

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States District Court
Northern District of California

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE META PIXEL TAX FILING CASES

Case No. 22-cv-07557-PCP

**ORDER DENYING MOTION TO
DISMISS**

Re: Dkt. No. 183

In this consolidated putative class action against defendant Meta Platforms, Inc., plaintiffs filed an amended complaint that included a new claim alleging that the Meta Pixel operates as a pen register prohibited by the California Invasion of Privacy Act (CIPA). This Court previously held that plaintiffs had plausibly stated a claim that the Pixel is an unlawful wiretap under CIPA. Meta now moves to dismiss plaintiffs’ new claim, arguing that plaintiffs have failed to state a pen register claim both because Meta does not “use” or “install” the Meta Pixel and because the Pixel cannot be both a wiretap and a pen register. For the reasons stated herein, Meta’s motion is denied.

BACKGROUND

Meta operates the social network Facebook.¹ It makes money by selling ads. Part of Meta’s value proposition is its ability to target users: Meta catalogs users’ names, birthdays, genders, locations, contact information, and communications, as well as technical identifiers like IP addresses and device IDs. Meta assembles the information it collects about individual users and draws inferences to uncover attributes like “interests,” “behavior,” and “connections.” Meta then offers advertisers the ability to target ads based on this data.

¹ For the purposes of Meta’s Rule 12(b)(6) motion, the Court assumes the truth of the allegations in plaintiffs’ second amended consolidated class complaint.

1 Meta has developed a tool called the Meta Pixel that third-party web developers can install
2 on their sites. On the back end, the Pixel is a snippet of JavaScript code that loads a library of
3 functions which developers can use to track actions users take on their sites. The Pixel logs these
4 user actions and sends them to Meta, where developers can use and analyze the data, such as by
5 measuring how effective their ads are or defining custom audiences for ad targeting. Every time
6 the Pixel logs an action on a third-party website, the Pixel sends the data to Meta. Meta then
7 attempts to match the action to one of its own users. If a user is logged into Facebook when
8 visiting a third-party site, web cookies allow Meta to link the data transmitted by the Pixel directly
9 to that specific user's Facebook account. If the Pixel data includes personal information like a
10 name or email, Meta can also use that to perform a match. In addition to the utility offered to
11 third-party developers, the Pixel benefits Meta, which amasses the data collected by the Pixel into
12 detailed "dossiers" that it keeps for registered Facebook users and non-users alike. This data, in
13 turn, is used to target ads based on individuals' interests and activity, including their activity on
14 non-Meta products. Meta offers other tools to developers that work similarly, including the
15 Facebook SDK (which allows advertisers to track user actions on mobile apps) and the
16 Conversion API (which allows developers to track actions taken by users who have opted out of
17 tracking).

18 H&R Block, TaxAct, and TaxSlayer are widely used services for filing taxes online. These
19 services installed the Pixel and other Meta tracking tools on their websites. As a result, the
20 tracking tools transmitted financial information about the tax sites' users to Meta, including
21 names, email addresses, and data about income, filing status, refund amounts, and dependents'
22 college scholarship amounts. In particular, plaintiffs allege that TaxAct sent its users' filing status,
23 adjusted gross income, and refund amount to Meta; that H&R Block transmitted data about health
24 savings accounts and college tuition grants and expenses; and that TaxSlayer transmitted phone
25 numbers and names, including of dependents. Plaintiffs allege that Meta's tracking tools link
26 specific users to the tax-related information sent by TaxAct, H&R Block, and TaxSlayer. The
27 Pixel also transmit webpage URL data from the tax filing websites to Meta. This data discloses
28 specific issues about which the users of the websites have inquired. For example, one user

1 inquired with H&R block whether they could “claim[] a boyfriend on taxes,” and the Pixel then
2 transmitted to Meta that a given user had visited the following URL:
3 <https://www.hrblock.com/tax-center/filing/dependents/claiming-boyfriend-on-taxes/>. The Pixel
4 transmitted thousands of similar URLs to Meta, revealing the putative class members’ inquiries
5 about matters such as COVID-19, lotteries, and obtaining loans.

