No. 26-1652

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DYWANNA DRUMMER, et al.,
Plaintiffs-Appellees

v.

COSTAR GROUP, INC.,
Defendant-Appellant

On Appeal From the United States District Court for the
Central District of California, Case No. 5:25-cv-01047-JGB-SP
The Honorable Jesus G. Bernal

BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Jonathan D. Urick
Mariel A. Brookins
U.S. CHAMBER LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

Megan L. Brown
Jeremy J. Broggi
Boyd Garriott
Stephanie Rigizadeh
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
(202) 719-7000
mbrown@wiley.law

Counsel for Amicus Curiae, Chamber of Commerce of the United States of America

June 4, 2026

RULE 26.1 CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus curiae* Chamber of Commerce of the United States of America hereby certifies that it is a non-profit, tax-exempt corporation incorporated in the District of Columbia. It has no parent corporation, and no publicly held company has 10% or greater ownership in the Chamber.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*[1]

The Chamber of Commerce of the United States of America is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases, like this one, that raise issues of concern to the nation's business community.

This case is of particular concern. The plaintiffs here have brought a novel kind of claim that, unfortunately, has recently become increasingly common among litigants seeking statutory damages untethered to any concrete injury. These claims target legitimate businesses and accuse them of "invasion of privacy" for using ubiquitous technologies. The claim here is particularly aggressive. It targets the alleged collection and transmission of IP addresses—a practice that is both commonplace and necessary for the basic functionality of the Internet.

[1] All parties have consented to the filing of this brief. No counsel for any party authored this brief in whole or in part and no entity or person, aside from *amicus curiae*, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of the brief. *See* Fed. R. App. P. 29(a)(4)(E).

The playbook is straightforward. A plaintiff visits a company's website and departs. He then files suit under the California Invasion of Privacy Act ("CIPA") alleging that the company collected his IP address. CIPA is a criminal statute, meaning that the plaintiffs are in effect accusing the company of an offense punishable by prison time. But CIPA also affords plaintiffs a private cause of action with a lucrative $5,000-per-violation bounty.

It is no mystery why such suits have proliferated. Plaintiffs can sue with ease because *every time* someone accesses a website, his browser transfers the IP address to the website's server. That is just how the Internet works. And plaintiffs incur no downside visiting these supposedly privacy-infringing websites. No harm, no penalty, no adverse impact of any kind. All they do is access a website, and then they can sue for thousands of dollars in statutory damages.

But the very things that make these suits attractive for plaintiffs are also the reasons why they cannot prevail. Start with the fact that they incur no harm. In federal court, a plaintiff cannot bring a suit unless he suffers a concrete injury. A website's routine collection of visitors' IP addresses inflicts no harm, and so the plaintiffs here have no standing. Next, the fact that the collection and transmission of IP addresses is ubiquitous is also the exact reason why no fair reading of CIPA would criminalize those activities. The California Legislature did not seek to outlaw the basic functions that allow the Internet to exist. Indeed, a completely different

California law applies to the activities and data here at issue, making misuse of CIPA as unnecessary as it is improper. Thus, not only do the plaintiffs here lack standing, but they are also wrong on the merits.

The Court should instruct the district court to dismiss this case. As the Chamber has consistently explained, the Judiciary's rigorous enforcement of Article III standing and its faithful interpretation of the Legislature's enactments is a fundamental check against abusive state-law litigation. *See, e.g.*, Brief of the Chamber of Commerce, et al., *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025) (No. 24-14); Brief of the Chamber of Commerce, *Variety Media, LLC v. Superior Ct.*, Case No. B350578 (Cal. Ct. App.) (Apr. 8, 2026); Brief of the Chamber of Commerce, *Fausett v. Walgreen Co.*, 2025 IL 131444 (Nov. 20, 2025) (No. 131444). Enforcing those limits here is critical to controlling the deluge of coercive CIPA litigation that ultimately renders every business in California a defendant-in-waiting.

ARGUMENT

I. PLAINTIFFS LACK STANDING.

Standing is "the irreducible constitutional minimum" required by Article III's "case-or-controversy requirement." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). To satisfy that minimum, Plaintiffs were required to plead a "concrete harm," *Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016), by demonstrating "a 'close

relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts," *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021).

