

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

VISHAL SHAH, et al.,
Plaintiffs,
v.
FANDOM, INC.,
Fandom.

Case No. 24-cv-01062-RFL

**ORDER DENYING MOTION TO
DISMISS**

Re: Dkt. No. 20

Plaintiffs Vishal Shah and Jayden Kim have brought this class action lawsuit against Fandom alleging that its website gamespot.com caused their browsers to download third-party tracking software (“Trackers”). Plaintiffs allege that these Trackers are unauthorized pen registers under Section 638.51(a) of the California Invasion of Privacy Act (“CIPA”), and that they record and send users’ IP addresses to third parties without their consent. Fandom moves to dismiss Plaintiffs’ First Amended Complaint. Fandom argues, among other things, that websites across the Internet commonly require users’ computers to send their IP addresses to third parties as part of the process of loading those sites. At this stage of the litigation, the Court is required to accept the allegations of the operative complaint as true. Plaintiffs have plausibly alleged that they did not expect their IP addresses to be disseminated to the companies operating the Trackers, and did not impliedly or expressly agree to such dissemination by visiting gamespot.com. For the reasons explained further below, the motion to dismiss is **DENIED**. (Dkt. No. 20.)

I. ALLEGATIONS OF THE FIRST AMENDED COMPLAINT

Fandom owns and operates a video gaming website called gamespot.com. According to Plaintiffs, when a user visits that website, their browser sends an HTTP request to Fandom’s

server. In response, Fandom’s server sends an HTTP response back to the user’s browser with instructions. These instructions tell the browser how to display the website. The HTTP response also instructs the Trackers to be installed on the user’s browser. The Trackers are owned by third parties GumGum, Audiencerate, and TripleLift.

Once the Trackers are installed on the user’s browser, they instruct the user’s browser to send the user’s IP address to the third party. The Trackers also store a cookie in the user’s browser cache. As long as the user has not cleared their browser cache, the Trackers will locate the cookie stored in the cache every time the user visits Fandom’s website in the future. As a result, after the Trackers locate the cookie, they “cause[] the browser to send the cookie along with the user’s IP address” to the third party. (Dkt. No. 15 (“First Amended Complaint,” or “FAC”) at ¶¶ 37, 47, 56.) This process repeats itself every time the user visits Fandom’s website until the user clears their browser cache.

Plaintiffs allege that this amounts to a violation of the pen register statute because the IP addressing information is sent to the third parties without their consent. The third parties use their Trackers to “receive, store, and analyze information collected from website visitors, such as visitors of Defendant’s website.” (*Id.* ¶¶ 35, 45, 54.) By collecting a user’s IP address, advertisers can target customers based on their “neighborhood” and “postal code,” including whether they are on a college campus or in the vicinity of an upcoming event. (*Id.* ¶¶ 28-29.) In addition, because an IP address is “associated with a specific internet-connected device,” it provides “a level of specificity previously unfound in marketing.” (*Id.* ¶ 27.) Plaintiffs allege that “companies can use an IP address . . . to personally identify individuals,” as well as specific households and businesses. (*Id.* ¶¶ 27-28, 31.) The operators of the Trackers allegedly use the IP addresses collected “to serve targeted advertisements and conduct website analytics.” (*Id.* ¶ 69.)

II. LEGAL STANDARD

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). A

complaint that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court’s decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corporation v. Twombly*, 550 U.S. 544 (2007), a plaintiff’s “factual allegations [in the complaint] ‘must . . . suggest that the claim has at least a plausible chance of success.’” *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014).

The court “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But “allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively.” *Levitt*, 765 F.3d at 1135 (quoting *Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014)). “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.” *Iqbal*, 556 U.S. at 678. “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (quoting *Twombly*, 550 U.S. at 556).

III. DISCUSSION

Section 638.51(a) of the California Invasion of Privacy Act prohibits any person from “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order.” The statute defines a “pen register” as “a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.” Cal. Penal Code § 638.50(b). Plaintiffs adequately plead each element of this definition. Plaintiffs’ theory is that the third-party Trackers operate as pen registers under the meaning of the statute because they are processes that record users’ IP addressing information, but not the content of the electronic communications being transmitted from users’ computers or

smartphones to Fandom’s website.

At the motion to dismiss stage, these allegations are sufficient to plausibly allege that the Trackers operate as a “process” under the meaning of the statute. As the Court noted in *Greenley v. Kochava, Inc.*, “[t]he [pen register] definition is specific as to the type of data a pen register collects—‘dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,’ but it is vague and inclusive as to the form of the collection tool—‘a device or process.’ This indicates courts should focus less on the form of the data collector and more on the result.” 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (quoting Cal. Penal Code § 538.50(b)). As Plaintiffs allege, the Trackers are “at least a ‘process’ because it is ‘software that identifies consumers, gathers data, and correlates that data.’” (FAC ¶¶ 39, 49, 59 (quoting *Greenley*, 684 F. Supp. 3d at 1050)).

