Case No. B350578

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
SECOND APPELLATE DISTRICT, DIVISION 3

VARIETY MEDIA, LLC,
Petitioner,

v.

SUPERIOR COURT OF LOS ANGELES COUNTY,
Respondent,

and,

SEAN ROSE,
Real Party in Interest.

Petition from the Superior Court of California, County of Los Angeles
No. 25STCV018565 (Hon. David S. Cunningham III)

REAL PARTY IN INTEREST'S CONSOLIDATED ANSWER TO *AMICI CURIAE* BRIEFS

STEFANIE OSTROWSKI
(SBN 344463)
GUPTA WESSLER LLP
2001 K Street NW
Suite 850 North
Washington, DC 20006
(202) 888-1741
steffi@guptawessler.com

JENNIFER D. BENNETT*
(SBN 296726)
GUPTA WESSLER LLP
235 Montgomery Street
Suite 629
San Francisco, CA 94104
(415)573-0336
jennifer@guptawessler.com

(additional counsel on inside cover)

May 21, 2026

Counsel for Real Party in Interest

LAWRENCE TIMOTHY FISHER
(SBN 191626)
JOSHUA WILNER
(SBN 353949)
KAILI CAROLL LYNN
(SBN 334933)
BURSOR & FISHER, P.A
1990 N California Blvd
9th Floor
Walnut Creek, CA 94596-3745
(925) 300-4455
ltfisher@bursor.com
jwilner@bursor.com
klynn@bursor.com

PHILIP L. FRAIETTA
(SBN 354768)
BURSOR & FISHER, P.A
50 Main St
Suite 475
White Plains, NY 10606-1979
pfraietta@bursor.com

MAX S. ROBERTS*
(SBN 363482)
BURSOR & FISHER, P.A
1330 AVENUE OF THE AMERICAS
32ND FLOOR
NEW YORK, NY 10019
mroberts@bursor.com

Counsel for Real Party in Interest

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other authorities

INTRODUCTION

In its Petition, Variety asked this Court to determine whether California's pen-register provision "appl[ies] to the internet." (Pet. at 42.) The answer is a resounding yes. The California Legislature copied—nearly word for word—the federal pen-register definition, which was drafted precisely *because* Congress wanted its definition to cover internet pen registers. When the California Legislature enacted virtually the same language in 2015, there had been over a decade and a half of federal-court decisions confirming, again and again, that the federal pen-register provision applies to the internet.

Variety's amici do not dispute any of this. Instead, they try to argue that California's definition is somehow narrower than the federal definition—despite the nearly identical text. These arguments fail.

First, amici argue that canons of construction narrow the definition's scope. None of those canons, however, can add a telephone-only limitation that the pen-register definition doesn't contain. And any canon would apply equally to the identically worded federal definition, which amici do not even attempt to argue is limited to devices installed on telephones. So amici's position would mean that applying identical canons to identical statutory text yields one result as to a California statute, but another result as to a federal statute. That's not how canons of construction work.

Second, amici argue that other provisions of California law "conflict" with the pen-register definition and thereby silently limit it. Two statutes are in conflict where one requires what another prohibits. That is not the case here. The California Legislature has enacted a number of statutes protecting consumer privacy in different ways. Nothing prevents private parties from complying with all of them.

Third, amici argue that interpreting the pen-register provision to mean what it says would "criminaliz[e] the internet" by prohibiting internet

companies from collecting metadata—such as a user's IP address—that they need to serve websites to users. But the statute does not prohibit companies from collecting information with a user's consent—and by requesting a website, a user impliedly consents to the use of their IP address to provide it. Notably, no amicus is willing to argue that the trackers at issue here—trackers that record the websites a user visits—are required for the internet to function.

When all is said and done, amici's position boils down to a policy argument. They disagree with the Legislature's decision to prohibit companies from installing trackers that provide data brokers their users' web history without consent. That's an argument for the Legislature, not the courts.

And it's an argument the Legislature is actively considering. A currently pending bill, SB 690, would amend the pen-register provision to permit companies to install pen registers that collect data in furtherance of a "commercial business purpose." Many of the entities that have filed amicus briefs in this case are simultaneously lobbying in favor of that amendment, arguing that it is necessary precisely because the pen-register statute applies to the internet. The Legislature recently put the bill on a two-year track to give itself "additional time" to address "outstanding concerns surrounding consumer privacy." But amici don't want to wait. Rather than permit the legislative process to run its course, they ask this Court to short-circuit that debate and do now what the Legislature has so far declined to do. This Court should not accede to that request. It should interpret the statute that the Legislature enacted—not the unenacted bill amici are lobbying for.

ARGUMENT

I. California's pen-register prohibition is not limited to pen registers installed on telephones.

1. In its Petition, Variety asked this Court to hold that California's pen-register definition is limited to "telephonic pen registers." (Pet. at pp. 32–33.)[1] It insisted this result follows from the "ordinary meaning" of the term "pen register," which, it said, is established by judicial "[i]nterpretations of the federal pen register statute." (Pet. at pp. 34–36.) And it argued that because the California Legislature should be "presumed to have known" the scope of the federal definition when it enacted its own pen-register provision, this Court should "presume" that the Legislature intended its definition to carry "the same meaning" as federal law. (Pet. at p. 36.)

There's just one problem for Variety. As the Return explains, federal law's definition of "pen register" is not—and never was—limited to devices installed on telephones. (See Ret. at pp. 20–22.) Prior to 2001, the federal pen-register definition—"a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached" (Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1871)—was widely interpreted to apply to the internet, despite its reference to a "telephone line." (Ret. at pp. 20–21.) And Congress amended that definition in 2001 for the specific purpose of ensuring that courts know that it applies to the internet. (Ret. at pp. 21–22). There can thus "be no doubt" that the federal pen-register definition "encompasses … communication over the

[1] Unless otherwise noted, all internal quotation marks, citations, alterations, brackets, and ellipses have been omitted from quotations throughout this brief.

internet." (*In re Application of U.S. for an Order Authorizing Use of a Pen Register* (D. Mass. 2005) 396 F.Supp.2d 45, 47.)