6 As relevant here, the plaintiffs in this case allege that the Pixel sent this data to Meta from
7 the TaxAct, H&R Block, and TaxSlayer websites. They contend that this violates the provision of
8 CIPA that prohibits installing a wiretap without the consent of all parties to a communication. *See*
9 Cal. Penal Code § 631. On May 9, 2025 plaintiffs filed a second amended consolidated class
10 complaint which further asserts that the Pixel violates the provision of CIPA that prohibits
11 installing a pen register without a court order. *See id.* § 638.51. Plaintiffs contend that the Pixel is
12 a pen register because it “is a device or process that records or decodes dialing, routing,
13 addressing, or signaling information from the electronic communications transmitted to or from
14 subject tax filing websites.” Meta now moves to dismiss plaintiffs’ pen register claim under Rule
15 12(b)(6).

16 LEGAL STANDARDS

17 Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include a “short and plain
18 statement of the claim showing that the pleader is entitled to relief.” Under Federal Rule of Civil
19 Procedure 12(b)(6), a defendant may move to dismiss a complaint for failure to state a claim upon
20 which relief can be granted. Dismissal is required if the plaintiff fails to allege facts allowing the
21 Court to “draw the reasonable inference that the defendant is liable for the misconduct alleged.”
22 *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “Dismissal under Rule 12(b)(6) is appropriate only
23 where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable
24 legal theory.” *Mendondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). To
25 survive a Rule 12(b)(6) motion, a plaintiff need only plead “enough facts to state a claim to relief
26 that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

27 In considering a Rule 12(b)(6) motion, the Court must “accept all factual allegations in the
28 complaint as true and construe the pleadings in the light most favorable” to the non-moving party.

1 *Rowe v. Educ. Credit Mgmt. Corp.*, 559 F.3d 1028, 1029–30 (9th Cir. 2009). While legal
 2 conclusions “can provide the [complaint’s] framework,” the Court will not assume they are correct
 3 unless adequately “supported by factual allegations.” *Iqbal*, 556 U.S. at 679. Courts do not “accept
 4 as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable
 5 inferences.” *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quoting *Spewell*
 6 *v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)).

7 ANALYSIS

8 Pursuant to Section 638.51(a) of the California Penal Code, “a person may not install or
 9 use a pen register ... without first obtaining a court order[.]” A pen register is a “device or process
 10 that records or decodes dialing, routing, addressing, or signaling information transmitted by an
 11 instrument or facility from which a wire or electronic communication is transmitted, but not the
 12 contents of a communication.” Cal. Penal Code. § 638.50(b). Meta makes two arguments in
 13 support of its motion to dismiss. First, Meta argues that the complaint fails to allege facts showing
 14 that Meta either “install[ed] or use[d]” the Pixel. Second, Meta argues that because the complaint
 15 alleges that the Pixel discloses the “contents of communications” between users and the tax
 16 websites, the plaintiffs have effectively pleaded themselves out of their pen register claim.

17 **I. The complaint makes plausible allegations that Meta “used” a pen register.**

18 Meta argues that the complaint fails to plausibly allege that Meta either installed or used
 19 the Pixel, which is necessary to state a claim under Section 638.51. Because the complaint
 20 adequately alleges that Meta used the Pixel, the Court need not address whether the complaint
 21 sufficiently alleges that Meta installed the Pixel.

22 The central thrust of Meta’s argument is that CIPA imposes liability for *using* a pen
 23 register but not for *using data received from* a pen register. In Meta’s view, it is the tax websites
 24 who both install and use the Pixel while Meta, by contrast, merely uses the data that it receives
 25 from the Pixel without using the Pixel itself. In support of its argument, Meta points to textual
 26 differences between CIPA’s pen register and wiretap provisions. Whereas CIPA imposes liability
 27 on any person who unlawfully “uses, or attempts to use,” information obtained from a wiretap,
 28 CIPA’s pen register provisions include no such prohibition. Cal. Penal Code § 631(a). Meta notes

1 a similar distinction in the analogous federal statutes. *Compare* 18 U.S.C. § 2511(b) (imposing
2 liability on individuals who “use ... the contents” of illegally obtained communications), *with* 18
3 U.S.C. § 3121(a) (imposing liability only on individuals who “install or use a pen register”).

