UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DAWN FREGOSA,

Plaintiff,

v.

MASHABLE, INC.,

Defendant.

Case No. 25-cv-01094-CRB

ORDER DENYING MOTION TO DISMISS

Docket No. 34

I. INTRODUCTION

Plaintiff Dawn Fregosa brings this putative class action against Defendant Mashable, Inc. ("Mashable") under the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, et seq. Fregosa alleges that Mashable violated the Pen Register Act by embedding third-party trackers on its website. According to the Second Amended Complaint ("SAC"), these trackers unlawfully recorded users' IP addresses and device identifiers and transmitted that data to third parties for advertising and profiling.

Mashable moves to dismiss the SAC under Rule 12(b)(6), raising three arguments: (1) that the Pen Register Act applies only to person-to-person communications rather than general website activity; (2) that even if the Pen Register Act applies, Fregosa has not plausibly alleged a violation of the Act; and (3) that the rule of lenity requires dismissal because the Pen Register Act is ambiguous.

For the reasons set forth below, each argument is unavailing. The statutory text, structure, and purpose, as well as recent decisions from this District, establish that CIPA's pen register prohibition extends to software processes that record addressing information in electronic communications, including the kind of web-tracking alleged here. The SAC

plausibly alleges installation of trackers and use of resultant information by Mashable, and no grievous ambiguity warrants applying the rule of lenity. Accordingly, the motion to dismiss is **DENIED**.

II. BACKGROUND

A. Factual Background

Defendant Mashable owns and operates a digital news and entertainment website. Second Am. Compl. (SAC) (Dkt. 30) ¶ 1. Plaintiff Dawn Fregosa is a California resident who regularly visited Mashable's website between 2017 and December 2024. SAC ¶ 187.

Fregosa alleges that when she visited the Mashable website from her home in California, Mashable's servers instructed her browser to install and run third-party trackers operated by Microsoft, Wunderkind, and PubMatic. SAC ¶¶ 2–6. These trackers collect users' IP addresses and "device fingerprints" (device type, browser type, persistent identifiers) enabling cross-site recognition and targeted advertising. Id. Third parties operate these trackers and use them to engage in targeted advertising based on website visitors' location (which can be determined by IP address) and browsing data. Id.

Fregosa describes the mechanics of website tracking broadly as follows: when a user loads the Mashable webpage, the user's browser sends an HTTP request to Mashable's server. Id. ¶¶ 22–24. The server responds with instructions on how to properly display the website (e.g., what images to load, the text to display, music to play, etc.). Id. As part of this process, Mashable's servers also send instructions to browsers that install trackers on the user's browser. Id. ¶ 24. These trackers, supplied by Microsoft, Wunderkind, and PubMatic, prompt the browser to transmit identifying information — including the user's IP address and device metadata — to the third parties. Id. The trackers enable those entities to recognize the same device on subsequent visits, whether to Mashable's site or to other websites that deploy their code. Id. The SAC further alleges that Mashable and these third-party operators actively participate together in the broader data-brokerage and online advertising ecosystem. Id. ¶¶ 57–186.

Plaintiff analogizes this conduct to traditional pen registers, which record outgoing

telephone numbers by capturing "dialing, routing, addressing, or signaling information." She alleges that the trackers here perform the same functional role by recording addressing information associated with outgoing HTTP requests, and that Mashable "installed" and "used" those trackers without first obtaining a court order as required by CIPA. Id. ¶¶ 49–56; see Cal. Penal Code § 638.51(a) ("[A] person may not install or use a pen register or a trap and trace device without first obtaining a court order . . . .").

B. Procedural History

Fregosa's First Amended Complaint was dismissed for lack of personal jurisdiction, with leave to amend. Dkt. 12; 19. Fregosa filed her SAC with expanded jurisdictional allegations and additional detail about Mashable's contacts with California. Fregosa seeks to represent a class defined as "all California residents who accessed the Website in California and had their IP address collected by the Trackers." Id. ¶ 211.

Mashable does not challenge jurisdiction this time. See MTD (Dkt. 34). Mashable instead moves to dismiss solely under Rule 12(b)(6), arguing that the SAC fails to state a claim under CIPA § 638.51.

