B350578

IN THE CALIFORNIA COURT OF APPEAL
SECOND APPELLATE DISTRICT, DIVISION 1

VARIETY MEDIA, LLC,
Petitioner,

v.

SUPERIOR COURT OF THE STATE OF CALIFORNIA,
Respondent.

From the Superior Court for the State of California,
County of Los Angeles, Case No. 25STCV01865,
Hon. David S. Cunningham III

APPLICATION OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER VARIETY MEDIA, LLC

COVINGTON & BURLING LLP
Abby C. Wright+
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-5799
awright@cov.com

COVINGTON & BURLING LLP
*Kathryn E. Cahoy (SBN 298777)
5 Palo Alto Square
3000 El Camino Real, 10th Floor
Palo Alto, CA 94306
Telephone: (650) 632-4735
kcahoy@cov.com

COVINGTON & BURLING LLP
Deborah Malamud+
30 Hudson Yards
New York, NY 10001
Telephone: (212) 841-1253
dmalamud@cov.com

+Pro hac vice forthcoming

Attorneys for Amicus Curiae the Chamber of Commerce for the United States of America

CERTIFICATE OF INTERESTED PERSONS

This is the initial certificate of interested entities or persons under California Rules of Court, Rule 8.208, submitted on behalf of the Chamber of Commerce of the United States of America as *amicus curiae*. The undersigned certifies that no entity or person has an ownership interest of 10 percent or more in the party. The undersigned knows of no other interested entities or persons that must be listed in the Certificate.

DATE: April 8, 2026

Respectfully submitted,

By: /s/ Kathryn Cahoy
Kathryn Cahoy

Counsel for Amicus Curiae

APPLICATION OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER VARIETY MEDIA

The Chamber of Commerce of the United States of America ("Chamber") respectfully seeks leave to file a brief as *amicus curiae* in support of Petitioner Variety Media.

The Chamber 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 federal and state courts.

To that end, the Chamber regularly files *amicus curiae* briefs in cases in California courts, like this one, that raise issues of concern to the nation's business community. *See, e.g.*, *EpicentRx, Inc. v. Superior Ct.* 572 P.3d 1 (Cal. 2025); *Ramirez v. Charter Commc'ns, Inc.*, 551 P.3d 520 (Cal. 2024); *Bielski v. Coinbase, Inc.*, 87 F.4th 1003 (9th Cir. 2023); *Jane Doe No. 1 v. Uber Techs., Inc.*, 294 Cal. Rptr. 3d 664 (Cal. Ct. App. 2022).

As the nation's leading business organization, the Chamber is uniquely positioned to explain the importance of interpreting the California Invasion of Privacy Act ("CIPA"), and the pen register provisions in particular, consistent with their text, structure, and context, all of which confirm that they apply to the interception and seizure of telephonic data, not the routine collection of online

data like Internet Protocol addresses. A contrary interpretation—one expanding the scope of the pen register provisions to encompass commonplace practices involved in the operation of nearly every website accessible in California—would impose massive civil (and even criminal) liability on the business community and harm both the internet and its users.

The Chamber's members are frequent targets of class action lawsuits across the country seeking to impose liability under state data privacy laws. These members have invested substantial resources to ensure they comply with the patchwork of data privacy laws that different States have enacted, including California's Consumer Privacy Act (the "CCPA"). These businesses' compliance regimes would be upended if CIPA were interpreted to reach online data collection activity expressly permitted and regulated by the CCPA. The Chamber has a significant interest in ensuring that this Court enforces the proper understanding of CIPA and thereby maintains the regulatory balance that the Legislature has chosen and upon which businesses rely.

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 this brief. *See* Cal. Rules of Court, rule 8.200, subd. (c)(3).

CONCLUSION

The Court should grant this application and permit the Chamber to file the attached *amicus curiae* brief.

Dated: April 8, 2026

Respectfully Submitted,

/s/Kathryn Cahoy

Kathryn Cahoy (SBN 298777)
kcahoy@cov.com
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
Telephone: (650) 632-2112

Abby C. Wright+
awright@cov.com
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-5799

Deborah Malamud+
dmalamud@cov.com
COVINGTON & BURLING LLP
30 Hudson Yards
New York, NY 10001
Telephone: (212) 841-1253

+*Pro hac vice forthcoming*

Counsel for Amicus Curiae

B350578

IN THE CALIFORNIA COURT OF APPEAL
SECOND APPELLATE DISTRICT, DIVISION 1

VARIETY MEDIA, LLC,
Petitioner,

v.

SUPERIOR COURT OF THE STATE OF CALIFORNIA,
Respondent.