As Variety itself admits, after the federal definition was amended to clearly apply to the internet, California copied it. (Pet. at p. 35.) So there can "be no doubt" that California's definition applies to internet communication, too.

2. In response, no one—not Variety and not any of its amici—even tries to argue that the federal pen-register statute is limited to devices installed on telephones. By 2015, federal law had been using the term "pen register" to apply to internet surveillance for decades. (See Ret. at pp. 20–22.) Even one of Variety's amici concedes that pen registers apply to the internet. (See Asana Br. at p. 46 [recognizing that pen registers include devices that intercept internet communication such as e-mail].) Everyone has long understood that they do.

Neither does anyone dispute that—as Variety conceded in its Petition—California copied the federal definition. (See Pet. at p. 35; accord Alliance Br. at p. 24.) Enacting a provision with the same scope as federal law was the whole point. As amici (and Variety) recognize, the Legislature wanted to "harmonize state and federal law" (Alliance Br. at p. 24) by "closing th[e] gap" between them (Pet. at p. 35) so that California law enforcement would have the same surveillance powers as federal law enforcement. (See also Retail Litigation Center Br. at p. 18; Reply at p. 32–33; Ret. at pp. 45–46.) To accomplish this, it gave its pen-register definition the same scope as the federal definition. (See Ret. at pp. 54–55.)

The Legislature knew that the federal definition it was copying applied to the internet. The committee reports expressly observe that the federal definition the Legislature copied "permit[s] government officials to obtain information from computers and cell phones." (Assemb. Comm. Pub. Safety Analysis of AB 929, at p. 12 fn. 4 (Apr. 7, 2015) (Return RJN,

Exh. E.) If the Legislature had wanted to depart from that definition, it wouldn't have copied it. In fact, when it departed from federal law by requiring local law enforcement to make a showing of probable cause before installing a pen register, it said so expressly. (See Ret. at p. 46 fn. 10.) If the Legislature had intended to limit California law enforcement's authority to only a fraction of the authority available to their federal counterparts, it would have pointed that out too.

3. Faced with the reality that California copied a federal definition that everyone knew applied to the internet, Variety and its amici are left arguing that California's definition is somehow narrower than the identically worded federal one. None of their arguments persuade.

First, the Retail Litigation Center gestures towards the *noscitur a sociis* canon, arguing (at 17) that "the inclusion of terms like 'dialing'" in the statutory definition limits its application to devices installed on telephones. But it does not even attempt to argue that the identical list in federal law is so limited. So this *noscitur a sociis* argument would require the canon to operate differently when applied to a California statute than it does when applied to a federal one. It doesn't. Under California or federal law, the canon functions the same way. (Compare *People v. Prunty* (2015) 62 Cal.4th 59, 73, with *Yates v. United States* (2015) 574 U.S. 528, 543; see also *Martinez v. Cot'n Wash, Inc.* (2022) 81 Cal.App.5th 1026, 1046 [turning to federal law to aid with application of the canon].)

A proper application of the canon does not limit the terms to telephonic metadata. Variety contends that, because the terms "dialing" and "signaling" are "forms of *call* metadata," the remaining items in the list—"addressing" and "routing"—must be read to apply only to telephones. (Reply at p. 22 [emphasis added].) This argument rests on a failed premise: Nothing about the terms "dialing" or "signaling" is telephone-specific. (See *Cleveland v. Johnson* (2012) 209 Cal.App.4th 1315, 1319

[explaining that a person may access the internet by "*dialing-up* with their own computer, modem and phone line"] [emphasis added]; *People v. Nguyen* (2017) 12 Cal.App.5th 574, 584 [discussing the "Internet *signal* emanating from" a suspect's residence] [emphasis added].) And even if those terms were limited to telephonic metadata, any seeming "dissimilarities" between the terms are "less significant than their similarities." (*People ex rel. Lungren v. Superior Ct.* (1996) 14 Cal.4th 294, 307–08.) Whatever the device, all four terms refer to communication metadata.

Moreover, the point of the *noscitur a sociis* canon is to avoid an interpretation that would "make other items in the list unnecessary." (*Ibid.*) Variety insists that, even if the terms apply only to telephonic communication, the term "routing" is not duplicative of the term "dialing" because, it says, "routing" "describes the method by which the telephone service connected the call"—not simply "the numbers that a person inputs on the phone." (Reply at pp. 19–20.) But as Variety's own authority for that distinction makes clear, the numbers a caller dials "rout[e]" the call "to [its] intended destination." (See *Verizon Cal., Inc. v. Peevey* (9th Cir. 2006) 462 F.3d 1142, 1147–48 [cited by Variety in Reply at p. 19].) So a call's "routing" metadata is wholly encompassed by the call's "dialing" metadata. But that's not true of "routing" metadata on the internet. The only way to avoid superfluity, then, is to recognize that the Legislature included all four forms of metadata not to distinguish between various forms of *telephonic* metadata (because the terms don't), but to ensure—using identical words as the federal definition—that both telephone and internet communication are covered. (Cf. Ret. at p. 21 [quoting Senators explaining that the federal provision was intentionally drafted in a "technology neutral" way to codify case law holding that the provision applies "to modern communication technologies such as … the Internet"].

Amici next point out that a different, procedural provision of CIPA—section 638.52(d)—differs from federal law. (See Chamber Br. at p. 7; Retail Litigation Center Br. at p. 26; Southwestern Law Br. at p. 9; see also Reply at pp. 24–25.) That provision instructs a magistrate issuing a pen-register order to specify in the order "the number and, if known, physical location of the telephone line to which the pen register … is to be attached." (Cal. Penal Code § 638.52(d)(3).) For one, that provision has no application here: Variety never sought a court order to install its pen registers. And even if the provision did apply, courts would have no trouble complying with it. Where aspects of section 638.52(d) are not applicable, courts recognize that they simply don't need to be included in an order. (See Ret. at pp. 40–41; *Shah v. MyFitnessPal, Inc.* (N.D. Cal. Jan. 27, 2026) --- F.Supp.3d ---, 2026 WL 216334, at *8 ["[A] fair reading of Section 638.52(d) would allow an officer seeking a judicial order for an online pen register to provide the equivalent of a 'number' for the online device."].) To conclude otherwise would be to graft a requirement onto the pen-register definition that the Legislature declined to add itself. (See Cal. Penal Code § 638.52(b) [listing requirements for when a magistrate "shall" enter an order authorizing the installation and use of a pen register].)