The district court concluded that Plaintiffs alleged a concrete harm, but that holding must be reversed for two reasons. *First*, the district court's concreteness analysis cannot be reconciled with this Court's decision in *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025). *Second*, a proper analysis of *Popa* and the Supreme Court's concreteness precedents shows that Plaintiffs have not alleged facts to support Article III standing.

A. This Court's Decision In *Popa v. Microsoft* Requires Reversal.

The district court's Article III holding must be reversed for a simple reason: it is flatly inconsistent with this Court's controlling decision in *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025).

Start with the similarities between *Popa* and this case. *Popa* considered a state-wiretap law claim. 153 F.4th at 787. So too here. ER-8 ("The Complaint alleges one cause of action: a violation of the California Inva[s]ion of Privacy Act."). *Popa* concerned a plaintiff's allegations that a company captured "information" when the plaintiff "visited [a] website." 153 F.4th at 786. So too here. ER-9 (alleging defendant "installed tracking software … on its websites"). And *Popa* "turn[ed] on … whether [the plaintiff] … alleged a 'concrete' injury sufficient to

support Article III standing." 153 F.4th at 788. So too here. ER-11–12. In other words, *Popa* fits this case like a glove.

Popa's standing analysis was also crystal clear. To assess concreteness, a court must "assess whether an individual plaintiff has suffered a harm that has traditionally been actionable in our nation's legal system." 153 F.4th at 791. To do so, the court must "look to the *specific* underlying harm experienced by the plaintiff and compare it, in detail, to a *specific* common-law tort." *Ibid.* (emphasis in original). In *Popa*, the plaintiff could not meet this burden. She identified "common-law privacy torts," which required "'highly offensive' interferences or disclosures" to be "actionable at common law." *Ibid.* However, "Popa identifie[d] no embarrassing, invasive, or otherwise private information collected" that could satisfy the "highly offensive" standard. *Ibid.* Thus, she did not "adequately allege[ ] standing." *Id.* at 795.

Despite this case being squarely controlled by *Popa*, the district court declined to employ its analysis. The district court held that the alleged "collection and dissemination of [plaintiffs'] IP addresses" was "a cognizable injury in fact." ER-12. That's it. No mention of any "*specific* underlying harm." *Popa*, 153 F.4th at 791 (emphasis in original). No identification of any "*specific* common-law tort." *Ibid.* (emphasis in original). No discussion of the "highly offensive" standard. *Ibid.* No consideration of whether any information was "embarrassing, invasive, or

otherwise private" or whether the alleged harm met other common-law requirements. *Ibid.* That was error. Article III "*requires*" *Popa*'s concreteness analysis, *ibid.* (emphasis added), and it is completely absent from the district court's opinion.

For this reason alone, the district court's analysis cannot stand. *See, e.g.*, *Acad. of Country Music v. Cont'l Cas. Co.*, 991 F.3d 1059, 1069 (9th Cir. 2021) (vacating district court order that "erred as a matter of law" and "failed to follow Supreme Court and Ninth Circuit precedent").

B. Plaintiffs Did Not Adequately Plead Standing.

This Court should instruct the district court to dismiss the Complaint for failure to allege a concrete injury.

Start with the fundamentals. "To have Article III standing," Plaintiffs must have "suffered a concrete harm." *TransUnion*, 594 U.S. at 417. "No concrete harm, no standing." *Ibid.* That requirement is ironclad "even in the context of a statutory violation." *Robins*, 578 U.S. at 341. Where, as here, plaintiffs allege an intangible harm, they must show that their "injuries" have "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion*, 594 U.S. at 425. And, as this Court explained in *Popa*, that analysis requires a court to "look to the *specific* underlying harm experienced by the plaintiff and compare it, in detail, to a *specific* common-law tort." 153 F.4th at 791.

Plaintiffs cannot make this showing. They allege one so-called harm: "the collection and dissemination of their IP addresses." ER-12. And while they do not connect that alleged harm to a "*specific* common-law tort," 153 F.4th at 791, they gesture at an "expectation of privacy," ER-12.[2] Even charitably assuming that Plaintiffs' vague invocation of privacy means "the common-law privacy torts of intrusion upon seclusion and public disclosure of private facts," *Popa*, 153 F.4th at 791, they flunk concreteness for at least two reasons.