From the Superior Court for the State of California,
County of Los Angeles, Case No. 25STCV01865,
Hon. David S. Cunningham III

[PROPOSED] BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER VARIETY MEDIA, LLC

COVINGTON & BURLING LLP
Abby C. Wright+
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-5799
awright@cov.com

COVINGTON & BURLING LLP
*Kathryn E. Cahoy (SBN 298777)
5 Palo Alto Square
3000 El Camino Real, 10th Floor
Palo Alto, CA 94306
Telephone: (650) 632-4735
kcahoy@cov.com

COVINGTON & BURLING LLP
Deborah Malamud+
30 Hudson Yards
New York, NY 10001
Telephone: (212) 841-1253
dmalamud@cov.com

+Pro hac vice forthcoming

Attorneys for Amicus Curiae the Chamber of Commerce for the United States of America

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

INTRODUCTION AND SUMMARY OF ARGUMENT

In 2018, the Legislature enacted the California Consumer Privacy Act (the "CCPA"), Cal. Civ. Code § 1798.100 *et seq*. That law—billed as the nation's first comprehensive privacy statute—expressly regulates data that websites collect from users. The CCPA broadly permits online data collection, including of Internet Protocol ("IP") addresses (unique identifiers for each device accessing the internet), while requiring websites to disclose their data collection practices and to offer users an opportunity to opt out of the sale or sharing of their data for certain advertising purposes. To enforce that scheme, the CCPA generally relies on the Attorney General and the California Privacy Protection Agency—not criminal penalties or private lawsuits by users.

The CCPA applies broadly, not only to members of the Chamber of Commerce of the United States (the "Chamber"), but to countless other businesses, non-profit organizations, and governmental entities that operate websites central to their missions. To properly route digital information on the interconnected networks that make up the internet, these website operators routinely gather basic information about visitors to their sites, including the IP addresses of devices accessing those sites and certain technical information about those devices (metadata). This data collection enables websites to load properly, ensures content is accessible to all users, helps to debug errors, prevents fraud by identifying suspicious activity, and thwarts cyberattacks.

Plaintiffs here, however, offer a legal theory that would render the CCPA's express regulation of the collection and use of this data essentially meaningless. They contend that a *different*

set of statutory provisions—the "pen register" provisions the Legislature added to the California Invasion of Privacy Act ("CIPA") in 2015—*bans* the vast majority of businesses operating websites from collecting IP addresses; makes violations punishable by *criminal* penalties; and authorizes private plaintiffs to seek rapidly escalating civil penalties of $5,000 *per violation*. *See* Cal. Penal Code § 638.51 (criminal penalties); *id.* § 637.2 (civil penalties). That theory is so sweeping that it would render nearly every website with users in California (including the websites for the Attorney General, the California Privacy Protection Agency, and this Court) in violation of a criminal law just for collecting data necessary for the internet to function. And Plaintiffs are not alone in pursuing this theory: CIPA's wiretapping provisions have spawned dozens of similar lawsuits saturating dockets in both state and federal courts in California.

CIPA's pen register provisions do nothing of the kind: their text, structure, and context confirm that they focus on the interception and seizure of *telephonic* data and do not apply to the collection of online data like IP addresses. Unlike the CCPA, CIPA's pen register provisions make no mention whatsoever of IP addresses specifically or online data generally, and certain provisions presume that a particular "telephone line" and "number" is being tapped. Moreover, even if CIPA could be read as Plaintiffs construe it, the clear conflict that would result between the CCPA's express, but calibrated regulation of online data collection and CIPA's silent, but blunderbuss regulation of the

same should be resolved in favor of the more specific, later-enacted law: the CCPA.

The consequences of adopting Plaintiffs' interpretation would be staggering. Data analytics tools that collect and interpret information about user behavior, website operations, and performance are ubiquitous, and they serve critical functions. Holding their use to be unlawful under CIPA would thus result in enormous liability for the Chamber's members, along with other businesses and organizations. And there would be no concomitant benefit to users; indeed, it would degrade users' internet experience and make it harder for website operators to keep users safe and protected online.

Common sense underscores what the statutory text and practical realities make clear: the Legislature did not silently outlaw routine online data collection practices, foisting astronomical liability on website operators of all sizes and stripes, when it enacted a narrow, telephone-focused amendment to CIPA in 2015. This Court should grant immediate review and provide much-needed guidance confirming that CIPA does not reach the conduct challenged here.

ARGUMENT

I. CIPA Does Not Apply to Collection of IP Addresses and Similar Data by Standard Analytics Tools.

As several California courts have concluded,[1] the text, structure, and context of CIPA's pen register provisions make

[1] *See, e.g.*, *Sanchez v. Cars.com Inc.*, 2025 WL 487194, at *3 (Cal. Super. Ct. Jan. 27, 2025) (holding that CIPA does not extend to "internet communications"); *Casillas v. Transitions Optical, Inc.*,

plain that it is narrowly targeted at the interception and seizure of telephone signaling information, not collection of online data like IP addresses. And the subsequent enactment of the CCPA, a comprehensive internet-focused privacy statute, eliminates any potential doubt: the CCPA expressly permits precisely the collection of IP addresses and similar data that Plaintiffs contend CIPA silently prohibits and penalizes. The best reading of CIPA is therefore that it does not regulate the routine collection of IP addresses and similar data on which Plaintiffs' claims here are based.

A. CIPA's Text, Structure, and Context Reflect a Focus on Interception and Seizure of Telephone Signaling Data, Not Routine Online Data Collection.

The relevant provisions of CIPA generally prohibit the installation and use of a "pen register" or "trap and trace device," Cal. Penal Code § 638.51(a), on pain of both criminal penalties, *id.* § 638.51(c), and private lawsuits (like this one) brought by "[a]ny person injured" for statutory damages of $5,000 per violation (or three times actual damages), *id.* § 637.2(a).