Plaintiffs also sufficiently allege that the Trackers record addressing information, but not the content of the outgoing communication transmitted from the user’s computer or smartphone to Fandom’s website. For purposes of the statute, the “instrument or facility” from which the electronic communication is allegedly transmitted is the user’s “computer[] or smartphone[.]” (*See id.* ¶ 117.) The “electronic communication” that the user’s computer or smartphone transmits is the HTTP request to load Fandom’s website, sent from the user’s browser to Fandom’s website. As Plaintiffs allege, the HTTP request—the electronic communication sent to Fandom’s website—transmits the IP addressing information along with the request to load the website. The Trackers do not record the rest of the HTTP request (*i.e.*, the request to load Fandom’s website), but only the addressing information (*i.e.*, the user’s IP address). (*Id.* ¶ 119.)

Construing the pleadings in the light most favorable to Plaintiff, the IP addresses collected by the Trackers fall within the statutory definition of “addressing” information. *In re Zynga Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014) (“IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of the communication” (internal citation omitted)). Fandom argues that the IP addresses are the “contents” of the communication, since the IP addresses are transmitted “through” or “within”

the cookie to the third party. (Dkt. No. 20 at 20.)¹ But, as pled by Plaintiffs, the “electronic communication” at issue is the transmission of the HTTP request from the user’s computer or smartphone to Fandom’s website. The Trackers are not alleged to collect the contents of that HTTP request, only the user’s IP address. Whether the Trackers later send the user’s IP address to the third party inside a cookie, or through some other transmission method, is immaterial. The analogy to a traditional pen register is instructive. A traditional phone pen register collects information about a phone call from Party A to Party B—such as the phone number called and length of the call—but does not collect the contents of what was said (which would be a wiretap). The traditional pen register will then transmit the phone number and length of call to the law enforcement officer. The phone number and length of call may be the “contents” of what is sent to the law enforcement officer, but that does not take the pen register outside Section 638.50(b), because the relevant “contents” of the “electronic communication” at issue is what was said on the phone call. Likewise, here, the “contents” referenced by Section 638.50(b) are the users’ HTTP requests to load Fandom’s website, not the Tracker’s transmission of the users’ IP addresses to the third party.

Fandom also argues that the claim fails because the Trackers do not collect any “*recipient* ‘dialing, routing, addressing or signaling information’ relating to an outgoing communication,” but instead collect the *sender’s* IP address. (*Id.* at 16.) According to Fandom, because the Trackers do not operate like traditional phone pen registers—which collect the recipient phone number dialed during the outgoing call—they do not meet the definition of pen registers under CIPA. But the Court’s analysis must begin with the statutory text, and if that text is clear, must end there. *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 951 (9th Cir. 2009) (quoting *McDonald v. Sun Oil Co.*, 548 F.3d 774, 780 (9th Cir. 2008)). Nothing in the statutory definition limits pen registers to those that operate the same way as a traditional phone pen register. “[T]he Court cannot ignore the expansive language in the California Legislature’s chosen definition.”

¹ Citations to page numbers refer to the ECF pagination.

Greenley, 684 F. Supp. 3d at 1050. By the plain meaning of § 638.50(b), collection of the recipient phone number or IP address is not a required element. All that is required is that the Trackers record addressing information transmitted by the user’s computer or smartphone in connection with the outgoing HTTP request to Fandom’s website, regardless of whether that addressing information pertains to the sender or the recipient of the communication at issue. Plaintiffs have so alleged. (*See* FAC ¶¶ 41, 51, 61 (alleging that the Trackers “capture[] the outgoing information—the IP address—from visitors to websites”); FAC ¶ 25 (alleging that “the IP address enables a device to communicate with another device—such as a computer’s browser communicating with a server”).)

Nor is it persuasive that the type of pen registers typically used by law enforcement require the originating telephone number or IP address to be identified and often collect recipient information. The statutory definition of a pen register is likewise not limited to the type most often utilized by law enforcement. Although Fandom points to § 638.52, that section does not alter the definition of a pen register. Instead, that section lists the procedures that law enforcement officers must follow when applying for a pen register. Under § 638.52(d), for a court to authorize the installation of a pen register on a telephone, the “number . . . of the telephone line to which the pen register . . . is to be attached” must be included. Fandom contends that, even assuming this provision applies to IP addresses, it would be “nonsensical to apply for authorization to install the [Tracker] as a pen register” because in order to apply for the pen register, one would have to provide the very information the Trackers collect. (Dkt. No. 20 at 17.) Section 638.52, however, merely lists requirements relating to a particular type of pen register: one that is installed on a telephone line. For that type of pen register, the Legislature understandably required law enforcement officers seeking court approval to disclose the phone number to which the pen register would be attached. But that does not alter the statutory definition of a pen register stated in § 638.50(b) or the prohibition on non-law enforcement use of such pen registers.

