scenario sounds in fraud or deceit does not mean it sounds in wiretapping.[80]

---

[80] As § 2511(2)(d) contemplates that a "party" to a communication can "intercept" it, we are led to believe that the present version of the Wiretap Act gives "intercept" a broader connotation than "the ordinary meaning of 'intercept' . . . [which] is 'to stop, seize, or interrupt in progress or course before arrival.'" *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (quoting *Webster's Ninth New Collegiate Dictionary* 630 (1985)); *see also Goldman v. United States*, 316 U.S. 129, 134 (1942) ("The natural meaning of the term 'intercept' . . . indicates the taking or seizure by the way or before arrival at the destined place."), *overruled on other grounds by Katz*, 389 U.S. 347; Black's Law Dictionary (10th ed. 2014) (defining "intercept" as "to covertly receive or listen to (a communication)"). We will not, therefore, adopt the defendants' other alternative argument, which is that the plaintiffs' Wiretap Act claim should fail for want of an "interception." If the plaintiffs' claims had been brought under the Wiretap Act as it existed when *Pasha* was decided, however, the plaintiffs would likely fail to show an "interception" for the same reason that, today, they fail to show that the defendants were not parties to the relevant communications within the meaning of § 2511(2)(d). *See Pasha*, 333 F.2d at 198 ("Interception connotes a situation in which by surreptitious means a third party overhears a telephone conversation between two persons. We believe that impersonation of the intended receiver is not an interception within the meaning of the statute.").

Finally, the plaintiffs argue that § 2511(2)(d) should not apply because the defendants' acquisition of the communications at issue was tortious under California law. The basis for this argument is that § 2511(2)(d) is inapplicable when the communication at issue 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." But the plaintiffs point to no legal authority providing that the exception to § 2511(2)(d) is triggered when, as here, the tortious conduct is the alleged wiretapping itself. By contrast, all authority of which we are aware indicates that the criminal or tortious acts contemplated by § 2511(2)(d) are acts secondary to the acquisition of the communication involving tortious or criminal use of the interception's fruits.[81]

---

[81] *See Caro v. Weintraub*, 618 F.3d 94, 98, 100 (2d Cir. 2010) ("[T]he defendant must have the intent to use the illicit recording to commit a tort or crime beyond the act of recording itself. . . . Intent may not be inferred simply by demonstrating that the intentional act of recording itself constituted a tort. A simultaneous tort arising from the act of recording itself is insufficient."); *Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202-03 (9th Cir. 1999) ("Under section 2511, the focus is not upon whether the interception itself violated another law; it is upon whether the *purpose* for the interception—its intended use—was criminal or tortious. . . . Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere."); *Desnick*, 44 F.3d at 1353 ("[T]here is no suggestion that the defendants sent the testers into the Wisconsin and Illinois offices for the purpose of defaming the plaintiffs by charging tampering with the glare machine.").

As the Second Circuit explained in *Caro v. Weintraub*, "to survive a motion to dismiss, a plaintiff must plead sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording."[82] And though the plaintiffs may well plead facts that constitute violations of California laws related to intrusion upon seclusion, for purposes of the exception to § 2511(2)(d), "[i]nvasion of privacy through intrusion upon seclusion presents a problem . . . —it is a tort that occurs through the act of interception itself."[83] As the plaintiffs plead no tortious or criminal *use* of the acquired internet histories, § 2511(2)(d) is not inapplicable on the basis of the criminal-tortious purpose exception.

Based on the facts alleged in the pleadings, the defendants were parties to any communications that they acquired, such that their conduct is within the § 2511(2)(d) exception.[84] We will accordingly affirm the District Court's dismissal of the plaintiffs' Wiretap Act claim.

B. The Stored Communications Act

We next address the plaintiffs' claim for violation of the Stored Communications Act, 18 U.S.C. § 2701. Enacted in 1986, the Stored Communications Act was born from congressional recognition that neither existing federal statutes

---

[82] *Caro*, 618 F.3d at 100 (emphasis added).

[83] *Id.* at 101.

[84] *See* 18 U.S.C. § 2511(2)(d).

nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to "stored communications in remote computing operations and large data banks that stored e-mails."[85]

To state a claim under the Stored Communications Act, a plaintiff must show that the defendant "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[86]

The District Court dismissed this claim on the basis of the Act's requirement that the illicit access be with respect to "a facility through which an electronic communication service is provided."[87] As pled in the complaint, the illicit access at issue was to the plaintiffs' personal web browsers.