The statutory definitions of the terms "pen register" and "trap and trace device," are the starting points of the analysis. Rather than use a generic statutory term like "prohibited data

---

2024 WL 4873370, at *2 (Cal. Super. Ct. Sept. 9, 2024) (holding that CIPA "does not address the privacy rights of internet users"); *Rodriguez v. Ink Am. Int'l Grp. LLC*, 2025 WL 4034985, at *4 (Cal. Super. Ct. Dec. 10, 2025) (holding that CIPA's pen register provision "indicates a deliberate choice not to sweep ordinary website analytics within CIPA's pen register and trap and trace provisions").

collection device," the Legislature built CIPA's pen register provisions around two preexisting terms—"pen register" and "trap and trace device"—ordinarily used to refer to real, physical devices that capture telephone data.

The statute defines a "pen register" to include "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). That statutory definition tracks ordinary meaning, under which a pen register generally refers to "a device that registers the numbers dialed from a telephone." Merriam-Webster, *pen register*, https://www.merriam-webster.com/legal/pen%20register (last visited Mar. 31, 2026); *see also, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 736 n.1 (1979) ("pen register" is a "device that records the numbers dialed on a telephone").

The term "trap and trace device" is defined as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code 638.50(c). In ordinary parlance, a trap and trace device captures the originating number of an incoming call. *See, e.g.*, *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1112 (9th Cir. 2005) (referring to use of "trap-and-trace-devices" to "record[] the incoming calls to … telephones"); *United States v. Carneiro*, 861 F.2d 1171, 1173 n.2

(9th Cir. 1988) ("The trap and trace device records the originating telephone numbers of incoming telephone calls"). These devices are tools "available to law enforcement … to record all outgoing numbers from a particular telephone line," and "to record what numbers have called a specific telephone line." Assemb. Floor Analysis, Assemb. B. 929, 2015–2016 Reg. Sess. (Cal. July 8, 2015), https://www.leginfo.ca.gov/pub/15-16/bill/asm/ab_0901-0950/ab_929_cfa_20150708_162802_asm_floor.html.

The Legislature's use of these terms, along with their statutory definitions, provides a strong initial signal that the statute's focus is telephone data collection and that it does not reach the routine collection of IP addresses and other similar data by the millions of websites accessible in California.

Context confirms that reading. Statutory language must be interpreted not "in isolation, but in the context of the statutory framework as a whole in order to determine its scope and purpose and to harmonize the various parts of the enactment." *Brown v. City of Inglewood*, 570 P.3d 885, 890 (Cal. 2025) (internal quotation marks and citation omitted); *accord, e.g.*, *Doe v. Kachru*, 338 Cal. Rptr. 3d 1, 17 (Cal. Ct. App. 2025) (cautioning against "lift[ing] selected words out of a statute and examin[ing] them sans the statutory framework of which they are a part").

Read as a harmonious whole, the proper interpretation of CIPA's pen register provisions is clear: the provisions target the interception and seizure of telephone data, not routine collection of IP addresses. *See Rodriguez v. Ink Am. Int'l Grp. LLC*, 2025 WL 4034985, at *3 (Cal. Super. Ct. Dec. 10, 2025) (contrasting the

federal Pen Register Act scheme and concluding that "CIPA's history and structure represents a telephonic limitation"). The rest of the statutory scheme confirms this. Absent from CIPA's pen register provisions—adopted in 2015, well after the internet became part of everyday life—is *any* express reference to IP addresses specifically, or to online data (or the internet) generally. By contrast, CIPA *does* expressly refer to collection of telephone data.

Indeed, CIPA's provisions do not make sense if applied to anything else. CIPA's operative prohibition provides that "a person may not install or use a pen register or a trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53." Cal. Penal Code § 638.51(a). And Section 638.52(d)(3) requires that the magistrate's order granting an approval request "shall specify … [t]he *number* and, if known, *physical location of the telephone line* to which the pen register or trap and trace device is to be *attached*" (emphasis added); *see also id.* § 638.53(a)(1) (authorizing oral approval in emergency situations subject to requirements of section 638.52). A magistrate cannot comply with that mandatory command if the application is not for the collection of telephone data. Likewise, Section 638.52(c) provides that an approved application does not authorize collection of information "that may disclose the physical location of the subscriber, except to the extent that the location may be determined from the *telephone number*" (emphasis added). And other aspects of the approval provisions similarly presume the existence of a relevant telephone "number" and "line." *See id.* § 638.52(g) (barring "the person

owning or leasing *the line to which the pen register or trap and trace device is attached*" from "disclos[ing] [its] existence" (emphasis added)).

Because these provisions presume a telephone line is being tapped, and courts must consider a provision's "language in its broader statutory context and, where possible, harmonize that language with related provisions by interpreting them in a consistent fashion," *ZB, N.A. v. Superior Ct.*, 448 P.3d 239, 246 (Cal. 2019) (internal quotation marks and citation omitted), Plaintiffs' reading of CIPA's operative prohibition must be rejected. Applying that prohibition to online data analytics tools assumes that the prohibition in section 638.51(a) draws no distinction between telephone and online data, even though the approval process applies only to telephone data.