Giving effect to CIPA’s broad statutory language is consistent with the California

Legislature’s stated intent to protect privacy interests, as well as the California courts’ approach when applying statutes to new technologies. CIPA’s preamble states that “[t]he Legislature by this chapter intends to protect the right of privacy of the people of this state.” Cal. Penal Code § 630. “In light of this intent, the California Supreme Court has instructed courts to interpret CIPA in the manner that ‘fulfills the legislative purpose of CIPA by giving greater protection to privacy interests.’” *Matera v. Google Inc.*, No. 15-cv-04062, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016) (quoting *Flanagan v. Flanagan*, 41 P.3d 575, 581 (Cal. 2002)).² Moreover, California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted. “The California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme.” *In re Google Inc.*, No. 13-MD-02430, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013). As such, courts have repeatedly held that other provisions of CIPA are not limited to the traditional versions of the tools at issue, based on “the plain language of the statute,” “the California Supreme Court’s pronouncements regarding the broad legislative intent underlying CIPA to protect privacy,” and “the California courts’ approach to updating obsolete statutes in light of emerging technologies.” *Id.* (applying Section 631 of CIPA to emails); *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet communications.”). The same reasoning applies here.

Fandom also contends that “the Accused Code does not fall under CIPA because it does not involve telephone surveillance and tracking.” (Dkt. No. 20 at 7.) But CIPA was passed in part because “the development of new devices and techniques for the purpose of eavesdropping

² Fandom cites a recent ruling from the Superior Court of California for Los Angeles County, *Palacios v. Fandom, Inc.*, No. 24STCV11264, which relied upon legislative materials from the June 2015 Senate Amendments to CIPA. (Dkt. No. 31.) Those materials, however, merely describe traditional telephone-based pen registers as being among the “variety of electronic tools” used by law enforcement “to apprehend criminals in this age of rapidly changing technology.” (Dkt. No. 20-14 at 3.) Nowhere in those materials did the Legislature state an intent to add a statutory requirement limiting pen registers to those traditional forms.

upon private communications . . . has created a serious threat to the free exercise of personal liberties.” Cal. Penal Code § 630. As such, CIPA’s pen register definition expressly includes recording of information about “electronic communications.” Cal. Penal Code § 638.50(b). In turn, § 629.51(a)(2) defines “[e]lectronic communication” as “any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.” The HTTP request transmitted from users’ computers or smartphones constitutes an electronic communication, and the Trackers record the addressing information associated with this communication. Based on the expansive statutory definition of a pen register, “tracking software could plausibly constitute a pen register under §§ 638.50 and 638.51.” *Moody v. C2 Educ. Sys. Inc.*, 2:24-cv-04249, 2024 WL 3561367, at *2 (C.D. Cal. July 25, 2024) (discussing *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023)).

Plaintiffs also sufficiently allege that Fandom installed the Trackers on their browsers. Fandoms argue that the third parties, not Fandom, were responsible for maintaining and installing the Trackers. But the Court is required to take Plaintiffs’ allegations as true on a motion to dismiss, and Plaintiffs sufficiently allege that Fandom was responsible for the installation of the trackers. According to Plaintiffs, “when companies build their websites, they install or integrate various third-party scripts into the code of the website.” (FAC ¶ 63.) And in this case, Fandom “incorporated the code of the Trackers into the code of its website.” (*Id.* ¶ 66.) Thus, “when a user visits the website, the website’s code—as programmed by [Fandom]—installs the Trackers onto the user’s browser.” (*Id.* ¶ 67.) Even if third parties “developed and used the [Tracker] software,” it is alleged that Fandom was responsible for integrating the third-party script into its own website. (Dkt. No. 20 at 7.) Based on this, Plaintiffs’ allegation that Fandom installed the Trackers is sufficient to state a claim.