4 The problem with Meta’s argument is that the complaint clearly asserts that Meta uses the
5 Pixel. Plaintiffs generally allege that Meta provides the Pixel to the tax services who then install
6 the Pixel on their websites. The Pixel tracks user activity on those websites and, as it tracks that
7 activity, it “transmit[s information] in real time to Meta’s servers in California, where the
8 information is stored.” SAC ¶30. Indeed, the complaint is replete with allegations that Meta uses
9 the Pixel to intercept data sent between the user and the tax websites and transmit that data back to
10 its own servers. It is only after Meta has received that information from the Pixel that it can use
11 that data to provide third-party websites with Meta’s analytics services. Whether or not Meta’s
12 mere use of the data generated from the Pixel violates Section 638.51, the complaint adequately
13 alleges that Meta is using the Pixel to record and transmit that data to its servers in order to enable
14 the Pixel’s core value proposition.

15 Meta’s attempt to distinguish using the Pixel from using data collected by the Pixel might
16 be more principled if, for example, the complaint alleged that the tax services collected data and
17 then sent that data to Meta themselves. But the complaint instead alleges that the tool Meta
18 admittedly created sends data to Meta in real time without any intervening actor breaking the
19 chain of transmission. The complaint alleges that Meta receives some information from the Pixel
20 before the tax services themselves receive the data.² For certain “high-traffic websites,” Meta even
21 “employs account managers to help website developers and owners use the Meta pixel” in return
22 for significant ad revenue. SAC ¶80. Thus, the complaint plausibly alleges that Meta used the
23 Pixel to collect user data.

24 Unable to avoid plaintiffs’ allegations, Meta relies instead upon a shaky analogy. It states
25

26 ² To be sure, the complaint often states that the Pixel transmits the contents of communication in
27 real time. But plaintiffs have also alleged that the Pixel collects the sort of “dialing, routing,
28 addressing, or signaling information” encompassed within Section 638.50(b), which Meta does
not dispute. Plaintiffs are therefore entitled to the inference that the Pixel transmits that “dialing,
routing, addressing, or signaling information” data in real time as well.

1 that while a police officer may be held liable under Section 638.51 for installing or using a pen
2 register without a court order to identify phone numbers called by the suspect of an investigation,
3 Meta is more like the prosecutor who subsequently uses the data collected by a pen register to
4 initiate a prosecution. Meta argues that the prosecutor cannot be held liable for using that data to
5 later prosecute the suspect. But this analogy supplies only half of the picture painted by the
6 complaint. A more apt example derived from plaintiffs’ allegations would involve a prosecutor
7 who purchased a pen register, handed that pen register to a police officer and then instructed the
8 police officer to install it without a court order and further aided the officer in doing so. If the
9 prosecutor then used the pen register to collect phone numbers in real time—whether or not the
10 prosecutor later used those phone numbers to prosecute a suspect—the prosecutor would have
11 “used” the pen register under the plain terms of the statute. The fact that the complaint alleges that
12 the Pixel allows Meta to collect data in real time in order to provide third-party websites with the
13 analytics services that flow from installation of the Pixel defeats any notion that Meta does not
14 itself use the Pixel for the purposes of Section 638.50(b).

15 The complaint therefore plausibly alleges that Meta used a pen register.

16 **II. The Pixel’s disclosure of the contents of communication does not preclude it from also**
17 **being a pen register.**

18 Meta next argues that plaintiffs have pleaded themselves out of a pen register claim. CIPA
19 defines a pen register as a “device or process that records or decodes dialing, routing, addressing,
20 or signaling information transmitted by an instrument or facility from which a wire or electronic
21 communication is transmitted, *but not the contents of a communication.*” Cal. Penal Code. §
22 638.50(b) (emphasis added). In Meta’s view, the central theory of plaintiffs’ lawsuit is that the
23 Pixel is a wiretap because it collects the contents of communications. Meta argues that plaintiffs
24 cannot have it both ways and that, by including the language “but not the contents of a
25 communication” in its definition of a pen register, CIPA precludes a device from being both a pen
26 register and a wiretap.