---

[85] *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 791 (5th Cir. 2012); *see also id.* at 793; *United States v. Councilman*, 418 F.3d 67, 80-81 (1st Cir. 2005) (en banc); S. Rep. No. 99-541, at 5 (1986); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-15 (2004).

[86] 18 U.S.C. § 2701(a); *see also id.* § 2707(a) (cause of action).

[87] *In re: Google*, 988 F. Supp. 2d at 445-47; 18 U.S.C. § 2701(a).

But according to the District Court, "an individual's personal computing device is not a 'facility through which an electronic communications service is provided.'"[88] We agree, and we find persuasive the analysis of the Fifth Circuit in *Garcia v. City of Laredo*, which held that "a home computer of an end user is not protected by the [Act]."[89]

As noted by the *Garcia* court, though the Act does not define the term "facility," the Act does define the term "electronic communication service," which it defines as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[90] This most naturally describes network service providers, and, indeed, "[c]ourts have interpreted the statute to apply to providers of a communication service such as telephone companies, [i]nternet or e-mail service providers, and bulletin board services."[91] The Act also defines "electronic storage" as "(A)

---

[88] *In re: Google*, 988 F. Supp. 2d at 446.

[89] 702 F.3d at 793 (quoting Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. at 1215).

[90] 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1)); *see also Garcia*, 702 F.3d at 792.

[91] *Garcia*, 702 F.3d at 792 (citing *Councilman*, 418 F.3d at 81-82; *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 462-63 (5th Cir. 1994)); s*ee also In re iPhone*, 844 F. Supp. 2d. at 1057 ("[T]he computer systems of an email provider, a bulletin board system, or an [internet service provider] are uncontroversial examples of facilities that

any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[92] Temporary storage incidental to transmission and storage for purposes of backup protection are not how personal computing devices keep communications, but how third party network service providers do—or at least did, in 1986.[93]

There is then the language of 18 U.S.C. § 2701(c)(1), which provides that the prohibitory language of the Act "does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communication service." This makes sense when talking about third-party access to network service providers' own facilities. But were the prohibitory language understood to apply to facilities other than those of network service providers, the language of the exception becomes problematic. As one district court has explained, "[i]t would certainly seem odd that the provider of a communication service could grant access to one's home

---

provide electronic communications services to multiple users.").

[92] 18 U.S.C. § 2510(17).

[93] *See* Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. at 1213-15 ("The [Act] . . . freez[es] into the law the understandings of computer network use as of 1986.") (citing S. Rep. No. 99-541 at 2-3).

computer to third parties, but that would be the result of [the plaintiffs'] argument."[94]

The origin of the Stored Communications Act confirms that Congress crafted the statute to specifically protect information held by centralized communication providers. "'Sen. Rep. No. 99–541 (1986)'s entire discussion of [the Stored Communications Act] deals only with facilities operated by electronic communications services such as "electronic bulletin boards" and "computer mail facilit[ies]," and the risk that communications temporarily stored in these facilities could be accessed by hackers. It makes no mention of individual users' computers . . . .'"[95]

The plaintiffs take a different view, arguing that the plain language of the terms "facility" and "electronic communication service" are sufficiently flexible to encompass contemporary personal computing devices that are used to engage with telecommunications services. After all, when the Act was enacted, Black's Law Dictionary defined "facilities" as "that which promotes the ease of any action, operations, transaction, or course of conduct."[96] And the

---

[94] *In re: iPhone*, 844 F. Supp. 2d at 1058 (quoting *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d. 1263, 1270-71 (N.D. Cal. 2001)).

[95] *Garcia*, 702 F.3d at 793 (second and third alterations in original) (quoting *In re DoubleClick Inc. Privacy Litig.,* 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (quoting S. Rep. No. 99–541, at 36).

[96] Black's Law Dictionary 705 (5th ed. 1979).

plaintiffs here use their web browsers to access network services such as email and websurfing.