To hold that CIPA's pen register provisions cover collection of routine data like users' IP addresses would also defy the "common sense" that courts must apply when interpreting a statute. *Gattuso v. Harte-Hanks Shoppers, Inc.*, 169 P.3d 889, 897 (Cal. 2007); *accord, e.g.*, *People v. Venice Suites, LLC*, 286 Cal. Rptr. 3d 598, 607 (Cal. Ct. App. 2021). For a run-of-the-mill website—whether a business, a non-profit entity, or a governmental entity—Plaintiffs' interpretation could be read to *always* criminalize (and subject to severe civil penalties and private litigation) collection of IP addresses and similar data, regardless of user consent. That is because, as Variety Media explains, only "peace officers" may seek court approval, Cal. Penal Code §§ 638.52(a), 638.53(a), and some courts have concluded that

many (perhaps most) websites are not "provider[s] of electronic or wire communication services" who may obtain consent without court approval, Pet. 50–51 (citing *Mirmalek v. Los Angeles Times*, 2024 WL 5102709, at *5 (N.D. Cal. Dec. 12, 2024)). As the Chamber explains below, *see infra* pp. 19–21, and as Variety Media has explained in its petition, *see* Pet. 18–19, IP address collection is a basic feature of website operation. One would therefore not expect the Legislature to regulate collection of IP addresses and similar data with a shotgun approach.

In sum, as Plaintiffs would have it, in 2015—well into the internet age—the Legislature enacted a statute that criminalized the collection of both telephone and online data (regardless of user consent, in the mine run of cases) yet created a court approval process that functions only for telephonic data sought by law enforcement. And it did all of this without mentioning the internet, either in legislative debates, as Variety Media explains, *see* Pet. 56–57, or, more importantly, in the statutory text. Plaintiffs' breathtaking position defies both logic and bedrock interpretive principles: "The Legislature," after all, "does not … hide elephants in mouseholes." *Mendoza v. Fonseca McElroy Grinding Co., Inc.*, 492 P.3d 993, 1005 (Cal. 2021) (internal quotation marks and citation omitted); *see also Van Buren v. United States*, 593 U.S. 374, 393 (2021) (rejecting interpretation of Computer Fraud and Abuse Act that "would attach criminal penalties to a breathtaking amount of commonplace computer activity"). The "unreasonable, impractical, or arbitrary results" to which Plaintiffs' reading would lead provide reason enough to avoid it. *Poole v. Orange Cnty. Fire*

Auth., 354 P.3d 346, 350 (Cal. 2015) (internal quotation marks and citation omitted); *see also City of Los Angeles v. PricewaterhouseCoopers, LLP*, 553 P.3d 1194, 1205 (Cal. 2024) (courts must "avoid … interpretation[s] that would lead to absurd consequences") (internal quotation marks and citation omitted).

The "unreasonable" results of Plaintiffs' interpretation are underscored even further by a focus on the language of the prohibition, which under Plaintiffs' reading would mean "a person may not *install* or *use*" a pen register even on their own line. Cal. Penal Code § 638.51. A broad reading of the CIPA pen register provisions thus leads to the result that a person using or installing a caller ID display on his or her own telephone line would be violating CIPA's pen register ban—and committing a crime—every time the device captures a calling number or if the person disclosed the captured numbers to a third party. And even a web-based email client that captures and displays senders' email addresses would be prohibited (criminally) by CIPA. But, as courts interpreting pen-register and trap and trace laws akin to CIPA have recognized, these statutes were "designed to protect telephone users from unauthorized *third-party* or governmental intrusions," not to "protect telephone users from one another." *Wis. Pro. Police Ass'n v. Pub. Serv. Comm'n*, 555 N.W.2d 179, 188 (Wis. Ct. App. 1996) (interpreting federal Pen Register Act) (emphasis added); *see also S. Bell Tel. & Tel. Co. v. Hamm*, 409 S.E.2d 775, 778 (S.C. 1991) (similar holding under state law).

B. Applying CIPA's Pen Register Provisions to Online Data Collection Is Irreconcilable with the CCPA.

The enactment of the CCPA just three years after CIPA forecloses any argument that CIPA applies to collection of IP addresses and similar data. Reading CIPA as Plaintiffs do brings the two laws into irreconcilable conflict—one that must be resolved in favor of the CCPA, the later-enacted law and the only one that specifically and expressly regulates IP address collection.

Unlike CIPA, the CCPA expressly and unambiguously addresses collection of online data, including "online identifier[s], "Internet Protocol address[es]," "Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement," and "geolocation data." Cal. Civ. Code § 1798.140(v)(1)(A), (F), (G) (definition of "personal information"). And it regulates that collection in a calibrated way. Rather than ban (much less criminalize) data collection across the board, the CCPA generally permits collection of the kind at issue here, provided it is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." *Id.* § 1798.100(c). The CCPA protects user privacy principally by requiring that businesses collecting data *disclose* their collection practices to users, *see id.* § 1798.110, and provide users an opportunity to opt-out of the *sale* or *sharing* of the data collected for certain advertising purposes, *see id.* § 1798.120. The CCPA thus attempts to safeguard user privacy in a way that

accounts for both user choice and the need for businesses and other organizations to collect online data for their websites to function and their operations to succeed, which in turn benefits the users of those websites.