Contrary to what amici insist, the Legislature's use of the phrase "telephone line" in a different, procedural provision of CIPA does not suggest an intent to narrow the statute's pen-register definition to devices installed on telephones. That provision is also copied from the federal pen-register statute—this time, the pre-PATRIOT Act version. (Compare Cal. Penal Code § 638.52(d), with Pub. L. No. 99-508, 100 Stat. 1869–70 § 3123(b).) And that version of the federal law, too, was interpreted to apply to the internet. (See Ret. at pp. 20–21.) So amici's argument is that, by copying a federal provision that everyone (except one judge) agreed applied to the internet and combining it with a federal definition that everyone (no

exceptions) agrees applies to the internet, the California Legislature somehow demonstrated an intent to enact a statute that applies only to telephones. That can't be right.[2]

II. There is no conflict between the pen-register provision and other California privacy laws.

Getting nowhere on the text of the pen-register provision itself, Variety's amici turn to other California statutes—many of which were never enacted—that they say silently limit the pen-register provision's scope. They do not.

First, the Alliance for Legal Fairness points (at 21–23) to never-enacted bills from 1999 and 2011, which it insists demonstrate that the Legislature did not intend for CIPA's pen-register provision to "regulate the internet." These "[u]npassed bills" have "little value" as "evidence of legislative intent." (*Carter v. California Dep't of Veterans Affs.* (2006) 38 Cal.4th 914, 927–28.) "At most," the bills "might arguably reflect the Legislature's intent in" 1999 and 2011. (*People v. Mendoza* (2000) 23 Cal.4th 896, 921.) But they provide "limited, if any, guidance even as to that intent"—let alone as to the intent

---

[2] For the first time in Reply, Variety argues (at 44) that the trackers at issue here are not pen registers because they "do not collect the *destination* of *outgoing* communications." This argument is waived twice over, as Variety never made the argument below or in its Petition. (See *People v. Superior Court* (2023) 93 Cal.App.5th 394, 405 fn. 23.) It's also wrong. A device or process qualifies as a pen register under California law if it "record[s] addressing information transmitted … in connection with the outgoing HTTP request," "regardless of whether that addressing information pertains to the sender or the recipient of the communication at issue." (*Shah v. Fandom, Inc.* (N.D. Cal. 2024) 754 F.Supp.3d 924, 929.) That's precisely what Variety's trackers do. The trackers are also trap and trace devices because, from Variety's perspective, they capture the metadata associated with "incoming" web requests. (Cal. Penal Code § 638.50(c).) As the Return explained, because any distinction between a "pen register" and a "trap and trace device" is irrelevant to this case, we use the term "pen register" to encompass both. (See Ret. at p. 19 fn. 2.)

of the different legislature that enacted the pen-register provision years later. (*Ibid.*) Courts "can rarely determine from the failure of the Legislature to pass a particular bill what the intent of the Legislature is with respect to existing law." (*Id.* at pp. 921–22; see also *California Highway Patrol v. Superior Ct.* (2006) 135 Cal.App.4th 488, 506 fn. 13 [legislative history of "unpassed legislation" has "little value as evidence of legislative intent"].)

The Alliance fares no better when it finally turns to bills that *were* enacted. These statutes protect consumer privacy in other ways—by, for example, requiring websites to disclose their data collection practices (Cal. Bus. & Prof. Code §§ 22575–22579) and by prohibiting website operators from collecting information about minors (*id.* §§ 22584–22585). The fact that the Legislature protected consumer privacy in other ways prior to its enactment of the pen-register provision is hardly a reason to narrow the pen-register provision's scope. All these statutes—enacted and unenacted—show is that the Legislature has long been concerned about consumers' data privacy. The pen-register provision is of a piece with this trend.

Second, amici (and Variety) argue that a later-enacted statute—the CCPA—somehow "conflict[s]" with the pen-register provision and thereby silently narrowed it. (See, e.g., Chamber Br. at pp. 11–12; Reply at p. 52.) There is no conflict. Both statutes protect Californians' privacy. And they do so in complementary ways.[3]

---

[3] Although Open Web asserts (at 18) that the pen-register provision also "conflicts" with the Delete Act (Cal. Civ. Code §§ 1798.99.80–88), it never says how. The statutes aren't in conflict. The Delete Act establishes reporting requirements for data brokers (*id.* § 1798.99.85) and instructs a state agency to create a tool through which consumers can request that data brokers delete their personal information (*id.* § 1798.99.86). It says nothing about *what* information data brokers may collect or *how* they may collect it—let alone whether websites can surreptitiously install pen registers on their behalf.

The CCPA is a broad-based privacy law. The statute imposes "duties" on all businesses (subject to a few exceptions) that collect any form of personal information about their consumers; it is "not limited" to businesses that collect information "over the internet." (Assembly Comm. on Priv. & Consumer Prot. Analysis of AB 375, at p. 10 (June 27, 2018) (Alliance for Legal Fairness RJN, Exh. A); see Cal. Civ. Code § 1798.140(d).) Covered businesses must "inform consumers" of the "categories of personal information" they collect, how long they will retain that information, and what it will be used for. (Cal. Civ. Code § 1798.100(a).) They must use that information only for purposes that are "reasonably necessary and proportionate" to the purposes for which the information was collected. (*Id.* § 1798.100(c).) And they must "implement reasonable security procedures" to prevent consumer information from being illegally accessed. (*Id.* § 1798.100(e).) These duties extend to information that a consumer voluntarily discloses to a business, information that a business learns about a user, and information that a business infers from a consumer's actions. (*Id.* § 1798.140(v)(1).)

The CCPA also grants corresponding "rights" to consumers. These rights include "the right to know what personal information" a business collects and "whether that information is sold"; the right to "prohibit the sale" of personal information; the right to "request deletion of" personal information; and the right to "nondiscrimination in service and price" when these rights are exercised. (*California Privacy Protection Agency v. Superior Court* (2024) 99 Cal.App.5th 705, 713; see Cal. Civ. Code §§ 1798.105, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125.) Consumers also have the right to correct inaccurate information that a business has about them. (Cal. Civ. Code § 1798.106.)