First, Plaintiffs have "not explain[ed]" how the collection and dissemination of their IP addresses "caused [them] to experience any kind of harm that is remotely similar to the 'highly offensive' interferences or disclosures that were actionable at common law." *Popa*, 153 F.4th at 791. Nor could they. An IP address is simply "a digital routing number" assigned to Internet-connected devices and used to "facilitate the orderly flow of electronic traffic." *United States v. Lowers*, 170 F.4th 134, 142 n.5 (4th Cir. 2026). That technical number looks nothing like "the hypotheticals set out in the Restatement" as examples of actionable privacy torts—things like "look[ing] into the windows of [a neighbor's] bedroom … [and] taking intimate pictures with a telescopic lens" or "publish[ing], without [a person's] consent, a picture of [her] nursing her child." *Popa*, 153 F.4th at 791. IP addresses

[2] Plaintiffs also allege that their collected data was "economically valuable," ER-12, but, as CoStar explains (at 34–35), they never connect that conclusory allegation to an actual dollars-and-cents harm.

"do[ ] not implicate a similarly sensitive sphere," *ibid.*, as district courts throughout this Circuit have recognized.[3]

Second, Plaintiffs' IP addresses are not private information. As one would expect, common-law privacy torts are actionable for only *private* matters. *See* Restatement (Second) of Torts § 652D cmnt. B (Am. Law Inst. 1977) (explaining that claim for public disclosure of private facts "applies only to publicity given to matters concerning the private, as distinguished from the public, life of the individual"); *id.* § 652B cmnt. C (explaining that claim for intrusion upon seclusion is actionable "only when [the defendant] has intruded into a private place, or has otherwise invaded a private seclusion"; "there is no liability for the examination of a public record concerning the plaintiff").

IP addresses are not "private" in any sense of the word. IP addresses are "a series of numbers and letters" assigned to an "Internet-connected device." *The Domain Name System*, ICANN, https://tinyurl.com/rm5asp2m (last visited June 4, 2026). They are allocated at a macro level by the Internet Corporation for Assigned

[3] *See e.g.*, *Rodriguez v. Brushfire Recs.*, 2025 WL 3692144, at *7 (C.D. Cal. Dec. 15, 2025) (denying standing because collection of "IP address" was not "a highly offensive intrusion"); *Khamooshi v. Politico LLC*, 786 F. Supp. 3d 1174, 1180 (N.D. Cal. 2025) (denying standing because "IP addresses are information about an address associated with a device, not sensitive personal information" "whose disclosure would be considered highly offensive to a reasonable person" (quotations omitted)); *see also Xu v. Reuters News & Media Inc.*, 2025 WL 488501, at *5 (S.D.N.Y. Feb. 13, 2025) (denying standing because collection of IP address was not "offensive to a reasonable person").

Names and Numbers ("ICANN")—a California-based nonprofit. *See About ICANN*, ICANN, https://tinyurl.com/kzryb8x (last visited June 4, 2026). But an individual user typically operates from an IP address sub-allocated by their "Internet service provider." *Cox Commc'ns, Inc. v. Sony Music Ent.*, 607 U.S. ___, 146 S. Ct. 959, 965 (2026). There is not a one-to-one relationship between IP addresses and users. "For example, a household, coffee shop, or college dormitory ordinarily has one IP address, but has multiple individual users." *Ibid.*; *see also Cobbler Nevada, LLC v. Gonzales*, 901 F.3d 1142, 1146 (9th Cir. 2018) ("it is not always easy to pinpoint the particular individual or device" associated with "an IP address").