In considering the plaintiffs' argument that we should give "facility" a broad, plain language meaning, we are reminded that "[a] fair reading of legislation demands a fair understanding of the legislative plan."[97] And we agree with the Fifth Circuit that the Act clearly shows a specific congressional intent to deal with the particular problem of private communications in network service providers' possession. The textual cues surrounding the term "facility," bolstered by the legislative history and enactment context of the Act, support the conclusion that "the words of the statute were carefully chosen: '[T]he statute envisions a provider (the [Internet Service Provider] or other network service provider) and a user (the individual with an account with the provider), with the user's communication in the possession of the provider.'"[98] And "[t]his is consistent with the [Act]'s purpose: home computers are already protected by the Fourth Amendment, so statutory protections are not needed."[99] In this context, "facility" is a term of art denoting where network service providers store private communications.

---

[97] *King v. Burwell*, 135 S. Ct. 2480, 2496 (2015).

[98] *Garcia*, 702 F.3d at 793 (emphases removed) (alteration in original) (quoting Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. at 1215 n.47).

[99] Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. at 1215.

Other Courts of Appeals have understood the Act in a similar manner. In *In re: Zynga Privacy Litigation*, the Ninth Circuit explained that the Act "covers access to electronic information stored in *third party* computers."[100] So, too, the Eleventh Circuit in *United States v. Steiger*, which held that "the [Stored Communications Act] clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system," but that the Act "does not appear to apply to the [government's] source's hacking into [the plaintiff's personal] computer . . . because there is no evidence that [the] computer maintained any 'electronic communication service[.]'"[101] The plaintiffs point to various district court decisions that have accepted that personal computers can be protected "facilities" under the Stored Communications Act.[102] However, as another district court observes, these decisions "provide little analysis on this point of law, instead

---

[100] 750 F.3d at 1104 (emphasis added).

[101] 318 F.3d 1039, 1049 (11th Cir. 2003). In *Steiger*, the Eleventh Circuit noted that "reading . . . the Wiretap Act to cover only real-time interception of electronic communications, together with the apparent non-applicability of the [Stored Communications] Act to hacking into personal computers to retrieve information stored therein, reveals a legislative hiatus in the current laws purporting to protect privacy in electronic communications." *Id*.

[102] *E.g.*, *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1125 (W.D. Wash. 2012) *Expert Janitorial, LLC v. Williams*, 2010 WL 908740, at *5 (E.D. Tenn. 2010); *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001).

assuming [the plaintiffs'] position to be true due to lack of argument and then ultimately ruling on other grounds."[103] The plaintiffs point to no decision of any Court of Appeals holding that a personal computing device is protected by the Stored Communications Act.

In sum, the defendants' alleged conduct implicates no protected "facility." The District Court's dismissal of the claim for violation of the Act will therefore be affirmed.

C. Computer Fraud and Abuse Act

The plaintiffs' final federal claim is for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The Act creates a cause of action for persons "who suffer[] damage or loss" because, inter alia, a third party "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[104]

The District Court dismissed this claim for failing to meet the statutory requirement of "damage or loss."[105] Under the Act, "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or

---

[103] *In re iPhone*, 844 F. Supp. 2d at 1057-58.

[104] 18 U.S.C. § 1030(a)(2)(C), (g).

[105] *In re Google*, 988 F. Supp. 2d at 448.

information."[106] Meanwhile, "the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[107]

On appeal, the plaintiffs contend that they have properly pled "loss" under the statute because they have alleged that their "impermissibly seized [p]ersonally [i]dentifiable [i]nformation is both 'currency' and a marketable 'commodity.'"[108] By capturing and making economic use of such information, the plaintiffs say, the defendants have taken the value of such information for themselves, depriving the plaintiffs of their own ability to sell their internet usage information. Insofar as the plaintiffs have a right to capture that value for themselves, the plaintiffs contend that the defendants' conduct has caused them harm.

The complaint plausibly alleges a market for internet history information such as that compiled by the defendants. Further, the defendants' alleged practices make sense only if that information, tracked and associated, had value. However, when it comes to showing "loss," the plaintiffs' argument lacks traction. They allege no facts suggesting that they ever

---

[106] 18 U.S.C. § 1030(e)(8).

[107] *Id.* § 1030(e)(11).