C. Statutory Framework

CIPA was enacted to protect Californians' privacy rights. See Cal. Penal Code § 630. The chapter contains several distinct provisions regulating different types of surveillance. At issue here is the Pen Register Act, codified at §§ 638.50–638.55. The Pen Register Act prohibits the installation or use of a pen register or trap-and-trace device without first obtaining a court order or user consent. Cal. Penal Code § 638.51(a)–(b). CIPA provides a private right of action with statutory damages of $5,000 per violation or three times the amount of actual damages, whichever is greater, as well as injunctive relief. Cal. Penal Code § 637.2.

The Act defines a "pen register" broadly 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) (emphasis added). A "trap

and trace device" is similarly defined as a process that captures incoming addressing information. Cal. Penal Code § 638.50(c).

Historically, these terms described devices attached to telephone lines that recorded outgoing or incoming phone numbers dialed. But more recent litigation in this district has tested whether software trackers embedded in websites qualify as "pen registers" when they collect users' IP addresses, device identifiers, and browsing data. Several judges in this district, including Judges Lin, Orrick, Pitts, Ryu, Tigar, and the undersigned, have held that such allegations suffice at the pleading stage. See, e.g., Shah v. Fandom, Inc., 754 F. Supp. 3d 924 (N.D. Cal. 2024) (Lin, J.) (holding that courts should focus "less on the form of the data collector and more on the result" and that trackers are "at least a 'process' because it is 'software that identifies consumers, gathers data, and correlates that data'"); Mirmalek v. L.A. Times Commc'ns LLC, No. 24-cv-1797-CRB, 2024 WL 5102709 (N.D. Cal. Dec. 12, 2024) (Breyer, J.) (Courts cannot ignore the "expansive language in the California Legislature's chosen definition [of pen register]" which is "vague and inclusive as to the form of the collection tool (i.e., 'device or process')") (brackets in original); In re Meta Pixel Tax Filing Cases, No. 22-cv-07557-PCP, 2025 WL 2243615 (N.D. Cal. Aug. 6, 2025) (Pitts, J.); Gabrielli v. Haleon US Inc., No. 25-cv-02555-WHO, 2025 WL 2494368 (N.D. Cal. Aug. 29, 2025) (Orrick, J.); Garon v. Keleops USA, Inc., No. 25-cv-02124-DMR, 2025 WL 2522374 (N.D. Cal. Sept. 2, 2025) (Ryu, J.); Riganian v. LiveRamp Holdings, Inc., No. 25-cv-00824-JST (N.D. Cal. July 18, 2025) (Tigar, J.).

Courts in the District have emphasized that the inclusion of the term "process" in the definition of a pen register was intended to extend the statute's reach beyond physical telephone hardware to include software tools that carry out materially similar functions. See Mirmalek v. L.A. Times Commc'ns LLC, No. 24-cv-01797-CRB, 2024 WL 5102709, at *3 (N.D. Cal. Dec. 12, 2024) (denying motion to dismiss and stressing the "vague and inclusive" language in the statute's definition of "pen register").

III. REQUESTS FOR JUDICIAL NOTICE

Mashable filed two requests for judicial notice in connection with its motion to

dismiss and its reply brief in support of its motion to dismiss. Dkt. 35, Dkt. 40.

The first request is for the court to take judicial notice of four exhibits, all of which are California superior court orders dismissing CIPA pen register claims: Sanchez v. Cars.com Inc., No. 24STCV13201, 2025 WL 487194 (Cal. Super. Jan. 27, 2025); Rodriguez v. Plivo Inc., No. 24STCV08972, 2024 WL 5184413 (Cal. Super. Oct. 2, 2024); Casillas v. Transitions Optical, Inc., No. 23STCV30742, 2024 WL 4873370 (Cal. Super. Ct. Sept. 9, 2024); and Licea v. Hickory Farms LLC, No. 23STCV26148, 2024 WL 1798147 (Cal. Super. Mar. 13, 2024). These are matters of public record and may be judicially noticed for their existence and procedural posture, though not for the truth of any disputed facts.

The second request is for the court to take judicial notice of a transcript of the testimony of California State Senator Anna Caballero at an April 29, 2025 hearing regarding Senate Bill 690, which addresses CIPA litigation. Legislative history materials are properly subject to judicial notice for the fact that they were made, though not for the accuracy of statements therein.

Accordingly, the Court **GRANTS** Mashable's requests for judicial notice.