Because IP addresses are used to connect devices across the Internet, they are shared with—and collected by—many parties, including the websites a user chooses to visit. For example, this Court's *own website* provides: "If you visit our site to view or download information, we collect and store the following information: … The IP address from which you accessed the Judiciary's website." *Privacy Policy*, United States Court of Appeals for the Ninth Circuit, https://tinyurl.com/by6mt5ym (updated June 3, 2026). And there are lawful services that monitor and collect IP addresses from across the public Internet. *See Cox*, 146 S. Ct. at 965 (describing copyright enforcement service that "trace[s] … infringing activity to a particular IP address"). An alphanumeric string created by one third party (ICANN), assigned by another third party (an Internet service provider), used by other third parties (users

on a shared IP address), and constantly shared with scores of even more third parties (e.g., websites the user chooses to visit) is not private. Indeed, courts throughout this Circuit and beyond have recognized that the non-private nature of IP addresses forecloses standing for privacy claims premised on their collection.[4]

The non-private nature of IP addresses is true as a general matter and doubly true here. As the Supreme Court has explained, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Carpenter v. United States*, 585 U.S. 296, 308 (2018); *accord In re Facebook, Inc.*

[4] *See also, e.g.*, *In re USA Today Co., Inc. Internet Tracking Litig.*, 2026 WL 932655, at *2 (N.D. Cal. Apr. 6, 2026) (denying standing because "there is no legally protected privacy interest in IP addresses"); *Maghoney v. Dotdash Meredith, Inc.*, 2026 WL 497402, at *5 (S.D. Cal. Feb. 23, 2026) (denying standing because "no reasonable expectation of privacy attaches to IP addresses"); *Bradshaw*, 2025 WL 3171740, at *4–*6 (denying standing because "the case law overwhelmingly supports th[e] argument" that "there is no reasonable expectation of privacy in one's IP address"); *Rodriguez v. Culligan Int'l Co.*, 2025 WL 3064113, at *4 (S.D. Cal. Nov. 3, 2025) (denying standing because "[c]ourts have consistently held that internet users have no expectation of privacy in their IP addresses"); *Mitchener v. CuriosityStream, Inc.*, 815 F. Supp. 3d 845, 851 (N.D. Cal. 2025) (denying standing because "it is well established in the Ninth Circuit that 'there is no legally protected privacy interest in IP addresses'"); *Khamooshi*, 786 F. Supp. at 1179 (denying standing because, "[a]s many courts have explained, 'there is no legally protected privacy interest in IP addresses'" because "[w]hen internet users visit a website, their devices automatically send their IP addresses to the website's server as part of the communication process"); *Carolus v. Nexstar Media Inc.*, 2025 WL 1338193, at *1 (N.D. Cal. Apr. 9, 2025) (denying standing because "people do not have a reasonable expectation of privacy in IP addresses"); *Xu*, 2025 WL 488501, at *5 (denying standing because "the cases are legion holding that a person does not have a legitimate expectation of privacy in an IP address which he voluntarily turned over to a third party in order to access its website").

Internet Tracking Litig., 956 F.3d 589, 604 n.7 (9th Cir. 2020) ("we have … found analogies to Fourth Amendment cases applicable when deciding issues of privacy related to technology"). Here, Plaintiffs allege that they "visited" CoStar's websites, ER-12, meaning that they "voluntarily turned over" their IP addresses "to direct [CoStar]'s servers." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Thus, Plaintiffs had "no expectation of privacy in … [their] IP addresses." *Ibid.*; *see also United States v. Rosenow*, 50 F.4th 715, 738 (9th Cir. 2022) ("no expectation of privacy in … IP address[ ] … because it is voluntarily transmitted to third parties" (quotations omitted)); *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014) (similar); *Bradshaw v. Lowe's Companies, Inc.*, 2025 WL 3171740, at *5 (S.D. Cal. Nov. 12, 2025) (collecting appellate decisions).

The district court was also wrong to place significance on "Defendant's alleged transmission of the IP address to others with whom Plaintiff did not share the address." ER-12. That is because once someone "voluntarily turns [information] over to third parties," he no longer has a "legitimate expectation of privacy … even if the information [wa]s revealed on the assumption that it w[ould] be used only for a limited purpose." *Carpenter*, 585 U.S. at 308. When one "reveal[s] his affairs to another," he "takes the risk … that the information will be conveyed" to another party. *United States v. Miller*, 425 U.S. 435, 443 (1976); *see also United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000) (similar); *accord Khamooshi*, 786 F.

Supp. at 1179–80 (rejecting that "disclosure of IP addresses gives rise to a privacy injury"). And, as explained, a user's IP address was never private to begin with—a fact that does not change regardless of how many times it is transmitted.

Without concrete injury, there can be no case. This Court should remand with instructions to dismiss.