27 The relevant statutory language is ambiguous. On the one hand, that language could be
28 interpreted, as Meta contends, to define a pen register as a device that records *only* “dialing,

1 routing, addressing, or signaling information” and that does *not* record “the contents of a
2 communication.”³ On the other hand, it could be interpreted to define a pen register as any device
3 that records “dialing, routing, addressing, or signaling information” while clarifying that a device
4 that records *only* “the contents of a communication” is not a pen register, and is instead subject
5 solely to CIPA’s wiretap provisions. The statute does not, through its language alone, clarify
6 whether it establishes two entirely nonoverlapping zones of regulation, as Meta contends, or
7 whether a device that collects wiretap content and pen register metadata is subject to *both* CIPA’s
8 wiretap provisions and its pen register provisions.

9 In the absence of a conclusive basis in the text for resolving such a matter of statutory
10 interpretation, California courts “determine the Legislature’s intent so as to effectuate the law’s
11 purpose.” *Skidgel v. Cal. Unemp. Isn. Appeals Bd.*, 12 Cal. 5th 1, 14 (2021) (citation omitted); *see*
12 *People v. Cole*, 28 Cal. 4th 964, 975 (2006) (“If, however, the language supports more than one
13 reasonable construction, then we may look to ... the ostensible objects to be achieved and the
14 legislative history.”). Here, there is no doubt that the California Legislature, in enacting CIPA,
15 intended “to protect the right of privacy of the people of this state from what it perceived as a
16 serious threat to the free exercise of personal liberties that cannot be tolerated in a free and
17 civilized society. This philosophy appears to lie at the heart of virtually all the decisions
18 construing [CIPA].” *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (cleaned up).

19 Recognizing this intent, the California Supreme Court “has instructed courts to interpret CIPA in
20 the manner that ‘fulfills the legislative purpose of CIPA by giving greater protection to privacy
21 interests.’” *Matera v. Google, Inc.*, 15-cv-04062-LHK, 2016 WL 8200619, at *19 (N.D. Cal.
22 2016) (quoting *Flanagan*, 27 Cal. 4th at 775).

23 Given CIPA’s purpose to protect Californians’ privacy, it is highly unlikely that the
24 Legislature intended to permit the installation and use of pen registers so long as those devices
25

26
27 ³ Because Meta has not moved for dismissal on that basis, the Court assumes without deciding that
28 the complaint plausibly alleges that the Pixel records “dialing, routing, addressing, or signaling
information” that has been “transmitted by an instrument or facility from which a wire or
electronic communication is transmitted[.]” Cal. Penal Code § 638.50(b).

1 also record the contents of a third party’s communications. Under Meta’s interpretation of the
2 statute, an entity could escape liability under CIPA’s pen register provisions by combining the
3 functionality of a wiretap with that of a pen register. That entity could also escape liability under
4 CIPA’s wiretap provisions by utilizing only the information tracked by pen registers and not
5 “read[ing], or attempt[ing] to read ... the contents” of communication. Cal. Penal Code § 631(a).
6 Such an entity could engage in the very conduct that CIPA proscribes—using a pen register
7 without a court order—while escaping liability through a statutory loophole that is available only
8 because that entity collects even more sensitive information (the content of Californians’
9 communications) along with the information recorded by pen registers. In contravention of the
10 California Legislature’s intent in enacting CIPA, Meta’s proposed loophole would allow any
11 entity to avoid CIPA’s pen register provisions simply by employing more intrusive forms of
12 technology.