CCPA's remedial scheme is similarly measured: it does not provide for criminal penalties or (with one exception not applicable here) a private right of action, but rather relies on administrative enforcement by the California Privacy Protection Agency (which may impose administrative fines of $2,500 per violation or $7,500 per intentional violation or violation involving the personal information of minors under 16 years of age, *id.* § 1798.155(a)) and the Attorney General (who may pursue the same penalties in civil actions, *id.* § 1798.199.90(a)).[2]

Plaintiffs' reading of CIPA's pen register provisions would render the CCPA a dead letter as applied to online data collection. Although the CCPA broadly permits online data collection, Plaintiffs contend that CIPA broadly bans it, perhaps without even a consent exception for most websites. *See supra* pp. 8–9. Although the CCPA mandates disclosure of data collection practices and provides users with the right to opt out of the sale and sharing of data collected for certain advertising purposes, Plaintiffs say CIPA does not permit the collection in the first place, rendering those provisions utterly meaningless. And although the CCPA opts for an administrative enforcement regime—foregoing both criminal penalties and $5,000-a-violation civil lawsuits—Plaintiffs insist

[2] The CCPA authorizes private lawsuits only regarding certain security breach-related violations. *See* Cal. Civ. Code § 1798.150(a)(1), (a)(1)(A), (c).

CIPA authorizes both as remedies for routine online data collection practices.

Given this square conflict, only one of these two statutes can possibly apply to collection of online data like IP addresses. And it is clear which one: the CCPA. For one thing, the CCPA itself commands that "[w]herever possible, law relating to consumers' personal information should be construed to harmonize" with its provisions, not the other way around. Cal. Civ. Code § 1798.175. For another, the canons of interpretation courts employ to decide which of two conflicting statutes governs—that "more specific provisions take precedence over more general ones," *PricewaterhouseCoopers,* 553 P.3d at 1208 (internal quotation marks and citation omitted), and that "later enactments supersede earlier ones," *Lopez v. Sony Elecs., Inc.*, 420 P.3d 767, 771 (Cal. 2018) (internal quotation marks and citation omitted)—both favor CCPA too.

Finally, as explained, courts must "apply common sense to the language at hand" when interpreting statutes, *Gattuso*, 169 P.3d at 897, and "avoid … interpretation[s] that would lead to absurd consequences," *PricewaterhouseCoopers*, 553 P.3d at 1205 (internal quotation marks and citation omitted). Common sense dictates that the Legislature did not intend for its landmark comprehensive privacy law to be rendered all but ineffectual as to online data collection by another law, enacted just three years earlier, focused on telephonic data collection; that result would be absurd. The far more sensible inference is that CIPA never applied to collection of online data like IP addresses to begin with. *See*

supra pp. 4–10; *see also Santa Clarita Org. for Plan. & the Env't v. Abercrombie*, 192 Cal. Rptr. 3d 469, 483 (Cal. Ct. App. 2015), *as modified* (Sept. 22, 2015).[3]

As a final matter, if any ambiguity remains, it should be resolved against extending CIPA to collection of online data like IP addresses. CIPA's substantive prohibition on the use of pen registers and trap and trace devices—a prohibition housed in the Penal Code—is enforceable by criminal penalties in addition to civil lawsuits. *See* Cal. Penal Code § 638.51(c). And under the rule of lenity, any ambiguity in a statute imposing criminal liability not resolved by the usual tools of interpretation must be resolved by "giving the defendant the benefit of every reasonable doubt on questions of interpretation." *People v. Reynoza*, 546 P.3d 564, 583 (Cal. 2024) (internal quotation marks and citation omitted). That principle applies even where, as here, the statute is invoked in a civil posture. *See Harrott v. Cnty. of Kings*, 25 P.3d 649, 659 (Cal. 2001).[4] To the extent, therefore, that any doubt remains about the

[3] Plaintiffs' view of CIPA would also raise conflicts with new privacy laws. Late last year, Governor Newsom signed into law Assembly Bills 45 and 566, building on existing California laws like the Confidentiality of Medical Information Act that seek to protect individuals who receive certain healthcare services. *See* Assemb. B. 566, 2025–26 Reg. Sess. (Cal. 2025) (California Consumer Privacy Act of 2018: opt-out preference signal) (signed by Governor Newsom Oct. 8, 2025); Assemb. B. 45, 2025–26 Reg. Sess (Cal. 2025) (Privacy: health data) (signed by Governor Newsom Sept. 26, 2025). These new laws, like the CCPA, squarely address websites and provide users with a simple mechanism to communicate when they do not wish to sell or share their personal information for certain purposes.

[4] Under applicable precedent of the California Supreme Court, CIPA's legislative history commands the same result. *See, e.g.*, *Dep't of Corr. & Rehab. v. Workers' Comp. Appeals Bd.*, 563 P.3d

proper interpretation of CIPA, the rule of lenity demands the Court reject Plaintiffs' boundless reading. As explained above, that interpretation would render most website operators criminal offenders for engaging in routine collection of essential online data even though the Legislature did *not* take that step when it expressly regulated online data collection in the CCPA. *See Vita v. New England Baptist Hosp.*, 494 Mass. 824, 826-27 (2024) (applying the rule of lenity to hold that Massachusetts' wiretap act did not apply to "the tracking of a person's browsing of, and interaction with, published information on websites").

II. The Court Should Provide Much-Needed Certainty and Hold That Routine Collection of IP Addresses Does Not Result in Liability Under CIPA.