IV. LEGAL STANDARD

Under Rule 12(b)(6), the Court may dismiss a complaint for failure to state a claim upon which relief may be granted. The Court may base dismissal on either "the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." Godecke v. Kinetic Concepts, Inc., 937 F.3d 1201, 1208 (9th Cir. 2019) (cleaned up). A complaint must plead "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (cleaned up). A claim is plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice" to survive a 12(b)(6) motion. Id. (citing Bell Atlantic v. Twombly, 550 U.S. 544, 555 (2007)). When evaluating a motion to dismiss, the Court

"must presume all factual allegations of the complaint to be true and draw all reasonable inferences in favor of the nonmoving party." Usher v. City of L.A., 828 F.2d 556, 561 (9th Cir. 1987). "[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308, 322 (2007).

V. DISCUSSION

Mashable argues that the SAC should be dismissed for three key reasons:

1. Mashable contends that California's pen register provisions apply only to "person-to-person communications, i.e., communications between or among people that occur on services like phone, text messages, email, and the like. It was never intended to govern commercial websites that do not provide people with any means to communicate with one another." SAC MTD at 1. Mashable emphasizes statutory text and legislative history, specifically recent legislative discussions about an amendment to the pen register law that would prevent its application to commercial tools for online advertising. Id. at 4–8.

2. Mashable argues that even if the pen register statute applied, the SAC fails to state a pen register claim. Id. at 2. Specifically, (a) pen registers capture outgoing data, but the data collected here is not analogous to "the outgoing numbers that someone dials from a monitored phone;" (b) Fregosa has not alleged a qualifying "communication with content" because accessing a public website is not communication with content; (c) Mashable is the intended recipient of any alleged communications, and the Pen Register Act does not prohibit a defendant from capturing information about users who contact or communicate with that defendant; and (d) to the extent Fregosa alleges third party collection of data, CIPA does not impose aiding-and-abetting liability. Id. at 2.

3. Mashable finally states that CIPA is, at best, ambiguous as to whether it applies to internet trackers, and because the statute carries criminal penalties, the rule of

lenity requires the Court to construe it narrowly. Id. at 2–3.

For the reasons set forth below, the Pen Register Act applies to the use of trackers under these circumstances, the SAC properly states a claim for a Pen Register Act violation, and the rule of lenity does not require dismissal. Accordingly, the motion to dismiss is **DENIED**.

A. Applicability of Pen Register Act to Internet Trackers

To state a claim for a violation of the Pen Register Act, a plaintiff must allege that a defendant installed or used a pen register without a court order. Cal. Penal Code § 638.51(a); Greenley v. Kochava, Inc., 684 F. Supp. 3d 1024, 1050–51 (S.D. Cal. 2023).

Mashable's principal argument is that CIPA's pen register provisions do not apply to the kind of website tracking alleged here. According to Mashable, the statute is limited to "person-to-person communications," such as telephone calls or emails, and was never intended to regulate online advertising technologies or websites. MTD at 3. This argument finds no support in the legislative text, legislative purpose, or the growing body of decisions from this District.

This Court has emphasized that the Legislature intentionally employed broad language to capture new uses of technologies: "'the Court cannot ignore the expansive language in the California Legislature's chosen definition [of pen register],' but 'vague and inclusive as to the form of the collection tool' (i.e. 'device or process')." Mirmalek v. L.A. Times Commc'ns LLC, 2024 WL 5102709, at *3 (quomting Greenley v. Kochava, Inc., 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023)). What matters under the statute is not the form of the tool, but rather the function — specifically, whether the process records routing or addressing information of a communication. See id. ("[C]ourts should focus less on the form of the data collector and more on the result.").

The statute defines a pen register broadly as any "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. Cal. Penal Code § 638.50(b). Nothing in the definition ties the statute to legacy technologies,