In contrast to the CCPA's broad approach, CIPA's pen-register provision is narrowly targeted. It regulates only one specific form of data

collection: nonconsensual surveillance of communication metadata by third parties. But where it applies, it packs a punch: It prohibits private parties from performing this type of surveillance, subject to a few limited exceptions, such as a user's consent. (Cal. Penal Code § 638.51(b).) This prohibition fits within the broader trend of privacy law. As the ACLU explains, the law—in California and elsewhere—has long subjected "forward-looking surveillance" to the "strictest … limits." (ACLU Br. at p. 22.) At the same time, the pen-register provision—unlike the CCPA—empowers local law enforcement to perform this type of surveillance if they satisfy the statute's procedural requirements. (Cal. Penal Code § 638.52.)

So interpreting the pen-register provision to mean what it says would not "render meaningless" or "nullify" the CCPA, as amici protest. (ACC Br. at p. 13; Alliance Br. at p. 15; see also Chamber Br. at pp. 1, 12). The pen-register provision does not "prohibit[] online data collection entirely" (Alliance Br. at 35)—it prohibits only one specific form. The CCPA regulates the rest.

That is not a conflict. Two statutes are in conflict when one requires what another prohibits. (See *State Dep't of Public Health v. Superior Ct.* (2015) 60 Cal.4th 940, 958–59 [holding that statutes conflicted where one required disclosure of information that the other prohibited disclosing].) That's not the case here: A business can comply fully with both the pen-register provision and the CCPA.

In amici's view, because the CCPA established an "opt-out" regime, the pen-register provision cannot be interpreted to require a consumer to "opt-in" to any form of data collection that is subject to the CCPA. (See, e.g., Alliance Br. at pp. 27–28; Chamber Br. at p. 11). "But the CCPA does not authorize a party to intercept communications without the communicator's knowledge or consent." (*Gilligan v. Experian Data Corp.* (N.D. Cal. Jan. 6, 2026) 2026 WL 32259, at *3.) So claiming the CCPA's "opt-out"

regime somehow conflicts with the CIPA is simply false. Anyway, amici's CCPA argument proves too much. The CCPA doesn't just regulate businesses that install trackers that send a user's metadata to third parties. It regulates businesses that collect any personal information about a consumer—including their telephone number—via any medium. (See, e.g., Cal. Civ. Code §§ 1798.100, 1798.105, 1798.106, 1798.115 [regulating businesses that collect "personal information"]; see also §§ 1798.140(v)(1)(B), 1798.80(e) [defining "personal information" to include a user's telephone number].) So if it's an irreconcilable conflict for the pen-register provision to require a user to consent before a business may collect information that would otherwise be regulated by the CCPA, why does the CCPA repeal the pen-register provision only to the extent it prohibits the collection of internet metadata—but not to the extent it prohibits the collection of telephonic metadata? Amici never say.

Amici point to other aspects of the statutory schemes that they insist demonstrate a conflict, but these arguments fare no better. The Alliance observes (at 37) that the CCPA exempts many small businesses from its requirements, whereas CIPA's pen-register provision does not. But as another amicus explains, complying with the CCPA is significantly more onerous than complying with the pen-register provision. (National Retail Federation Br. at p. 20.) The CCPA requires businesses to develop systems to process consumer requests to delete or correct consumer data. (Cal. Civ. Code §§ 1798.105, 1798.106.) They must keep track of all the information that they gather about their consumers—including information they infer from a consumer's actions—and be able to communicate that information to consumers who ask for it. (*Id.* § 1798.110.) And they must implement "reasonable security procedures" to protect that data from breaches. (*Id.* § 1798.100(e).) The Legislature recognized that these requirements would impose significant compliance costs on businesses, as amici (and Variety)

observe. (See Alliance Br. at p. 29; Reply at p. 51.) So it makes sense that the Legislature would have exempted from these requirements small businesses that may not have the resources to build out such systems. The pen-register provision does not impose any obligations on businesses to build additional website functionality—it requires only that they do not record communication metadata without consent. There was thus no need for a similar small-business carve out.

Nor do the different remedial schemes render the statutes incompatible. (See, e.g., Retail Litigation Center Br. at p. 20.) Many of the legal duties imposed by the CCPA—such as the requirement that a business provide the data it collects to a consumer who asks (Cal. Civ. Code § 1798.110)—can be violated without a consumer's privacy being infringed. A violation of the pen-register provision, on the other hand, necessarily means a consumer was surveilled without their consent. That's a serious offense that can come at great cost to a consumer.[4] And even then, the statutes subject violators to comparable civil penalties. As the Chamber recognizes (at 12), a violation of the CCPA can result in a penalty of up to $7,500 per violation—greater than the pen-register provision's civil penalty. (Compare Cal. Civ. Code § 1798.155(a), with Cal. Penal Code § 638.51(c); Cal. Penal Code § 637.2(a)(1).)

In a last-ditch effort to find some inconsistency between the statutes, Alliance (and Variety) observe that the CCPA's legislative history does not discuss the pen-register provision. (See Alliance Br. at pp. 28–29; Reply at p. 38.) For one, the CCPA was enacted after the pen-register provision, and

---

[4] The Retail Litigation Center argues (at 21) that this form of surveillance is less severe than "unauthorized telephonic surveillance." It's not clear why it thinks so. Nowadays, recording the websites an internet user visits may reveal even more about them than knowing what phone numbers they dialed. (See ACLU Br. at pp. 14–17; Ret. at p. 20.)

"post-enactment legislative history (a contradiction in terms) is not a legitimate tool of statutory interpretation." (*Niedermeier v. FCA US LLC* (2024) 15 Cal.5th 792, 816; see also *Brown v. City of Inglewood* (2025) 18 Cal.5th 33, 51 fn. 13 [recognizing that "subsequent legislative history" is afforded "little weight" in statutory interpretation].) And even if the legislative history of the CCPA were probative of legislative intent underpinning the earlier-enacted pen-register provision, that legislative silence would not demonstrate that the Legislature that enacted the pen-register provision intended for that provision to apply more narrowly than its plain text suggests. The legislative history of the CCPA fails to mention a number of statutes that impact consumer privacy. (See, e.g., Cal. Penal Code § 1546; Cal. Pub. Util. Code § 2891; Cal. Civ. Code § 56.) That does not mean the Legislature thought those provisions had no impact on internet privacy.