Web analytics tools—including the tools at issue here that collect basic online data like IP addresses—are ubiquitous on the internet. They are also crucial to the smooth functioning of websites operated by nearly every business, non-profit organization, governmental entity, religious organization, and school. Website operators use these essential tools both to keep their websites running (by identifying errors, detecting fraud, and the like) and to keep their businesses competitive (by, *e.g.*, identifying customer demographics and trends in consumer demand). Large businesses sometimes can develop these tools in-house, Kirti Saraswat, *Data-Driven Futures: How U.S. Enterprises*

1099, 1103 (Cal. 2025) ("If … the text is ambiguous, we may consult extrinsic sources, including the legislative history"). As Variety Media explains, CIPA's legislative history—like its text, structure, and context—reflects a focus on telephone signaling, not online data.

are Harnessing Analytics and AI for Competitive Edge, Ken Research (Sept. 9, 2025), https://www.kenresearch.com/articles/us-enterprise-machine-learning-adoption-strategy, but most businesses, including small and medium enterprises ("SME"), lack in-house engineering resources and thus depend on third-party tools, *see* Off. of Advocacy, U.S. Small Bus. Admin., *U.S. SME Access and Use of Digital Tools* 6 (Jan. 2023), https://www.trade.gov/sites/default/files/2023-06/SME_Digital_Tools.pdf.

If Plaintiffs' understanding of CIPA is adopted, the Chamber's members, along with millions of other businesses and organizations large and small, thus face a no-win situation: stop relying on the CCPA's disclosure and opt-out scheme and therefore stop using commonplace online data collection tools crucial to their website's functioning, or risk an extortionate lawsuit under CIPA seeking $5,000 per website visit, with little choice but to settle if CIPA is held to apply. Rather than cement those threats by adopting Plaintiffs' no-limits reading, this Court should confirm the proper interpretation of CIPA set forth in Part I.

A. Collection of Routine Online Data Is a Key to Success for Businesses and Organizations.

The prevalence of online activity cannot be overstated. Metrics from recent years indicate that 27.2% of business is conducted online in the United States, 96% of surveyed non-profit organizations held at least one fundraiser online in 2023, and nearly all surveyed local government officials (98%) report having a department or government-wide website to share information with citizens. IBISWorld, *Percentage of Business Conducted Online* (Aug. 18, 2025), https://www.ibisworld.com/united-states/

bed/percentage-of-business-conducted-online/88090/; OneCause, *The 2024 Fundraising Outlook Report: Strategic Reflection, Proactive Planning*, https://www.onecause.com/blog/2024-fundraising-outlook-report/; CivicPulse, *Web Accessibility in Local Government: Priorities, Progress, and Barriers* (March 17, 2025), https://www.civicpulse.org/research/technology-and-innovation/web-accessibility-local-government-survey. Reflecting this reality, "10% of total U.S. economic output" is driven by the digital economy. U.S. Chamber of Com., *The Digital Trade Revolution: How U.S. Workers and Companies Benefit From Digital Trade* 6 (2024), https://tradepartnership.com/wp-content/uploads/2024/03/USCC_Digital-Trade-Report.pdf. Because so much of the marketplace and the exchange of information, both for profit and not, now takes place on the internet, fully operative websites are a key component of the success of the Chamber's members. And a crucial component of that effective functioning is proper routing of data communication between website users and website operators.

To ensure such communication, websites gather information, which includes the IP address of the device and can include metadata about the device. *See* Network Encyclopedia, *Routing (in TCP/IP Networks)* (Apr. 12, 2024), https://networkencyclopedia.com/routing/ ("Routing in computer networking is a fundamental process crucial for ensuring that data packets find their way to the correct destination across diverse and complex internetworks"). Such information is necessary for sites to load properly, render accessible content, debug errors, prevent fraud by identifying suspicious internet activity, and defend

against cyberattacks. *See* Dotcom-Monitor, *Website Monitoring by Error Type: DNS, TCP, TLS, and HTTP* (Sept. 2025), https://www.dotcom-monitor.com/blog/website-monitoring-errors-dns-tcp-tls-http/ ("When a user types your domain into a browser, the first action is a … lookup translating the domain name into an IP address that tells the browser where to connect. If this step fails, nothing else can proceed"); John Miller, Dev, *IP Address Information: Essential Knowledge for Developers Regarding Website IP Data and Its Applications* (Sept. 25, 2024), https://dev.to/johnmiller/ip-address-information-essential-knowledge-for-developers-regarding-website-ip-data-and-its-applications-1h6i (IP address "plays a crucial role in detecting and preventing security threats"). In a study of approximately 100,000 websites, researchers found that disabling analytic scripts "significantly degrades functionality on approximately two-thirds of the tested websites." Abdul Haddi Amjad, et al., *Blocking JavaScript Without Breaking the Internet: An Empirical Investigation*, *Proceedings on Privacy Enhancing Technology Symposium* 391 (2023), https://petsymposium.org/2023/files/papers/issue3/popets-2023-0087.pdf.