[108] Appellants' Br. 45.

participated or intended to participate in the market they identify, or that the defendants prevented them from capturing the full value of their internet usage information for themselves. For example, they do not allege that they sought to monetize information about their internet usage, nor that they ever stored their information with a future sale in mind. Moreover, the plaintiffs do not allege that they incurred costs, lost opportunities to sell, or lost the value of their data as a result of their data having been collected by others. To connect their allegations to the statutory "loss" requirement, the plaintiffs' briefing emphasizes that lost revenue may constitute "loss" as that term is defined in the Act.[109] This is inapposite, however, in that the plaintiffs had no revenue.

We see no "damage" or "loss" in the pleadings. We will therefore affirm the District Court's dismissal of the claim for violation of the Computer Fraud and Abuse Act.

IV. State Law Claims Against Google

We now turn to the five California state law claims brought against Google only.

A. Freestanding Privacy Claims

We first consider, in tandem, the plaintiffs' freestanding privacy claims under the California Constitution[110] and California tort law.

---

[109] *Id*. at 43-45.

[110] Article I, Section 1 of the California Constitution states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending

"A privacy violation based on the common law tort of intrusion has two elements."[111] "First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy."[112] This means "the defendant must have 'penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data' by electronic or other covert means, in violation of the law or social norms."[113] Second, "the intrusion must occur in a manner highly offensive to a reasonable person."[114]

"The right to privacy in the California Constitution sets standards similar to the common law tort of intrusion."[115] "First, [the plaintiff] must possess a legally protected privacy interest. . . . Second, the plaintiff's expectations of privacy must be reasonable. . . . Third, the plaintiff must show that the

---

life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

[111] *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1072 (Cal. 2009).

[112] *Id*.

[113] *Id*. (quoting *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 490 (Cal. 1998)).

[114] *Id.*

[115] *Id.* at 1073.

intrusion is so serious 'in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.'"[116]

When presented with parallel privacy claims under tort law and the California Constitution, the California Supreme Court has performed a dual inquiry "under the rubric of both . . . tests."[117] This "consider[s] (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests."[118] In evaluating the offensiveness of an invasion, the court is to consider "pragmatic policy concerns" such that "no cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights."[119]

In dismissing the freestanding privacy claims, the District Court concluded that Google's alleged practices "did not rise to the level of a serious invasion of privacy or an egregious breach of social norms."[120] Contending the District

---

[116] *Id.* (quoting *Hill v. Nat'l Collegiate Athletic Assn.*, 865 P.2d 633, 655 (Cal. 1994)).

[117] *Id*. at 1073-74.

[118] *Id*. at 1074.

[119] *Id.* at 1079; *Hill*, 865 P.2d at 675 ("Whether [a] plaintiff has a reasonable expectation of privacy in the circumstances and whether [a] defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact.").

[120] *In re Google*, 988 F. Supp. 2d at 449.

Court got it right, Google says the plaintiffs voluntarily sent Google all the internet usage information at issue.[121] Moreover, Google argues, tracking cookies are routine.[122] Pointing to cases describing cookies as, more or less, innocuous,[123] Google offers that courts "routinely" find no actionable privacy invasion in cases involving tracking, collation, and disclosure of internet usage information.[124] Google gives particular attention to *Low v. LinkedIn*, where the Northern District of California explained that "[e]ven disclosure of personal information, including social security numbers, does not constitute an 'egregious breach of the social norms' to establish an invasion of privacy claim."[125]

For purposes of California privacy law, Google's emphasis on tracking and disclosure amounts to a smokescreen. What is notable about this case is *how* Google accomplished its tracking. Allegedly, this was by overriding the plaintiffs' cookie blockers, while concurrently announcing in its Privacy Policy that internet users could

---

[121] Google Br. at 59 (emphasis in original).

[122] *Id*.

[123] *Id.* at 61 (citing, *e.g.*, *Pharmatrak*, 329 F.3d at 14 ("Cookies are widely used on the internet by reputable websites to promote convenience and customization.")).

[124] *Id.* at 62 (citing *Stern v. Weinstein*, 512 Fed. App'x 701, 702 (9th Cir. 2013)).

[125] *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).