If anything can be discerned from the legislative silence, it cuts the other way. "Implied repeals based on silence, in either the text of the newer statute or its legislative history, are strongly disfavored." (*People v. Superior Court* (2022) 81 Cal.App.5th 851, 883.) In addition to protecting California consumers from intrusive, private surveillance, the pen-register provision simultaneously expanded the authority of California law enforcement. Had the Legislature intended the CCPA to walk either back, the Legislative history "would have at least mentioned that potentiality." (*People v. Siko* (1988) 45 Cal.3d 820, 825.) This is particularly true in light of the Legislature's explicit clarification that the CCPA was intended to "supplement existing laws" relating to consumers' personal information. (Assembly Comm. on Priv. & Consumer Prot. Analysis of AB 375, at p. 10 (June 27, 2018) (Alliance for Legal Fairness RJN, Exh. A).)

Finally, this Court need not guess how the Legislature wanted courts to interpret other privacy statutes in light of the CCPA. It provided explicit instructions. "[I]n the event of a conflict," the Legislature directed, "the

provisions of the law that afford the greatest protection for the right of privacy for consumers shall control." (Cal. Civ. Code § 1798.175.) This Court should follow that unambiguous directive. (See *Pacific Lumber Co. v. State Water Resources Control Bd.* (2006) 37 Cal.4th 921, 934 [interpreting a saving clause literally because "the Legislature meant what it said"].)[5]

III. Statutory canons of construction do not require another result.

1. Amici, like Variety, lean heavily on lenity. (See, e.g., Asana Br. at pp. 47-48; News/Media Alliance Br. at p. 19; Reply at pp. 59–60.) But as we explained in the Return (at 42), lenity applies only when a court can "do no more than guess what the legislative body intended" (*People v. Manzo* (2012) 53 Cal.4th 880, 889); the statute must contain "egregious ambiguity and uncertainty." (*People v. Nuckles* (2013) 56 Cal.4th 601, 611.) There is no ambiguity here. Nothing about the statutory definition is limited to telephones—it encompasses *any* "device or process" that collects "dialing, routing, addressing, or signaling" information, whatever the technology. (Cal. Penal Code § 638.50(b); see also Ret. at pp. 29–31, 42–43.) Congress chose this language for the express purpose of ensuring that the federal statute applied to the internet. (Ret. at pp. 21–22.) And by the time the California Legislature copied the federal definition, courts had been interpreting the federal definition to apply to the internet for nearly 15 years. (See Ret. at pp. 20–22; see also, e.g., *Riganian v. LiveRamp Holdings, Inc.* (N.D. Cal. 2025) 791 F.Supp.3d 1075, 1094 [recognizing that lenity did not limit the

[5] It's true that the CCPA instructs courts to "harmonize" laws "relating to consumers' personal information" with the CCPA. (Cal. Civ. Code § 1798.175; see Alliance Br. at p. 35; Chamber Br. at p. 13.) But "harmonization" does not authorize courts to "rewrite statutes." (*Brown, supra*, 18 Cal.5th at p. 46.) All it means is construing the statutes "so that all parts of the statutory scheme are given effect." (*Ibid.*) That is already true here.

pen-register provision's scope because the statute's express language was not "grievous[ly] ambigu[ous]"]; *Gilligan, supra,* 2026 WL 32259, at *4 [similar].)[6]

The lack of ambiguity dooms amici's constitutional avoidance arguments too.[7] (See *Dep't of Agric. Rural Dev. Rural Hous. Serv. v. Kirtz* (2024) 601 U.S. 42, 61 [recognizing that constitutional avoidance has "no application in the absence of statutory ambiguity"]; *Jennings v. Rodriguez* (2018) 583 U.S. 281, 296 [similar].) Amici nonetheless protest that the statute must be narrowed because no business could possibly expect to suffer criminal consequences for "engaging in routine collection of essential online data." (Chamber Br. at p. 15.) But the statute does not prohibit a website itself from collecting data that it needs to function. A company faces no civil liability under the statute if a user consents—including by voluntarily sending their IP address to a web server and asking the website to send them a webpage in response. (See *infra* at p. 29; Cal. Civ. Code § 3515 ["A person who consents to an act is not wronged by it."]; cf. *LoanMe, supra,* 11 Cal.5th at p. 201 [recognizing that "any perceived harshness" in the application of another CIPA provision "is lessened by the fact that a party can avoid liability under the statute by … obtaining … consent"].)

---

[6] Variety argues (at 59) that Mr. Rose carries a "double burden" under lenity—to prove that Variety's interpretation is unambiguously wrong, and Rose's interpretation unambiguously right. That's not how lenity works. "[L]enity does not apply every time there are two or more reasonable interpretations." (*Manzo*, *supra*, 53 Cal.4th at p. 889.) It functions as a "tie-breaking principle," of relevance only when two competing interpretations are in "equipoise." (*Ibid.*) As explained, the competing interpretations here are not in "equipoise." (See *Smith v. LoanMe* (2021) 11 Cal.5th 183, 202 [rejecting application of rule of lenity to another provision of the CIPA].)

[7] Any constitutional avoidance argument is forfeited, as Variety failed to raise a constitutional avoidance theory before the trial court or in its Petition. (See *supra* at p. 17 fn. 2; *New Mexico Cattle Growers' Ass'n v. United States Fish & Wildlife Serv.* (D.C. Cir. 2025) 148 F.4th 755, 767.)

More fundamentally, for a company to be criminally prosecuted under this statute, the prosecution would be required to prove "some form of guilty intent" (*In re Jorge M.* (2000) 23 Cal.4th 866, 872); the defendant "must know the facts that make his conduct illegal" (*People v. Coria* (1999) 21 Cal.4th 868, 878). Applying that "background" mens rea rule provides even more clarity to the statute in its criminal context, further demonstrating that the statute is not ambiguous at all—let alone egregiously so. (*Staples v. United States* (1994) 511 U.S. 600, 619 & fn. 17.)