refers to "persons," or excludes software processes embedded in websites. See Cal. Penal Code §§ 638.50, 638.51. On the contrary, the Legislature's choice of the phrase "device or process" reflects an intentional technology-neutral approach, ensuring the statute reaches novel surveillance methods as they emerged. Courts interpreting CIPA have consistently treated the broad statutory language as intentional and significant. In Mirmalek v. L.A. Times, this Court emphasized that the legislature could have used narrower, telephone-specific terminology but instead opted for expansive language to capture evolving privacy threats. No. 24-cv-01797-CRB, 2024 WL 5102709, at *3–4. Similarly, in Shah v. Fandom, Judge Lin held that website-based tracking software could plausibly constitute a pen register, rejecting the defendant's argument that the statute is confined to telephonic data. 754 F. Supp. 3d at 929–31 ("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."); see also In re Meta Pixel Tax Filing Cases, No. 22-cv-07557-PCP, 2025 WL 2243615, at *5 (N.D. Cal. Aug. 6, 2025) (recognizing "CIPA's purpose to protect Californians' privacy" and declining to adopt defendant's narrowed interpretation of the pen register statute); Gabrielli v. Haleon US Inc., No. 25-cv-02555-WHO, 2025 WL 2494368, at *11 (N.D. Cal. Aug. 29, 2025) (emphasizing the elasticity of the Pen Register Act in regulating new technologies).

The alleged trackers function similarly to traditional pen registers and fit within the statutory definition. As alleged in the SAC, when a user loads Mashable's website, their browser sends an HTTP request to Mashable's servers, and the embedded trackers cause the browser to transmit the user's IP address and device identifiers to third parties. SAC ¶¶ 57–186. An IP address, like a telephone number, is quintessential "addressing" information transmitted by the user's computer or smartphone in connection with an outgoing HTTP request to Mashable's website: it identifies the device sending the communication and determines where the packet is to be routed. Device "fingerprints" likewise serve as unique identifiers across websites and browsing sessions. Id. ¶¶ 54–55.

At the pleading stage, alleging that these trackers record such information, while not capturing the substantive content of the communications, is sufficient to plausibly state that they function as pen registers. See, e.g., Mirmalek, 2024 WL 5102709, at *3–5; Shah, 754 F. Supp. 3d at 933; In re Meta Pixel Tax Filing Cases, 2025 WL 2243615, at *4–6; Garon, 2025 WL 2522374, at *3–5.

Courts in this district have consistently recognized similar technologies as pen registers. See, e.g., Shah, 754 F. Supp. 3d at 929–31 (denying motion to dismiss where plaintiffs alleged that third-party trackers on news website captured IP addresses and other identifiers); Mirmalek, 2024 WL 5102709, at *3–4 (highlighting the broad statutory language of the Pen Register Act and holding that trackers that transmit IP addresses and user identifiers plausibly fall within the Act's scope). Mashable urges the Court to find that Shah, and by extension Mirmalek, were "wrongly-decided" because they unduly expanded the scope of the Pen Register Act. Reply iso MTD at 10–11. But the statute is not as limited as Mashable makes it out to be, and courts must not import restrictions untied to any statutory text, particularly when doing so would interfere with the statute's purpose. See, e.g., Yeager v. Blue Cross of Cal., 175 Cal.App.4th 1098, 1103 (Cal. Ct. App. 2009) ("We may not make a silent statute speak by inserting language the Legislature did not put in the legislation."); Shah, 754 F. Supp. 3d at 929 ("Nothing in the statutory definition limits pen registers to those that operate the same way as a traditional phone pen register."); Matera v. Google Inc., 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016) (Koh, J.) ("[T]he 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.'") (quoting Flanagan v. Flanagan, 27 Cal.4th 766, 775 (Cal. 2002)).

For the foregoing reasons, the Pen Register Act applies to website-based trackers and the telecommunications processes described in the SAC.

B. Sufficiency of Pleadings Under § 638.51

Mashable argues that even if the Pen Register Act could theoretically apply to web-based trackers, the SAC fails to allege facts sufficient to state a claim for violation of the

Pen Register Act. At this stage, however, the SAC adequately pleads the statutory elements.

1. Website-Embedded Trackers Are "Pen Registers"

The threshold question is whether the "device or process" alleged qualifies as a "pen register." See Cal. Penal Code § 638.50. Here, the SAC alleges that trackers record addressing information associated with the user's outgoing HTTP requests. SAC ¶¶ 57–186. Mashable argues that the technology at issue here is not a "pen register," because "a pen register records the called party's information, and not the calling party's information." MTD at 9. The core of the argument appears to be that the process at issue in this case is the reversal of a typical pen register situation, since the website trackers capture incoming data, rather than outgoing data.