II. PLAINTIFFS HAVE FAILED TO STATE A CLAIM.

Even if Plaintiffs had standing (they do not), their CIPA claims are meritless. The reason is simple: the statute's pen-register provisions are limited to *telephonic* information and do not reach *Internet* information, such as IP addresses.[5]

That interpretation is compelled by the "California canons of construction." *Santa Clarita Valley Water Agency v. Whittaker Corp.*, 99 F.4th 458, 485 (9th Cir. 2024). California courts' "fundamental task … is to determine the Legislature's intent so as to effectuate the law's purpose." *People v. Lopez*, 587 P.3d 587, 596 (Cal. 2026). That requires analysis of "the statute's words, giving them a plain and commonsense meaning." *Ibid.* Context is everything. A statute's words must be construed "keeping in mind the nature and obvious purpose of the statute." *Ibid.* And where, as here, a statute is part of the Penal Code, California courts "construe the law as favorably to criminal defendants as reasonably permitted," *People v.*

[5] Because this threshold limitation forecloses Plaintiffs' claim, the Court can reverse even without reaching CoStar's independent point (at 36–49) that pen registers include only devices that collect destination information.

Robles, 5 P.3d 176, 182 (Cal. 2000) (quotations omitted), even when they interpret the statute in a civil setting, *see, e.g.*, *Harrott v. Cnty. of Kings*, 25 Cal. 4th 1138, 1154 (Cal. 2001) ("The [rule of lenity] applies even though this is not a criminal prosecution because the statute we are construing imposes criminal penalties.").

Applied here, CIPA's pen-register provisions are limited to telephonic information and do not reach the collection of IP addresses. First, consider the statutory text. A "pen register" is "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); *see also id.* § 638.50(c) (defining "trap and trace device" as "device or process that captures … the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication"). The definition creates an exception for "a device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider." *Id.* § 638.50(b). Although this language is "highly technical," it must be construed "in conjunction with the context and purpose of the statute." *People v. Garcia*, 391 P.3d 1153, 1161 (Cal. 2017).

Here, that text, context, and purpose are overwhelmingly telephone-centric. The definition leads with "dialing" information and reaches only information transmitted in the course of a "communication." These are aspects of traditional telephone communications. Further, the definition conceives of a relationship with a "provider" of "communications services" and a "customer" who is "billed." That perfectly describes a telephone company and its subscribers. But it would be, at best, an awkward way to describe a website visitor, who is not engaged in any comparable service relationship or billing arrangement. It is thus plain that the Legislature wrote this definition with telephone calls in mind.[6]

That text tracks the long-accepted meaning of "pen register" as a "device that records the numbers dialed on a telephone." *Smith v. Maryland*, 442 U.S. 735, 736 n.1 (1979); *see also United States v. Carneiro*, 861 F.2d 1171, 1173 n.2 (9th Cir. 1988) ("trap and trace device records the originating telephone numbers of incoming telephone calls"). And indeed, that is the exact meaning contemplated by the Legislature. CIPA's author explained that "a 'pen register' … allows law enforcement officers to record all *outgoing numbers from a particular telephone line*." Assemb. Floor Analysis, Assemb. B. 929, 2015–2016 Reg. Sess., at 4 (Cal. 2015) (emphasis added), https://tinyurl.com/2hek6wdp. That historical

[6] Although the statute refers to "electronic communication," that phrase does not expand the provision beyond its core focus on communications-routing information of the sort captured in telephone-based systems.

understanding confirms the statute's focus and reinforces that its technical language was not intended to sweep in fundamentally different technologies than telephony.

The statutory structure reflects that understanding. When a California magistrate authorizes "the installation and use of a pen register or a trap and trace device," Cal. Penal Code §§ 638.52(b), 638.53(a)(1), he "shall specify … [t]he identity, if known, of the person to whom is leased or in whose name is listed *the telephone line* to which the pen register or trap and trace device is to be attached … [and] [t]he *number* and, if known, physical location of *the telephone line*," *id.* § 638.52(d)(1), (3) (emphasis added).[7] And when law enforcement lawfully collects information with "a pen register or a trap and trace device," it "shall not include any information that may disclose the physical location of *the subscriber*, except to the extent that the location may be determined from *the telephone number*." *Id.* § 638.52(c) (emphasis added).