13 The Court raised this concern at the hearing on Meta’s motion, and Meta replied that the
14 statute was in fact intended to operate in this precise manner. Meta notes that Section 638.51(b)
15 provides an exception to 638.51(a)’s command that a “person may not install or use a pen register
16 ... without first obtaining a court order” by allowing a “provider of electronic or wire
17 communication service [to] use a pen register” without first seeking a court order in a narrow set
18 of circumstances related to running their network and providing customer service. In Meta’s view,
19 Section 638.50(b)’s exclusion of “the contents of communication” from the definition of pen
20 register is intended to clarify that telecoms cannot install an authorized pen register that operates
21 as a shadow wiretap. According to Meta, installing a device that collects the contents of
22 communications deprives the offending telecom entirely of the pen register exception and instead
23 subjects it to CIPA’s wiretap provisions.

24 Meta’s argument, however, would effectively render Section 638.51(b)’s telecom
25 exception superfluous. If Meta is correct that any entity can install a pen register that also collects
26 the contents of communication without facing liability under CIPA’s pen register provisions, why
27 would Section 638.51(b) exist at all? A telecom could install a pen register to collect metadata for
28 the purposes clearly enumerated within subsection (b)—such as to protect its own rights or

1 property—but if it were also using that device to collect the contents of communications, Section
2 638.51(a)’s court order requirement would not apply and there would be no need for an exception.
3 More troubling still, a telecom could install a pen register to collect data for purposes that do not
4 fall within subsection (b)’s enumerated exceptions—such as for advertising purposes—but if that
5 same entity also used the device to record the content on its customers phone calls, the telecom
6 could install the pen register without the court order required by Section 638.51(a).

7 Although Meta expresses concern about an authorized pen register masquerading as a
8 shadow wiretap, its argument would allow an *unauthorized* pen register to circumvent judicial
9 oversight so long as that device included a modicum of nonessential wiretapping technology.
10 Because recognizing such a loophole would significantly limit the privacy protections offered by
11 CIPA’s pen register provisions, it is unsurprising that courts regularly allow both wiretap and pen
12 register claims to proceed. *See Zarif v. Hwareh.com, Inc.*, 23-cv-0565-BAS-DEB, 2025 WL
13 486317 (S.D. Cal. Feb. 13, 2025); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal.
14 2023); *Moody v. C2 Educ. Sys. Inc.*, 742 F. Supp. 3d 1072 (C.D. Cal. 2024). Given CIPA’s
15 purpose to protect Californians against the privacy intrusions that can result from either wiretaps
16 or pen registers, the better interpretation of Section 638.51 is that it defines a pen register as any
17 device that “records dialing, routing, addressing, or signaling information transmitted by an
18 instrument or facility from which a wire or electronic communication is transmitted,” but not a
19 device that records only “the contents of communications.” Under this construction of the statute,
20 Meta’s argument that plaintiffs fail to plead its use of a pen register without a warrant fails.

21 In any event, even assuming Meta were correct that CIPA precludes a single device from
22 being both a wiretap and a pen register, its motion would still fail. The complaint alleges that the
23 Pixel is a “small library of functions” with an array of capabilities that allows the website owner to
24 do a variety of things. SAC ¶27. One of those functions collects data such as “HTTP Headers” and
25 IP addresses, while a different function collects the contents of users’ communications. If the
26 various functionalities within the Meta Pixel operate independently from one another, as plaintiffs
27 plausibly allege, the process that records metadata in a pen register-like manner is a separate
28 “device” or “process” from the one that collects the contents of users’ communications. Under

1 Section 638.51, plaintiffs are entitled to pursue a claim against Meta for its use of the pen register
2 “device” without a warrant whether or not Meta has also installed or used a separate wiretap
3 device to record and review the contents of users’ communications.

4 **CONCLUSION**

5 For the reasons stated herein, Meta’s motion to dismiss plaintiffs’ pen register claim is
6 denied.

7 **IT IS SO ORDERED.**

8 Dated: August 6, 2025

9
10 

11 P. Casey Pitts
12 United States District Judge

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
United States District Court
Northern District of California