Fregosa pleads that Mashable embedded third-party trackers on its website and that, when the website was visited by users, the trackers recorded the IP address and device identifiers of the user and transmitted that information to Microsoft, Wunderkind, and PubMatic. Under § 638.50(b), a pen register includes any "device or process" that records or decodes dialing, routing, addressing, or signaling information. The definition is technology-neutral, not confined to legacy telephone equipment, and not particularly sensitive to the semantic distinction that Mashable seeks to draw. Courts in this district have widely recognized that trackers capturing IP addresses and related metadata fall comfortably within the definition of a "pen register." See Shah, 754 F. Supp. 3d at 931 ("The HTTP request transmitted from users' computers or smartphones constitutes an electronic communication, and the Trackers record the addressing information associated with the 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.'") (quoting Moody v. C2 Educ. Sys. Inc., 742 F. Supp. 3d 1072, 1076 (C.D. Cal. 2024)); see also Mirmalek, 2024 WL 5102709, at *4 ("Finally, the Trackers 'record' the addressing information by 'instruct[ing] the user's browser to send . . . the user's IP address' to the Tracker and by 'stor[ing] a cookie with the user's IP address in the user's browser cache.' .

. . Therefore, Plaintiff adequately alleges that the Trackers record addressing information, as required by CIPA.").

At the pleading stage, it is sufficient that Fregosa alleges a process designed to record addressing information from electronic communications. See Mirmalek, 2024 WL 5102709, at *4.

2. Website Visits Involve an "Electronic Communication"

Mashable suggests that website visits are not the type of "electronic communication" covered by the Pen Register Act. MTD at 10. Specifically, according to Mashable, merely visiting a website does not constitute a "communication" and therefore does not trigger the Pen Register Act. The statutory text belies Mashable's argument.

Section 638.50(b) covers information transmitted "by an instrument or facility from which a wire or electronic communication is transmitted." The statute uses expansive language and does not limit "electronic communication" in the way Mashable suggests. When a user enters Mashable's website, the browser necessarily transmits an HTTP request to Mashable's server. That request includes the user's IP address and other routing data that allow the server to deliver the requested content. This is a paradigmatic "electronic communication." Courts in this District have recognized as much. In Shah, the defendant operated a similar website. 754 F. Supp. 3d at 929. The court highlighted CIPA's expansive language, remarking that "[a]ll that is required [for a Pen Register Act claim] is that the Trackers record addressing information transmitted by the user's computer or smartphone in connection with the outgoing HTTP request to [defendant's] website, regardless of whether that addressing information pertains to the sender or the recipient of the communication at issue." Id. The court concluded that "[t]he 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.'" Shah, 754 F. Supp. 3d at 931 (quoting Moody, 742 F. Supp. 3d at 1076. This Court in Mirmalek

adopted the same reasoning. 2024 WL 5102709, at *4.

Likewise, in Gabrielli, Judge Orrick rejected the argument that web browsing falls outside the statute's scope, reasoning that CIPA's privacy-protective purposes would be frustrated by reading "communication" so narrowly as to exclude the everyday electronic interactions that the statute was designed to regulate. Gabrielli v. Haleon US Inc., No. 25-cv-02555-WHO, 2025 WL 2494368, at *12 (N.D. Cal. Aug. 29, 2025) ("Haleon also asserts, in passing, that Gabrielli's Section 638.51(a) pen register claim cannot coexist with his Section 631(a) wiretapping claim because pen registers 'do not record contents,' but wiretaps do. . . . This argument would lead to the conclusion that any pen register that also recorded the 'contents' of users' information would no longer fall under the protection of Section 638.51(a) of CIPA. That cannot have been the Legislature's intent.").

Mashable's position — that there must be an interpersonal exchange — is unsupported. Nothing in the text requires that a communication involve two human correspondents. An HTTP request from a user's browser to a website server is a sufficient communication. By alleging that she visited Mashable's website and that her browser transmitted HTTP requests containing identifying information, Fregosa has adequately alleged a qualifying communication under the statute.

3. Defendant's Status as a Party to the Communication

Mashable argues that the Pen Register Act cannot apply to it because of its role in the communications at issue. Mashable raises two related points: first, that as a direct party to users' communications, it cannot be liable for the receipt of IP addresses and other identifying data; and second, that it did not itself install or use the trackers, since those were operated by third-party vendors. Neither argument is persuasive at this stage.