Absent the ability to collect IP addresses and similar information, the Chamber's members, along with other organizations, will be hindered in their efforts to ensure that website content is accessible to all users, to diagnose user problems, and to tailor content to match user preferences. The net effect will be harm to customers, clients, and citizens in the form of degraded user experiences and diminished ability to access

information, make purchases, pay bills, and engage in any number of other functions now performed online. In fact, because website operators use analytics tools and device metadata collection to help detect fraud and malicious traffic, banning such tools—in the name of protecting users' privacy—could even end up *increasing* threats to privacy. *See, e.g.,* Alexandra Roland, *How Internet Telemetry Data Becomes Threat Intelligence*, Microsoft Defender Threat Intelligence Blog (Oct. 25, 2022), https://techcommunity.microsoft.com/blog/defenderthreatintelligence/how-internet-telemetry-data-becomes-threat-intelligence/3657881; *see also* Gregory M. Lebovitz, *Network security threat detection – Comparison of analytics methods* (Sept. 16, 2021), https://cloud.google.com/blog/products/networking/when-to-use-5-telemetry-types-in-security-threat-monitoring (describing use of network metadata for network-based threat detection, including malicious traffic and attacker movement). And that is a loss to individuals and businesses alike: businesses that cannot detect fraud face financial and reputational risks, and their customers suffer.

As explained above, if CIPA's framework applies to the use of data analytics tools like those at issue here, CIPA likely provides no exception for data collection even when users consent, at least for many websites. *See supra* pp. 8–9. An incorrect interpretation of CIPA therefore would force businesses to strip from their websites functions crucial to their operation. This means that for many website operators, the *only* option for compliance would be a slower, less accessible, and less secure website. Indeed, many websites could become entirely unusable.

B. Subjecting Web Operators to CIPA's Regime Opens up Businesses and Other Organizations to Ruinous Private Party Litigation.

Recasting the widespread collection of IP addresses and similar data as violations of CIPA's pen register provisions not only has untenable consequences for website operations, but it also threatens to impose destructive, retroactive liability on businesses and other organizations, including the Chamber's members.

Given that CIPA's pen register provisions target intrusive, unauthorized telephone surveillance of the sort that warrants criminal liability, its private right of action concomitantly authorizes significant per-violation statutory damages of $5,000 per violation. *See* Cal. Penal Code § 637.2(a)(1). But damages of that magnitude rapidly reach the stratosphere when applied to repeated visits to a website, rather than isolated instances of telephone surveillance: multiplying $5,000 by the number of individual user visits to frequently visited websites will yield tabs so sky-high that businesses will have little choice but to remove technologies that benefit website users, even when the plaintiffs' claims are untethered from any meaningful injury or privacy interests. *See, e.g., Popa v. Microsoft Corp.*, 153 F.4th 784, 791 (9th Cir. 2025) (CIPA plaintiff suffered no cognizable Article III injury where she failed to allege that website collected any "embarrassing, invasive, or otherwise private information").

Unless Plaintiffs' limitless interpretation of CIPA is rejected, virtually all businesses will face these costs. In 2024 alone, there were approximately 2,500 data privacy class actions, including litigation involving web-tracking tools. *US Data Privacy*

Litigation, Iapp (Mar. 10, 2025), https://iapp.org/resources/article/us-data-privacy-litigation-series. And the burden will fall disproportionately on those businesses least able to bear it. Small businesses bear roughly 50% of nationwide litigation costs and, "in proportion to revenue earned, the costs of the lawsuit system are seven times greater for businesses making $1 million or less in annual revenue compared to businesses that make $50 million or more." Inst. L. Reform, *The U.S. Lawsuit System Costs America's Small Businesses $160 Billion* (Jan. 4, 2024), https://instituteforlegalreform.com/blog/the-us-lawsuit-system-costs-americas-small-businesses-160-billion/. And per one estimate, navigating the complex patchwork of state privacy laws costs small businesses between $20-23 billion annually in compliance costs. Daniel Castro, Luke Dascoli & Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws*, Info. Tech. & Innovation Found. 12 (Jan. 2022), https://www.congress.gov/118/meeting/house/115376/documents/HHRG-118-IF17-20230301-SD021.pdf ("[T]he costs associated with data privacy laws adversely affect small businesses, often more so than their larger counterparts, because the high costs represent a larger proportion of their revenue").

As some of the courts rejecting CIPA lawsuits have recognized, collection of online data often does not involve any actual harm to user privacy*, see, e.g.*, *Popa*, 153 F.4th at 791. That is certainly the case with respect to collection of IP addresses and other device metadata. Yet the rapid proliferation of private suits under CIPA threatens serious harm to businesses navigating the

already-complicated web of privacy laws that *do* apply to their activities, as numerous courts have recognized. *See, e.g.*, *Licea v. Hickory Farms LLC*, 2024 WL 1698147, at *4 (Cal. Super. Ct. Mar. 13, 2024) ("public policy strongly disputes" a broad interpretation of CIPA that would render "every single entity" whose website is "voluntarily visited by a potential plaintiff … a [CIPA] violator, … potentially disrupt[ing] a large swath of internet commerce"); *Rodriguez*, 2025 WL 4034985, at *4 (noting *Licea*'s rationale with regard to public policy is "persuasive" and "adopt[ing] it"). Adopting Plaintiffs' interpretation will harm not only businesses, but also consumers, who will face higher prices to address soaring litigation and compliance costs *and* be left with websites that are no more protective of privacy, just less functional, less useful, and less safe.