"reset your browser to refuse all cookies."[126] Google further assured Safari users specifically that their cookie blockers meant that using Google's in-house prophylactic would be extraneous. Characterized by deceit and disregard, the alleged conduct raises different issues than tracking or disclosure alone.[127]

Directly pertinent to whether Google's alleged practices implicated a protected privacy interest, California tort law treats as actionable an "unwanted access to data by electronic or other covert means, in violation of the law or social norms."[128] Moreover, the California Constitution protects an interest in "conducting personal activities without observation," with the reasonableness of any given expectation "rest[ing] on an examination of customs . . . as well as the opportunity to be notified in advance and consent to the intrusion."[129] To Google's point, a sophisticated

---

[126] Compl. ¶ 80.

[127] *See* Kristen Lovin, *SafariGate: Benign Behavior or Malignant Breach?*, Colum. Sci. & Tech. L. Rev. (Feb. 22, 2012), http://stlr.org/2012/02/22/safarigate-benign-behavior-or-malignant-breach/ ("[O]ne could say that Google ignored the express desires of its users, elevating its own commercial interests over the user's personal privacy interests. This kind of disregard may be particularly troubling given the relative bargaining power that an individual consumer has against a monolith like Google.").

[128] *Hernandez*, 211 P.3d at 1072 (internal quotation marks omitted).

[129] *Id*. at 1073 (internal quotation marks omitted).

internet user may well have known that, in browsing the internet, her URL information was sent to Google. But such a user would also reasonably expect that her activated cookie blocker meant her URL queries would not be associated with each other due to cookies.[130] As the activated cookie blocker equates, in our view, to an express, clearly communicated denial of consent for installation of cookies, we find Google "intru[ded] upon reasonable expectations of privacy."[131]

As for whether the alleged conduct is "so serious in nature[] [and] scope . . . as to constitute an egregious breach of the social norms,"[132] Google not only contravened the cookie blockers—it held itself out as respecting the cookie blockers. Whether or not data-based targeting is the internet's pole star, users are entitled to deny consent, and they are entitled to rely on the public promises of the companies they deal with. Furthermore, Google's alleged conduct was broad, touching untold millions of internet users; it was surreptitious, surfacing only because of the independent

---

[130] It is no matter whether or not a given plaintiff had actual, subjective knowledge of her browser settings and the impact of those settings on the defendants' tracking practices. Like a principal's agent, a personal computing device acts as an extension of oneself for purposes of engaging with the internet. The decision to use one or another technology is the decision to choose its features, even if the lay user may not actually know what all those features are in their specifics.

[131] *Hernandez*, 211 P.3d at 1074.

[132] *Id.* at 1073 (internal quotation marks omitted).

research of Mayer and the Wall Street Journal; and it was of indefinite duration, with Google's counsel conceding at argument that their tracking cookies have no natural lifespan. Particularly as concerns Google's public statements regarding the Safari cookie blocker, we see no justification. Neither, apparently, do the elected branches, as California and federal executive agencies have themselves sought to penalize Google for the events alleged in the complaint.[133] Based on the pled facts, a reasonable factfinder could indeed deem Google's conduct "highly offensive" or "an egregious breach of social norms."[134]

A reasonable jury could conclude that Google's alleged practices constitute the serious invasion of privacy contemplated by California law. We will vacate the dismissal of the plaintiffs' claims under the California Constitution and California tort law.

B. California Invasion of Privacy Act

We next consider the plaintiffs' claim against Google for violation of the California Invasion of Privacy Act, Cal. Penal Code § 631(a). Like the federal Wiretap Act, § 631(a) "broadly prohibits the interception of wire communications and disclosure of the contents of such intercepted communications."[135] The California Supreme Court has

---

[133] Compl. ¶¶ 166-68; *infra* n. 12.

[134] *Id.* (internal quotation marks omitted).

[135] *Tavernetti v. Superior Court*, 583 P.2d 737, 739 (Cal. 1978).

explained that "Section 631 was aimed at one aspect of the privacy problem—eavesdropping, or the secret monitoring of conversations by third parties."[136]

The District Court dismissed the § 631(a) claim for the same reasons that it dismissed the plaintiffs' federal wiretapping claim. As discussed above, the pleadings demonstrate that Google was itself a party to all the electronic transmissions that are the bases of the plaintiffs' wiretapping claims.[137] Because § 631 is aimed only at "eavesdropping, or the secret monitoring of conversations by third parties,"[138] we will affirm the dismissal of the California Invasion of Privacy Act claim for the same reasons we affirm the dismissal of the federal Wiretap Act claim.