First, Mashable argues that, as the operator of the website at issue, it is a direct party to any communication from the user's browser and therefore cannot be liable for learning information that users necessarily disclose when visiting a website, such as their IP address. MTD at 10–11. This framing mischaracterizes the SAC. Fregosa does not allege that Mashable violated CIPA simply by receiving IP addresses as part of an ordinary

online exchange. Rather, the SAC alleges that Mashable affirmatively embedded third-party trackers that recorded and transmitted users' identifying information to outside entities for profiling and advertising purposes. Courts have rejected similar attempts to dismiss complaints when the allegations involved transmission of data to third parties. In Shah, the defendant raised this exact point, contending that users voluntarily disclosed their IP addresses by visiting the defendant's website. 754 F. Supp. 3d at 931. The court explained that consent is limited to the narrow conduct authorized, and that a user who expects to disclose information to the website operator does not thereby consent to disclosure to unrelated third parties. Id. at 931–32. Here too, Mashable cannot claim a categorical exemption merely because it was a party to the initial communication.

Second, Mashable argues that even if trackers can qualify as pen registers, Mashable cannot be liable because it was the third-party vendors, and not Mashable itself, that installed and operated the trackers. This defense is also insufficient at this stage. In Shah, the court held that plaintiffs adequately alleged installation where the defendant incorporated third-party code into its site, thereby causing users' browsers to run the trackers. Id. at 931 ("Even if third parties 'developed and used the [Tracker] software,' it is alleged that [defendant] was responsible for integrating the third-party script into its own website. Based on this, Plaintiffs' allegation that [defendant] installed the Trackers is sufficient to state a claim."). Similarly, in In re Meta Pixel Tax Filing Cases, Meta argued that it did not "use" a pen register because other entities installed the Pixel, and Meta only received the data afterward. No. 22-cv-07557-PCP, 2025 WL 2243615, at *3 (N.D. Cal. Aug. 6, 2025). Judge Pitts rejected that characterization, likening it to "a prosecutor who purchased a pen register, handed that pen register to a police officer and then instructed the police officer to install it without a court order and further aided the officer in doing so." Id. Under the plain language of the statute, the prosecutor would have "used" the pen register. Id. The SAC alleges a comparable dynamic: Mashable deliberately embedded third-party trackers on its website, knew that those trackers would capture visitors' IP addresses and device metadata, and used the resulting data in concert with Microsoft,

Wunderkind, and PubMatic to facilitate targeted advertising. SAC ¶¶ 57–186. That active role is enough to plead "use" under § 638.51, even if technical operations were handled by third parties.

Finally, Mashable also refers to an "aiding-and-abetting" concern, suggesting that Fregosa is improperly attempting to impose liability for the acts of third parties. MTD at 11–12. The SAC, however, pleads direct, not secondary, liability: it alleges that Mashable embedded third-party trackers in its own website, thereby causing users' browsers to install and run them, and that Mashable used the resulting data flows. On those facts, Mashable itself "installed" and/or "used" a "device or process" that records addressing information, i.e., a pen register. See Cal. Penal Code §§ 638.50, 638.51(a). This theory turns on Mashable's own conduct, not vicarious liability or aiding-and-abetting liability for the acts of others.

For the foregoing reasons, Mashable has not established any exemption from the Pen Register Act.

4. Effect of Senate Bill 690 on the Issues Presented

Mashable relies on the pending Senate Bill 690 as evidence that the California Legislature disagrees with Fregosa's interpretation of the Pen Register Act — and by extension, the Northern District's orders in Shah, Mirmalek, Gabrielli, and In re Meta Pixel Tax Filing Cases. See MTD at 8. The Senate's floor analysis describes S.B. 690 as an effort to "stop the thousands of shakedown letters and lawsuits against California businesses of all sizes for typical business activities, like website analytics or online advertising that are already governed by" other laws. Id. (quoting Senate Floor Analysis — Third Reading of S.B. 690 Before the S. Rules Comm., 2025–2026 Reg. Sess. (Cal. 2025) at 8).

Mashable's argument is unpersuasive for several reasons:

First, S.B. 690 is not the law. It has not passed the Legislature or been signed by the Governor. The Court must apply the statute as it currently exists, and the operative text of the Pen Register Act is clear in its scope and applicability. Unenacted bills are not a

proper basis for judicial narrowing of statutory text. See U.S. v. King, 24 F.4th 1226, 1232 (9th Cir. 2022) ("But we cannot rely upon unenacted bills to modify an existing statute, as that is a function of Congress.").