This case is thus nothing like the void-for-vagueness cases on which amici rely. There is no ambiguous standard that the government is tasked with applying. (See *FCC v. Fox Television* (2012) 567 U.S. 239 [application of agency regulation was unconstitutional as applied because the agency's enforcement of a regulation that prohibited "indecent" speech did not put network on notice as to what speech fell within that category]; *Connally v. General Constr. Co.* (1926) 269 U.S. 385, 388, 394 [statute requiring companies to pay workers the "current rate of per diem wages in the locality where the work is performed" was unconstitutionally vague because it was "impossib[le] [to] ascertain[]" the required wage amount from that standard].) Nor does this case involve an "unexpected … judicial enlargement" of a penal statute. (See Southwestern Law Br. at pp. 24–25 [citing *Bouie v. City of Columbia* (1964) 378 U.S. 347; *Clark v. Brown* (9th Cir. 2006) 450 F.3d 898, 903].) Mr. Rose is simply asking this Court to interpret the definition the same way that federal courts for decades have interpreted the identical federal definition.[8]

---

[8] It's no response that the California AG has never enforced the pen-register provision on similar facts. (See Alliance Br. at pp. 25, 34; Reply at p. 12.) The Attorney General's "interpretation of a statute does not elucidate legislative intent at enactment." (*United States v. Neely* (D.C. Cir. 2024) 124 F.4th 937, 945–46.) So courts interpreting a statute must look to its "plain

2. Further afield is amici's assertion that Mr. Rose's interpretation would raise concerns under the Dormant Commerce Clause. (See Retail Litigation Center Br. at p. 29; Southwestern Law Br. at p. 31.) Even Variety does not suggest as much. The argument thus "may not be considered." (*Qaadir v. Figueroa* (2021) 67 Cal.App.5th 790, 794 fn. 1; see also *ibid.* ["We will only consider those arguments by amici curiae which are raised by the parties on appeal."]).

But in brief: Nothing about the pen-register provision "seeks to advantage in-state firms or disadvantage out-of-state rivals." (*Nat'l Pork Producers Council v. Ross* (2023) 598 U.S. 356, 370.) And as Southwestern Law concedes (at 38), a state law is not unconstitutional "merely because it produces effects outside the state." So amici are left arguing that the "burden imposed" on interstate commerce is so obvious from the mere existence of the statute that this Court must narrow its reach. (*Nat'l Pork Producers Council*, *supra*, 598 U.S. at 391 (Sotomayor, J. concurring).) But they offer no facts suggesting that is the case. If amici believe the pen-register provision is unconstitutional, they can challenge it. What they cannot do is offer a constitutional argument with no support under the guise of constitutional avoidance. (See *United States v. Apel* (2014) 571 U.S. 359, 372–73 ["The canon of constitutional avoidance is not a method of adjudicating constitutional questions by other means."].)

IV. Holding that the pen-register provision means what it says would not render the internet illegal.

All that is merely prologue to amici's real complaint with the pen-register provision: They think it's bad for business. Amici paint a dire picture, protesting that it would be disastrous if California law "criminalized

---

language"—"[e]ven if the government ha[s] never prosecuted someone in [the defendant's] position." (*United States v. Sorensen* (10th Cir. 2015), 801 F.3d 1217, 1228.)

the internet." (Alliance Br. at p. 18; see also, e.g., Asana Br. at p. 48.) But that's not what the statute does. The provision prohibits websites from sending their users' metadata to third parties. It does not prohibit websites themselves from collecting metadata—including IP addresses—that they need to function.

First, the statute permits businesses to use pen registers "to operate" an "electronic communication service." (Cal. Penal Code § 638.51(b)(1).) As amici emphasize, the internet requires the exchange of IP addresses to function. When a user sends a web request to a server asking for a website to load, the website can fulfill that request only if it knows the IP address the user is asking it to deliver the website to. (See Asana Br. at pp. 16–17.) So a website's *own* collection and use of such information for the purpose of operating its site is not prohibited by the statute. Mr. Rose does not challenge Variety's own collection of IP addresses to operate its website. And Variety has never argued that installing a device that surreptitiously sends a user's information to third-party data brokers is necessary for the internet to function. (See *Drummer v. CoStar Grp., Inc.* (C.D. Cal. Oct. 22, 2025) 2025 WL 3190656, at *4.)[9]

Second, as Southwestern Law School admits (at 10), the statute carves out of the definition of "pen register" any device or process used by a provider or customer of an electronic communications service for the provider's "communications services." (Cal. Penal Code § 638.50(b).) This

[9] Variety now argues (at 66–67) that its installation of third-party trackers falls within this exception. It didn't raise this defense below or in its Petition, making this argument doubly waived. (See *supra* at p. 17 fn. 2). And the company never explains how installing a tracker that tells third parties the websites a user visits is necessary for Variety to operate its website.

carve out, too, means that the statute does not prohibit websites from collecting information required for a webpage.[10]

Third, consent is a defense. (See Ret. at pp. 50-51.) Where a user sends their IP address to a web server and asks the server to send a webpage in return, the user has "manifested by his or her conduct a voluntary consent" to that server receiving their IP address for the purpose of serving them the website. (*Hill v. NCAA* (1994) 7 Cal.4th 1, 26; see also *Drummer*, *supra*, 2025 WL 3190656, at *4 ["By visiting Defendant's websites, Plaintiffs have clearly consented to disclosing their IP addresses for the purpose of loading the website, so [CIPA's pen-register prohibition] would not apply."].)[11]

The pen-register provision thus does not prohibit websites from collecting information they need to make communication over the internet possible. Amici admit as much, recognizing that a pen register is a device or process that "*intercept[s]*" communication metadata. (Chamber Br. at pp. 2, 4

---

[10] Variety argues (at 66) that this provision applies only to billing. That's not what the provision says. Section 638.50(b) excludes three use cases from the pen-register definition: use of a device or process by a "provider or customer of a[n] … electronic communication service" (1) "for billing, or recording as an incident to billing," (2) "for communications services provided by such provider," and (3) "for cost accounting or other similar purposes in the ordinary course of its business." That is the only reading of the statute that explains why the provision exempts uses by a "provider *or customer*" of an electronic communication service. Customers, after all, do not "bill" their providers.