---

[136] *Ribas v. Clark*, 696 P.2d 637, 640 (Cal. 1985); *see also Powell v. Union Pac. R. Co.*, 864 F. Supp. 2d 949, 955 (E.D. Cal. 2012) ("Section 631 broadly proscribes third party access to ongoing communications."); *Thomasson v. GC Servs. Ltd. P'ship,* 321 Fed. App'x 557, 559 (9th Cir. 2008) ("California courts interpret 'eavesdrop,' as used in § 632, to refer to a third party secretly listening to a conversation between two other parties.").

[137] Judge Fisher believes that under *Ribas*, 696 P.2d 637, Google may be liable under Section 631(a) for recording the communications and sharing them with third parties. Judge Fisher does not write separately as it does not appear that California law is developed sufficiently on this question to reverse the judgment of the District Court.

[138] *Ribas*, 696 P.2d at 640.

C. Remaining State Law Claims

We will affirm the District Court's dismissals of the remaining state law claims against Google.

The District Court dismissed the plaintiffs' claim under the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, on the basis that, under the statute, "private standing is limited to any 'person who . . . has lost money or property' as a result of unfair competition."[139] Likewise, the District Court dismissed the plaintiffs' claim under the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, on the basis of § 502's requirement that a suit may only be brought by one who has "suffer[ed] damage or loss by reason of a violation."[140] As discussed above in connection with the Computer Fraud and Abuse Act, the complaint fails to show damage or actual loss. Accordingly, the dismissal of these claims was proper.

The California Consumers Legal Remedies Act, Cal. Civ. Code § 1770, proscribes various "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer."[141] On appeal, the plaintiffs argue that they

---

[139] *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 884 (Cal. 2011) (quoting § 17204).

[140] Cal. Penal Code § 502(e).

[141] Cal. Civ. Code § 1770(a).

plead a forced "sale" whereby they gave their trackable internet history information in exchange for advertisements delivered to their browsers (i.e., the "services"). The plaintiffs present no caselaw in support of their expansive construction of "sale." And California federal courts have expressly rejected defining "sale" as to include "transactions" based on non-tangible forms of payment, including internet usage information specifically.[142] Likewise, Black's Law Dictionary defines a sale as a "transfer or property or title for a price," requiring specifically "a price in money paid or promised."[143] We follow the view of the California federal courts, and see no "sale . . . of services" in the allegations of the complaint. The dismissal of this claim was thus proper, too.

V. Conclusion

In light of the foregoing, we will dispose of the plaintiffs' claims in the following manner.

We will affirm the dismissal of the three federal law claims brought against all defendants. Because the defendants were parties to all electronic transmissions at issue in this

---

[142] *See Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 864 (N.D. Cal. 2011) (rejecting plaintiff's contention that "his transfer of . . . information to defendant in exchange for free applications[] constitutes a 'purchase' or 'lease'" as finding "no support under the specific statutory language of the [Act]"); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *12 (N.D. Cal. 2013) (same).

[143] Black's Law Dictionary (10th ed. 2014) ("Sale").

case, and plaintiffs state no Wiretap Act violation per 18 U.S.C. § 2511(2)(d). The alleged intrusion upon the plaintiffs' personal computing devices does not implicate a "facility" protected by the Stored Communications Act. And the plaintiffs plead no cognizable losses as required by the Computer Fraud and Abuse Act.

We will vacate the District Court's dismissal of the plaintiffs' freestanding privacy claims against Google under the California Constitution and California tort law. A reasonable factfinder could conclude that the means by which defendants allegedly accomplished their tracking, i.e., by way of a deceitful override of the plaintiffs' cookie blockers, marks the serious invasion of privacy contemplated by California law. But we will affirm the dismissal of the remainder of the plaintiffs' state law claims. The plaintiffs fail to plead a violation of the California Invasion of Privacy Act for the same reason that they fail to plead a violation of the federal Wiretap Act. Likewise, because they do not show loss, the plaintiffs fail to show violations of the California Unfair Competition Law or the California Comprehensive Computer Data Access and Fraud Act. Finally, the plaintiffs do not plead a "sale" as required by the California Consumers Legal Remedies Act.