Finally, Fandom protests that the Trackers cannot be pen registers because the user “necessarily and voluntarily discloses” its IP address to Fandom by visiting its website. (*Id.* at 10-11.) Fandom initially framed this as a “consent” argument. (*Id.* at 11 (referring to cases

interpreting Section 631.51(b)'s provision that a pen register is permitted "[i]f consent of the user of that service has been obtained".) Fandom, however, bears the burden to establish consent and, on a motion to dismiss, would be required to show that the allegations of the complaint established consent as a matter of law. *See In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020). And consent is "generally limited to the specific conduct authorized." *Javier*, 2021 WL 940319, at *2. A user who consents to disclose their IP address to Fandom as part of accessing its website does not necessarily consent to disclose their IP address to the third parties operating the Trackers. The question would be "whether the user agreed to the specific use or collection." *Id.* (internal quotations and citation omitted). The First Amended Complaint repeatedly alleges that Plaintiffs did not consent to disclosing their IP addresses to the Trackers. (*See, e.g.*, FAC ¶ 70.) At oral argument, Fandom conceded the issue of consent and denied that it was attempting to advance a consent argument, in light of the allegations of the operative complaint.

Instead, Fandom reframed its position at oral argument as a challenge to Plaintiffs' statutory standing under § 637.2 to assert their claim under § 638.51(a). Section 637.2 confers a private right of action on "[a]ny person who has been injured by a violation of this chapter." Cal. Pen. Code § 637.2(a); *see also Moody*, 2024 WL 3561367, at *4 ("California Penal Code § 637.2 states that an individual injured by a violation of CIPA may bring a private action to enforce it."). At oral argument, Fandom contended for the first time that Plaintiffs had not established an injury under Section 637.2 because Plaintiffs had no privacy interest in their IP addresses. This argument was waived, as it was not raised in the briefs.

In any event, Plaintiffs sufficiently allege statutory standing. Plaintiffs plausibly allege that the collection of their IP addresses through the Trackers allows the third parties to obtain "personally identifying, non-anonymized information," and that the IP addresses reveal geographical location and other personal information sufficient for third parties to conduct targeted advertising. (FAC ¶¶ 71-72.) Plaintiffs further allege that they were unaware of this tracking, and did not consent to it, as noted above. Perhaps Plaintiffs should expect to reveal

their IP addresses to the gamespot.com website, and possibly even to third parties who provide the advertisements that load when Plaintiffs visit that website.³ But that does not necessarily mean that Plaintiffs should reasonably expect to have Trackers installed that send their IP addresses to third parties every time Plaintiffs visit gamespot.com. Plaintiffs have plausibly alleged that they were injured by being tracked across multiple visits for marketing and advertising purposes, and that they did not expect or agree to such tracking.

The Court recognizes Fandom’s concern that allowing this lawsuit to proceed could unsettle the basic operating rules of the Internet. It may be, as Fandom contends, that users routinely disclose their IP addresses to third parties in the process of accessing a website, and that websites sometimes do not obtain users’ consent for those practices through a Privacy Policy or Terms of Use. The Court’s task is to interpret the law as the Legislature wrote it. The pen register statute is broadly written, and under California law, is to be interpreted broadly to protect privacy and to be applied to new techniques and technologies. That statute reflects the Legislature’s judgment that an individual’s consent is required before others may track certain addressing information in their electronic communications for non-law enforcement purposes. To the extent that Fandom believes the statute may impose too many burdens when applied to the realities of modern technologies, and that it is too unwieldy to obtain users’ consent through disclosures of the practices at issue, the question of whether the statute’s scope should be narrowed ultimately rests with the Legislature, not the courts. Plaintiffs have plausibly alleged

³ The cases on which Plaintiffs rely involve situations where users were directly communicating with the party alleged to be operating the pen register and voluntarily sent that party their IP address. *See Capitol Recs. Inc. v. Thomas-Rasset*, No. CIV 06-1497(MJD/RLE), 2009 WL 1664468, at *3 (D. Minn. June 11, 2009) (holding that “the Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them”); *Malibu Media, LLC v. Pontello*, No. 13-12197, 2013 WL 12180709, at *4 (E.D. Mich. Nov. 19, 2013) (where Malibu Media allegedly operated a “honey pot” to encourage Pontello to send pirated materials via BitTorrent, and then identified Pontello using his IP address, the federal pen register statute did not apply because “Pontello consensually engaged in the transaction with [Malibu Media’s agent], and communicated his IP address as part of the packet his computer sent to [that agent]”).

that the Trackers operate as pen registers under the meaning of the statute, and that they were injured by being tracked in a way that they did not expect and to which they did not agree. That is sufficient at the pleadings stage.

IV. CONCLUSION

Based on the foregoing analysis, Fandom's motion to dismiss (Dkt. No. 20) is **DENIED**.

IT IS SO ORDERED.

Dated: October 21, 2024


RITA F. LIN
United States District Judge