These provisions—and scores of others—make sense only if CIPA's pen-register provisions are limited to the collection of telephonic information. *See also id.* §§ 638.52(g) ("the person owning or leasing *the line* to which the pen register or trap and trace device is attached" (emphasis added)), 638.52(i) ("shall immediately

[7] By contrast, the federal pen-register statute requires that such orders specify "the telephone line *or other facility* to which the pen register or trap and trace device is to be attached or applied." 18 U.S.C. § 3123(b)(1)(A) (emphasis added). That the California Legislature has declined to expand its own statute beyond "telephone line[s]" further reinforces its intentional telephonic limitation.

install the device on the appropriate *line*" (emphasis added)), 638.54(b)(1) (authorizing prohibition on "disclosing the existence of the pen register or trap and trace device … to the listed *subscriber*" (emphasis added)), 638.52(g) ("listed *subscriber*" (emphasis added)).

The telephonic limitation thus ensures, consistent with California's interpretive rules, that CIPA's provisions are "harmonized, both internally and with each other." *Shear Dev. Co., LLC v. California Coastal Comm'n*, 587 P.3d 548, 563 (Cal. 2026); *see also City of Gilroy v. Superior Ct.*, 581 P.3d 1138, 1145 (Cal. 2026) ("We construe statutory language in the context of the statutory framework, seeking … to harmonize its different components.").

That interpretation also harmonizes CIPA with another statute: the California Consumer Privacy Act ("CCPA"). *See Hohenshelt v. Superior Ct.*, 573 P.3d 944, 954 (Cal. 2025) ("We … construe every statute with reference to the whole system of law of which it is a part[.] … This rule applies [even where] the statutes to be harmonized appear in different codes."). Unlike CIPA, the CCPA *does* reach IP addresses. *See* Cal. Civ. Code § 1798.140(v)(1)(A) (defining "personal information" to reach, *inter alia*, an "Internet Protocol address"). And it does *not* ban their collection. Rather, it authorizes IP-address collection "reasonably necessary and proportionate to achieve the purposes for which the [IP address] was

collected or processed," *id.* § 1798.100(c), so long as the company collecting the information abides by certain rules, *see e.g.*, *id.* § 1798.110 (customer disclosure).

Plaintiffs' reading of CIPA would drive a truck through the Legislature's measured regulation of IP-address collection in the CCPA. If CIPA reaches IP addresses, it would mean that their collection is a *criminal* offense punishable "by imprisonment" and "fine[s]." Cal. Penal Code § 638.51(c). That would render a dead letter the CCPA's "necessary and proportionate" standard, as well as its rules governing IP-address collection. That outcome is precisely the kind of inter-statute conflict that the California Supreme Court strives to avoid. *See, e.g.*, *People v. Superior Ct. (Guevara)*, 577 P.3d 948, 964 (Cal. 2025) ("We decline to find a conflict between [statutes] where a reasonably possible alternative interpretation gives force and effect to all of their provisions and reconciles seeming inconsistencies in them." (cleaned up)). And if there were an irreconcilable conflict, the CCPA's measured regulation of IP-address collection would supersede CIPA's criminal ban because the CCPA is "more specific" and a "later enactment[ ]." *Lopez v. Sony Elecs., Inc.*, 420 P.3d 767, 771 (Cal. 2018).

Reading CIPA to criminalize the collection of IP addresses would also be so "broad" that it would defy "common sense." *Sellers v. Superior Ct.*, 582 P.3d 950, 955 (2026). It would mean that the California Legislature criminalized basic functionality necessary for the Internet to work, *see infra* Section III, and then

subsequently enacted through the CCPA a completely meaningless, highly detailed regulatory scheme governing IP address collection. And it would have done all of this without any express reference to IP addresses in the statutory text or legislative history. California courts reject such "absurd results." *People v. Faial*, 572 P.3d 510, 519 (Cal. 2025); *see also Van Buren v. United States*, 593 U.S. 374, 393 (2021) (rejecting "interpretation of [a] statute" that "would attach criminal penalties to a breathtaking amount of commonplace computer activity").