[11] Amici point out that the statutory consent exception applies only to "providers" of an "electronic communication service." (See, e.g., Asana Br. at p. 38; Alliance Br. at p. 19). But even if the provider of a website—an "electronic communication"—isn't an electronic communication service provider, the defense of consent exists both under the statute and from principles of the common law and the maxims of jurisprudence. (See Ret. at pp. 50–51; Cal. Civ. Code § 3515 ["A person who consents to an act is not wronged by it".]; *Hill, supra,* 7 Cal.4th at p. 26 [no invasion of privacy where a person "manifested by his or her conduct a voluntary consent to the invasive actions"].)

[emphasis added]; Southwestern Law Br. at p. 29; see also *Wis. Pro. Police Ass'n v. Pub. Serv. Comm'n of Wis.* (Ct. App. 1996) 205 Wis.2d 60, 80 [recognizing that the federal pen register statute is designed to protect parties to a conversation "from unauthorized third-party or governmental intrusions"—not "from one another"].) So in the same way that a phone with caller ID is not a pen register, neither is a website that receives a user's IP address to serve them a website. (Cf. *Rodriguez v. Autotrader.com, Inc.* (C.D. Cal. 2025) 762 F.Supp.3d 921, 930 [noting that "courts have consistently found" that a phone with caller ID is not a pen register].) Amici's parade of horribles will thus not come to pass: The pen-register provision does not make it illegal to operate a website. What CIPA does prohibit is the installation of a device or process that enables *third parties* to track the websites a user visits without that user's consent.

Although amici run through a number of ways data collection facilitates the functionality of their websites, they are conspicuously silent about the surveillance at issue here. Open Web, for example, extolls the virtues of customized advertising (at 7, 9–10), but it never argues that effective advertising requires websites to tell third parties all the websites a user visits or help data brokers compile comprehensive, de-anonymized profiles. In fact, Open Web and others concede that such surveillance is unnecessary. As amici point out, many browsers permit users to disable third-party trackers altogether—including the sort of trackers at issue here. (Asana Br. at pp. 25–27; Retail Litigation Center Br. at p. 22; Open Web Br. at p. 15.) That functionality hasn't destroyed the internet. And neither would a proper interpretation of CIPA. (*Lewis v. Magnite, Inc.* (C.D. Cal. Dec. 4, 2025) 2025 WL 3687546, at *13 ["Defendant's prophecy has not come to fruition in the last few years since other courts have interpreted CIPA [to apply to the internet] as this Court does."].)

Of course, if a website deems it important for third parties to track the websites a user visits, it can obtain its users' consent. If it's true, as Open Web insists (at 7), that consumers really "want" to be surveilled in this way, websites should have no trouble getting their consent. The Alliance responds (at 38) that the pen-register provision's consent requirement is somehow too "opaque" to enable businesses to comply with it. That's hard to believe. Consent is a defense to many offenses, and neither courts nor businesses have any trouble applying it—even without specific regulatory guidance. (See, e.g., *Hill, supra,* 7 Cal.4th at p. 26; *Lee v. Ticketmaster* (9th Cir. 2020) 817 F.App'x 393, 394–95; *Smith v. Facebook, Inc.* (9th Cir. 2018) 745 F.App'x 8, 8-9.) Indeed, "[t]he acquisition of consent when visiting websites (for the collection of cookies, for example) is a regular occurrence and hardly particularly 'technologically impractical.'" (*Javier v. Assurance IQ, LLC* (N.D. Cal. 2023) 649 F.Supp.3d 891, 900.)

Finally, Open Web argues (at 16–17) that the consent requirement will disadvantage third-party companies that create the surveillance tools that violate the Act. That's not a reason to narrow the statute's scope; any law that prohibits conduct will disadvantage companies that engage in that conduct. Anyway, as Open Web itself admits (at 17), those companies can require websites that install their trackers to obtain consent before doing so—as the law requires.

V. Amici's interpretations are unworkable—and their arguments belong (and are) before the Legislature.

1. Although amici all insist that California's pen-register provision does not encompass third-party trackers that record the websites users visit, they are studiously vague about what it does mean. In fact, they offer conflicting interpretations.

Some amici echo Variety's Petition and argue that the provision does not apply to any form of communication beyond the telephone. (See,

e.g., Chamber Br. at pp. 2, 4; News/Media Alliance Br. at p. 19.) One concedes that pen registers apply to the internet—but maintains that the statute does not extend to *this* type of internet communication (Asana Br. at pp. 13, 46, 48–49). Another argues that the provision encompasses internet communication when applied to law enforcement but only telephonic communication when applied to private businesses. (Alliance Br. at pp. 42–43.) And still others provide no positive construction at all, insisting only that the installation of trackers that record the websites users visit does not qualify. (Corporate Counsel Br. at p. 3; National Retail Federation Br. at p. 11; Open Web Br. at p. 7.)

For its part, Variety continues to insist that the provision applies only to "telephonic communication," but its reply is even less clear than its Petition on the scope of its rule. (Reply at p. 17.) At times, the company seems to suggest that the statute covers only communication via telephone *calls*. (Reply at p. 26.) It never explains where this call-only rule comes from. It certainly cannot be found anywhere in the statutory text. And why would the Legislature have prohibited surveillance that collects the telephone numbers that someone calls, but not the telephone numbers they text? Variety never says.