Second, as Fregosa notes, the provision that would have allowed the bill to apply retroactively was removed during the legislative process. Opp. to MTD at 7 (citing California Senate Bill 690, https://legiscan.com/CA/text/SB690/2025). Thus, even if S.B. 690 were enacted into law in its present form, it would have no effect on this case which exclusively concerns conduct that occurred before the bill's potential enactment.

Third, subsequent legislative activity carries little interpretive weight, particularly when it post-dates the conduct at issue. See Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc., 447 U.S. 102, 117–18 (1980) ("[V]iews of a subsequent Congress form an extremely hazardous basis for inferring the intent of an earlier one."); Carmona v. Div. of Indus. Safety, 13 Cal.3d 303, 311 n.8 (Cal. 1975) ("First, it is well established that courts will generally not rely even on statements made by individual lawmakers as a reliable expression of the intent of the entire legislative body.").

Finally, courts in this District have already declined to stay litigation pending the outcome of S.B. 690. In Garon v. Keleops, Judge Ryu rejected a request for a stay, reasoning that the bill's status was "too tenuous to form a basis to stay the case" given that "[t]here is no indication when SB690 will be enacted" or whether the proposed language would survive in its final form. No. 25-cv-02124-DMR, 2025 WL 2522374, at *6 (N.D. Cal. Sept. 2, 2025). That reasoning applies equally here. The Court should not defer adjudication or rewrite statutory text based on an unenacted proposal.

C. Rule of Lenity

Finally, Mashable invokes the rule of lenity, arguing that ambiguities in the statute must be resolved in its favor. MTD at 12–15. But as courts have recognized, the rule of lenity has little force in this context.

The rule of lenity applies "when two reasonable interpretations of the same provision stand in relative equipoise," not "every time there are two or more reasonable

interpretations of a penal statute." Smith v. LoanMe, Inc., 11 Cal.5th 183 (Cal. 2021). More specifically, the rule of lenity applies "only if the court can do no more than guess what the legislative body intended; there must be an egregious ambiguity and uncertainty to justify invoking the rule." People v. Super. Ct. of Riverside Cnty., 81 Cal.App.5th 851, 886 (Cal. Ct. App. 2022) (internal quotations omitted); see Vera v. O'Keefe, 791 F. Supp. 2d 959, 965 (S.D. Cal. 2011) (ruling in the invasion of privacy context that defendant "has at most shown that a narrower interpretation" of the statute "is conceivable, but that is insufficient to establish ambiguity. '[D]isputed words or phrases in criminal laws have in many instances been interpreted broadly, defeating defendants' claims'") (brackets in original).

As noted above, the statute contains no grievous ambiguity: its language, structure, history, and purpose are sufficiently clear, and they leave no need for the Court to merely speculate about its applicability. The statutory text is deliberately expansive, designed to encompass new technologies and apply to conduct like that alleged here. See Mirmalek, 2024 WL 5102709, at *3.

The district court has previously disregarded similar rule of lenity arguments in the pen register context. In Riganian, Judge Tigar disposed of a similar argument, reasoning that "[t]he 'rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a 'grievous ambiguity or uncertainty in the statute.'" Riganian v. LiveRamp Holdings, Inc., No. 25-cv-0824-JST, 2025 WL 2021802, at *12 (N.D. Cal. July 18, 2025) (quoting Barber v. Thomas, 560 U.S. 125, 139 (2010)). In the absence of any "grievous ambiguity" in the statute's express language, a defendant may not invoke the rule of lenity. Id.; see also Garon v. Keleops USA, Inc., 2025 WL 2522374, at *6 ("Like the defendant in Riganian, Keleops has not identified any 'grievous ambiguity or uncertainty' in CIPA.").

Because Mashable similarly has not identified a "grievous ambiguity" in the pen register statute, the rule of lenity does not apply, and the Court should not dismiss on this basis.

VI. CONCLUSION

For the foregoing reasons, the Court hereby **DENIES** Defendant Mashable's motion to dismiss the Second Amended Complaint.

IT IS SO ORDERED.

Dated: October 9, 2025

CHARLES R. BREYER
United States District Judge