It is thus unsurprising that a growing consensus of California lower courts—courts that apply California law every day—recognize that CIPA "was not intended to apply to website tracking tools." *Rodriguez v. Ink America Int'l Group LLC*, 2025 WL 4034985, at *3–*4 (Cal.Super. Dec. 10, 2025); *see also Balabbo v. Wildflower Brands, LLC*, 2026 WL 1122773, at *8 (Cal.Super. Apr. 06, 2026) ("The Court does not infer a legislative intent to criminalize the very process of recording or capturing information under the CIPA when that process is permitted under detailed circumstances under the CCPA."); *Schallert v. Palo Alto Networks, Inc.*, 2026 WL 754028, at *2 (Cal.Super. Mar. 06, 2026) ("the court finds that the CIPA does not extend to website communications"); *Cammorata v. Sonifi Sols., Inc.*, 2026 WL 500856, at *2 (Cal.Super. Feb. 18, 2026) (declining to "extend[ ] the application of CIPA to the internet"); *Schallert v. Orkin LLC*, 2025 WL 4332757, at *6 (Cal.Super. Dec. 15, 2025) ("the Court cannot conclude that the Legislature *sub silentio* intended

to establish a regulatory regime over web tracking through the cryptic reference to a 'trap and trace device'"); *Sanchez v. Cars.com Inc.*, 2025 WL 487194, at *2–*4 (Cal.Super. Jan. 27, 2025) (explaining CIPA reaches "information from telephone numbers, and not internet communications such as websites"); *Casillas v. Transitions Optical, Inc.*, 2024 WL 4873370, at *4 (Cal.Super. Sep. 09, 2024) ("The pen register statute did not, and does not, criminalize the process by which all websites communicate with all users who choose to access them.").

This Court should reject Plaintiffs' nonsensical reading of CIPA.

III. PLAINTIFFS' CLAIMS WOULD OPEN THE FLOODGATES OF CIPA LITIGATION.

The implications of accepting Plaintiffs' legal theory are significant. Article III and the telephonic limitation of CIPA are the dam protecting Californians from a flood of abusive litigation, and Plaintiffs would blast it wide open.

Start with the *already* widely-acknowledged issues surrounding CIPA litigation. Enacted to combat privacy intrusions into traditional telephony, plaintiffs have converted CIPA into a vehicle for "an onslaught of trivial demand letters and litigation." *See* Letter from Jordan Crenshaw, Senior Vice President, U.S. Chamber of Commerce to Assembly Privacy and Consumer Protection Committee, https://tinyurl.com/hxk2sn34 (Aug. 12, 2025).

Companies of all sizes and industries across the country face rising threats of CIPA litigation. Just ask the owner of California-based Elk Grove Plumbing and

Heating, who told The Sacramento Bee that she "had no idea" that her business could be "sued for wiretapping" by someone "whose name she didn't recognize." Kate Wolffe, *As Businesses Get Sued for Wiretapping, California Weighs Changes to Privacy Law*, The Sacramento Bee, https://tinyurl.com/bdeet5y3 (May 14, 2026). "We are not wiretappers," the owner explained. *Ibid.* "We are just plumbers." *Ibid.*

As one federal court recently observed: "The state of affairs with CIPA is untenable." *Doe v. Eating Recovery Ctr. LLC*, 806 F. Supp. 3d 1109, 1112 (N.D. Cal. 2025). Plaintiffs' lawyers continue to try and cram "new technologies" into "CIPA's … obtuse language," and legitimate "companies have no way of telling whether their online business activities will subject them to liability." *Ibid.* And that is not some esoteric regulatory-compliance question. "CIPA imposes criminal liability and punitive civil penalties." *Ibid.* Punishments for violating the statute can be ruinous.

While the situation is already bad, allowing Plaintiffs to reach IP addresses would make it much worse. The district court candidly acknowledged "that disclosing an IP address is a basic function of internet use." ER-12. Indeed, the Internet simply could not work without the disclosure and transmission of IP addresses. Every Internet-connected computer or server has an IP address. *Forrester*, 512 F.3d at 510 n.5; *see Beginner's Guide to Internet Protocol (IP) Addresses*, ICANN, https://tinyurl.com/c5wpphp3 (2011) ("*ICANN IP Guide*").

And those IP addresses are what enable the "transfer of data between two connected devices" such that they can "talk to each other." *What Is an IP Address? How Does It Work?*, Fortinet, https://tinyurl.com/5dndju7w (last visited June 4, 2026).