Even more damning to its interpretation is Variety's new concession that calls placed over the internet fall within the statute's scope. (Reply at pp. 27–28.) That concession is fatal to its position, advocated for in its Petition, that the pen-register provision doesn't "apply to the internet." (Pet. at p. 42.) And once you start down this path, the "clarity" Variety promises—and that Variety's amici say they need—falls away. (Pet. at p. 27; see, e.g., National Retail Federation Br. at p. 9.) Variety says that the pen-register provision applies "regardless of the device used to make the call," so long as there is "telephonic communication." (Reply at pp. 26–28.) But if "telephonic communication" encompasses calls placed over the internet

and doesn't require a telephone, then what does Variety mean? Do calls placed on a computer count? What about calls placed on a phone or computer using an application such as Facetime or Whatsapp? Do video calls count? Does it make a difference if a caller's video camera is turned on or off during the call? What if the caller simultaneously sends written messages, while the call is ongoing? And if, as Variety now concedes, some internet communication falls within the statute's scope, how are companies supposed to know what's in and what's out?

2. At bottom, amici's "statutory" arguments are thinly veiled policy arguments. "Crafting statutes to conform with policy considerations is a job for the Legislature, not the courts." (*California Ins. Guarantee Ass'n v. Workers' Comp. Appeals Bd.* (2004) 117 Cal.App.4th 350, 362.) And the Legislature is trying to do its job. It is presently considering SB 690, which seeks to narrow the pen-register provision to permit business to collect data "in a manner consistent with a commercial business purpose." (S.B. No. 690 (2025-2026 Reg. Sess.).) That bill has been put forward by many of the amici that appeared in this case. (See Supporters of SB 690, https://perma.cc/Q2E9-DMZL; Assembly Comm. on Pub. Safety Analysis of SB 690, at pp. 19–20 (July 1, 2025) (Return RJN, Exh. A.) Notably, the bill does not suggest that the pen-register provision is limited to telephones. To the contrary, the bill's author has observed that, as presently enacted, California's pen-register provisions "include[s] programs monitoring Internet communications." (*Id.* at p. 10; see also Ret. at p. 33.) It's precisely *because* the pen-register provision applies to internet data collection that lobbyists—including amici—think the amendment is necessary. (See Assembly Comm. on Pub. Safety Analysis of SB 690, at p. 18 (July 1, 2025) (Return RJN, Exh. A) [supporters of the bill explaining that it would "clos[e] [the] … loophole" presently allowing lawsuits challenging "online [data-collection] practices"].)

The debate surrounding SB 690 raises the exact same policy arguments that amici have presented to this Court. (See, e.g., *Ibid*; Assembly Comm. on Pub. Safety Hearing on SB 690, at pp. 3, 5 (July 1, 2025) (Legal Fairness RJN, Exh. S). And the debate is ongoing. The Legislature refused to enact the bill this past session. Instead, it put the bill on a two-year track to give itself "additional time" to address "outstanding concerns surrounding consumer privacy" and to allow the Legislature to "strike the right balance" between business interests and consumer privacy. (*Id.* at p. 2.) These "competing interests" warrant thoughtful consideration—by the Legislature. (*People v. Hicks* (2019) 40 Cal.App.5th 320, 329.)

If the Legislature wants to permit companies to install trackers that permit third parties to track the websites a user visits, it can amend the pen-register provision to do so. This Court should not short-circuit that legislative debate by resolving a policy dispute that the Legislature is currently considering.

CONCLUSION

Petitioner's request for issuance of a writ of mandate should be denied.

Respectfully submitted,

/s/ Jennifer D. Bennett
JENNIFER D. BENNETT
(SBN 296726)
GUPTA WESSLER LLP
235 Montgomery Street
Suite 629
San Francisco, CA 94104
(415) 573-0336
jennifer@guptawessler.com

STEFANIE OSTROWSKI
(SBN 344463)
GUPTA WESSLER LLP

2001 K Street NW
Suite 850 North
Washington, DC 20006
(202) 888-1741
steffi@guptawessler.com

LAWRENCE TIMOTHY FISHER
(SBN 191626)
JOSHUA WILNER
(SBN 353949)
KAILI CAROLL LYNN
(SBN 334933)
BURSOR & FISHER, P.A
1990 N California Blvd
9th Floor
Walnut Creek, CA 94596-3745
(925) 300-4455
ltfisher@bursor.com
jwilner@bursor.com
klynn@bursor.com

PHILIP L. FRAIETTA
(SBN 354768)
BURSOR & FISHER, P.A
50 Main St
Suite 475
White Plains, NY 10606-1979
pfraietta@bursor.com

MAX S. ROBERTS
(SBN 363482)
BURSOR & FISHER, P.A
1330 AVENUE OF THE AMERICAS
32ND FLOOR
NEW YORK, NY 10019
mroberts@bursor.com

May 21, 2026

Counsel for Real Party in Interest

CERTIFICATE OF WORD COUNT

This answer to amicus briefs complies with the type-volume limitation of California Rules of Court rule 8.204(c)(1) because this answer to amicus briefs contains 8,011 words as counted by Microsoft Word, excluding the parts of the response exempted by the rules. The brief complies with the typeface, type-style, page alignment, spacing, and margin requirements of Rule 8.74(b) because it has been prepared in proportionally left-aligned 1.5 spaced typeface using Microsoft Word in 13-point Baskerville font.

May 21, 2026

/s/ Jennifer D. Bennett
Jennifer D. Bennett

PROOF OF SERVICE

I, Benita Kisembo, hereby certify that at the time of service, I was at least 18 years of age and not a party to this action. My business address is 2001 K Street, NW, Suite 850 North, Washington, DC 20006, and my email address used to e-serve is benita@guptawessler.com. I certify that on May 21, 2026, I served this notice on the below interested parties via the Second District Court of Appeal's TrueFiling system:

via TrueFiling:

WILLIAM ALEXANDER DELGADO
DELGADO TARANGO O'NEILL LLP (DTO LAW)
915 Wilshire Blvd, Ste 1950
Los Angeles, CA 90017-3467
wdelgado@dtolaw.com

RICHARD JAGDISHWAR MILLETT
DELGADO TARANGO O'NEILL LLP (DTO LAW)
702 Marshall St., Ste 640
Redwood City, CA 94063-1826
rmillett@dtolaw.com

Counsel for Defendant-Petitioner

via Mail:

Hon. David S. Cunningham III
Los Angeles Superior Court
Spring Street Courthouse
312 North Spring Street
Los Angeles, CA 90012
(213) 310-7011

Respondent

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: May 21, 2026

/s/Benita Kisembo
Benita Kisembo