This Court's review of the proper scope of CIPA's pen register provisions is plainly needed. In the absence of such guidance, courts continue to reach conflicting conclusions on the basic steps websites must take to avoid liability under CIPA.[5] The result of

[5] *Compare, e.g., Deivaprakash v. Conde Nast Digital*, 798 F.Supp.3d 1100, 1104–06 (N.D. Cal. 2025) (holding that website operator's trackers were a prohibited pen register under CIPA); *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 933 (N.D. Cal. 2024) (holding that the mere collection of IP addresses constitutes a pen register), *with Sanchez*, 2025 WL 487194, at *3 (holding that CIPA does not extend to "internet communications"); *Casillas*, 2024 WL 4873370, at *2 (holding that CIPA "does not address the privacy rights of internet users"); *Rodriguez v. Ink Am. Int'l Grp. LLC,* 2025 WL 4034985, at *4 (Cal. Super. Ct. Dec. 10, 2025) (holding that CIPA's pen register provision "indicates a deliberate choice not to sweep ordinary website analytics within CIPA's pen register and trap and trace provisions"); *see also* Pet. 25 & App. A (collecting cases).

these "conflicting rulings" is that "companies have no way of telling whether their online business activities will subject them to liability." *Doe v. Eating Recovery Center LLC*, 806 F.Supp.3d 1109, 1112 (N.D. Cal. 2025). And businesses accordingly continue to face an onslaught of CIPA suits, just like this one, that shows no signs of slowing down, even when those businesses are in full compliance with the CCPA. This "state of affairs … is untenable," *id.*, especially given that the CCPA expressly *permits* what Plaintiffs say CIPA prohibits. And there are serious consequences for the courts, too: until courts reach a definitive resolution of CIPA's scope, CIPA cases will continue to flood dockets and consume valuable judicial resources relitigating the same basic question.

The Court thus should grant review and supply the guidance that the Chamber's members—along with countless other businesses, non-profit organizations, and governmental entities—require to continue to compete in the marketplace and fulfill their missions. And, in providing that guidance, the Court should take due account of the staggering consequences of adopting Plaintiffs' view that CIPA categorically bans online data collection, including routine collection of IP addresses. *See, e.g.*, *Venice Suites*, 286 Cal. Rptr. 3d at 607 (court must reach "a workable and reasonable interpretation keeping in mind the consequences that will flow"). The Court should reject an interpretation of CIPA's pen register provisions that invites repeated ruinous litigation and imposes massive deadweight costs on businesses of all sizes for the routine—and harmless—collection of IP addresses and similar data central to the operation of their websites.

CONCLUSION

For the foregoing reasons, the Petition should be granted, and a writ of mandate should issue in Petitioner Variety Media, LLC's favor.

Dated: April 8, 2026

Respectfully Submitted,

/s/Kathryn Cahoy
Kathryn Cahoy (SBN 298777)
kcahoy@cov.com
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
Telephone: (650) 632-2112

Abby C. Wright+
awright@cov.com
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-5799

Deborah Malamud+
dmalamud@cov.com
COVINGTON & BURLING LLP
30 Hudson Yards
New York, NY 10001
Telephone: (212) 841-1253

+*Pro hac vice forthcoming*

Counsel for Amicus Curiae

CERTIFICATION OF COMPLIANCE

Pursuant to California Rules of Court, rule 8.204(c), I certify that the total word count of this proposed *amicus brief*, excluding covers, table of contents, table of authorities, and certificate of compliance, is 5,785.

/s/ Kathryn Cahoy
Kathryn Cahoy

PROOF OF SERVICE

No. B350578

I am a resident of the State of California and over the age of eighteen years, and not a party to the within action. My business address is 1999 Avenue of the Stars, Suite 3500, Los Angeles, CA 90067. On April 8, 2026, I served the following document(s) described as:

APPLICATION FOR LEAVE TO FILE BRIEF OF *AMICUS CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA

[PROPOSED] BRIEF OF *AMICUS CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA

on the interested parties in this action as follows:

William Alexander Delgado
DTO Law
915 Wilshire Blvd, Ste 1950
Los Angeles, CA 90017

Joshua Wilner
Kalli Carroll Lynn
Lawrence Timothy Fisher
Bursor & Fisher, P.A.
1990 N. California Blvd, 9th Floor
Walnut Creek, CA 94596

Philip L. Fraietta
Bursor & Fisher, P.A.
50 Main St, Ste 475
White Plains, NY 10606

Max S. Roberts
Bursor & Fisher, P.A.
1330 Avenue of the Americas, 32nd Floor
New York, New York 10019

Jennifer Dale Bennett
Gupta Wessler PLLC
235 Montgomery Street, Suite 620
San Francisco, CA 94104

Stephanie Ostrowski
Gupta Wessler LLP
2001 K Street NW, Suite 850 North
Washington, DC 20006

[x] (BY TRUEFILING) By filing and serving the foregoing through Truefiling such that the document will be sent electronically to the eservice list on April 8, 2025; and

The Hon. David S. Cunningham III
Superior Court of California
Spring Street Courthouse
312 N Spring St., Dept. 011
Los Angeles, CA 90012

Court Counsel
Superior Court of Los Angeles County
111 North Hill Street, Room 546
Los Angeles, CA 90012

[x] (BY MAIL) By causing the document to be sealed in an envelope addressed to the recipient above, with postage thereon fully prepaid, and placed in the United States mail at 1999 Avenue of the Stars, Suite 3500, Los Angeles, CA 90067.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this proof of service is executed on April 8, 2026.

/s/ Denis Listengourt
Denis Listengourt