Thus, if a plaintiff has standing and a cause of action to sue for catastrophic damages for the "collection and transmission" of IP addresses, ER-12, he would have standing to challenge the basic functionality of the Internet. For example, plaintiffs could seek to extend liability to commonplace activities such as sending emails, visiting websites, or joining video conferences because, in all of these instances, a "computer sends data packets to the IP address of the other end of the connection and receives packets destined for its own IP address." *ICANN IP Guide* at 4. Indeed, as explained, this Court's *own website* collects IP addresses and would be an illegal pen register under Plaintiffs' theory. Absent the collection and transmission of "IP addresses, we would have to copy data from device to device manually, using CDs, DVDs, hard disks or flash storage, such as a USB drive." *Ibid.* In other words, Plaintiffs' legal theory would call into question core features of the modern Internet.

It is no answer, as the district court seemed to think, that these particular plaintiffs challenge the "alleged transmission of the IP address to others." ER-12. For one, as already explained, the transmission of IP addresses—just like collection—is required to make the Internet function. But, more fundamentally,

there is no reason to think the next plaintiff will challenge the exact same activity as the plaintiffs in this case. Once Pandora's box is open, it cannot be closed. If the collection and/or transmission of an IP address is an Article III injury, the basic infrastructure that makes the Internet work will be in the crosshairs of every plaintiff's lawyer in California.

Nor is there any comfort in Plaintiffs' allegation that CoStar shared their IP addresses to "underpin[ ] targeted advertising." ER-12. Again, Plaintiffs offer no limiting principle that would constrain future plaintiffs to those facts. And it is hard to imagine one without courts engaging in policy-laden decisions to authorize favored uses of IP addresses and de-authorize disfavored ones. This Court should decline the invitation to depart down that path to "freewheeling judicial policymaking" over the Internet. *Pereida v. Wilkinson*, 592 U.S. 224, 242 (2021).

Moreover, depriving Californians of effective advertising is a further reason to *reject* Plaintiffs' legal theory. Website technologies that promote effective advertising propel businesses' success in today's e-commerce landscape and enhance consumers' online browsing and shopping experiences. More than two-thirds of businesses have a website, and over a quarter of business activity is conducted entirely online. *See* Katherine Haan & Rachel Williams, *Top Website Statistics For 2025*, Forbes (May 1, 2026), https://tinyurl.com/yx4c5rje (citations

omitted). The Internet is critical in today's economy, because "ease and convenience of online transactions have made it a popular choice among consumers." *Ibid.*

In this Internet-driven marketplace, businesses with websites must maintain an effective online presence that allows them to meet consumer needs. By "[g]athering and analyzing metrics and data on how people use" websites, the U.S. General Services Administration has explained, businesses can "make customer-focused improvements." U.S. Gen. Servs. Admin., *An Introduction to Analytics*, https://tinyurl.com/mrysxsd6 (last visited June 4, 2026). And according to the Interactive Advertising Bureau ("IAB"), 71 percent of consumers "[p]refer ads tailored to their interests and shopping habits." Kristina Sruoginis, *The Value of Targeted Advertising to Consumers*, IAB, at 3, https://tinyurl.com/mrycpekn (last visited June 4, 2026). Plaintiffs' legal theory thus threatens today's e-commerce-driven ecosystem and consumers' ability to benefit from effective advertising.

This Court should reject legal theories that would threaten core Internet functionality, undermine effective advertising, and render every California business a defendant-in-waiting.

CONCLUSION

In light of the foregoing, this Court should reverse.

Respectfully Submitted,

/s/ Megan L. Brown

Jonathan D. Urick
Mariel A. Brookins
U.S. CHAMBER LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

Megan L. Brown
Jeremy J. Broggi
Boyd Garriott
Stephanie Rigizadeh
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
(202) 719-7000
mbrown@wiley.law

Counsel for Amicus Curiae,
Chamber of Commerce
of the United States of America

June 4, 2026

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 26-1652

I am the attorney or self-represented party.

This brief contains 5,602 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated ____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Megan L. Brown **Date** 06/04/2026
*(use "*s/[typed name]*" to sign electronically-filed documents)*