NO. 1045905

SUPREME COURT OF THE STATE OF WASHINGTON

CARLY BAKER, JANSSEN RAMOS SAVOIE, and AMBER SHAVIES, individually and on behalf of all others similarly situated,

Plaintiffs/Petitioners,

v.

SEATTLE CHILDREN'S HOSPITAL, a Washington nonprofit corporation,

Defendant/Respondent.

AMICI CURIAE BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AND THE WASHINGTON STATE HOSPITAL ASSOCIATION IN SUPPORT OF SEATTLE CHILDREN'S HOSPITAL

COVINGTON & BURLING LLP
Ingrid L. Price (WSBA No. 56076)
Abby C. Wright+
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662 6000
iprice@cov.com
awright@cov.com
+*Pro Hac Vice Forthcoming*

COVINGTON & BURLING LLP
Kathryn E. Cahoy+
3000 El Camino Real, 10th Floor
5 Palo Alto Square
Palo Alto, CA 94306
Telephone: (650) 632-4735

Attorneys for Amici Curiae

Additional Attorney Listed Below

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

I. IDENTITY AND INTERESTS OF AMICI

The Chamber of Commerce of the United States of America ("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.

The Washington State Hospital Association ("WSHA") is a nonprofit membership organization representing all Washington's 114 hospitals and several health-related organizations. WSHA works to improve the health of the people of the state by becoming involved in all matters affecting the delivery, quality, accessibility, affordability, and continuity of health care.

II. STATEMENT OF THE CASE

Amici adopt the Statement of the Case as set forth in Seattle Children Hospital's Supplemental Brief.

III. INTRODUCTION AND SUMMARY OF ARGUMENT

In 1967, decades before the advent of the internet, the Legislature enacted the Washington Privacy Act (WPA) to prevent third-party interception of private communications between two or more people. That law forbids the interception of such conversations made through various means of communication such as the telephone, radio, or telegraph, and prohibits the opening of sealed letters or telegrams. Plaintiffs urge this Court to conclude that the WPA extends much further, silently prohibiting websites from collecting data such as clicks on the screen and search terms entered into a website's search bar.

This Court should reject Plaintiffs' reading of the WPA. Not only does that reading defy common sense, but it also

finds no refuge in the language of the statute. The WPA covers communications *between people*, not data sent by an individual to a website. And to hold otherwise would lead to absurd results and criminalize routine internet practices. Members of *amici curiae*, along with numerous other businesses, non-profit organizations, and medical providers, will suffer significant harm if Plaintiffs' theory is adopted. Subjecting organizations to both criminal liability and potentially enormous class action damages awards—based on a recently invented interpretation of a nearly 60-year-old statute—would hamstring website operators, introduce substantial compliance uncertainty, and degrade users' internet experience by inhibiting ubiquitous data analytics tools that serve critical functions, including by helping patients quickly and reliably find information about medical services.

IV. ARGUMENT

A. The WPA Does Not Apply to Automated Data Transmissions Sent to Servers.

Plaintiffs contend that the WPA, RCW 9.73.030—a 1967 statute regulating surreptitious interception and recording of private communications between people—silently imposes sweeping criminal and civil liability for using a common web "cookie" that collects certain technical data about a user's interaction with a website, *see* Brief of Respondent Seattle Children's Hospital at 3–4, *Baker v. Seattle Children's Hospital*, 35 Wn. App. 2d 1018 (2025) (No. 864611).

The WPA does nothing of the sort. Contrary to Plaintiffs' shaky theory, the Legislature did not quietly outlaw routine website data practices through a wiretapping and eavesdropping law it enacted in 1967 before the internet was used by the public. *See* Robert Kahn, *Internet*, Encyc. Britannica (Mar. 20, 2026), https://perma.cc/3GMA-26LQ.

The text and structure of the WPA confirm that it is narrowly focused on person-to-person communications, not automated data transmissions to a server generated by clicks and information entered in the search bar of a website. Nor can Plaintiffs' theory be squared with the Legislature's 2023 enactment of the My Health My Data Act, a specific consumer health data privacy law governing privacy considerations for consumer health websites. *That* law—not the WPA—represents the Legislature's internet-privacy regime.

This Court should thus decline Plaintiffs' invitation to rewrite the WPA.

1. The WPA applies only to communications between natural persons intercepted by third parties.

The WPA generally prohibits recording or intercepting "[p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more

individuals" without consent. RCW 9.73.030(1)(a). The law creates both criminal liability and a private right of action. *See* RCW 9.73.080 ("[A]ny person who violates RCW 9.73.030 is guilty of a gross misdemeanor"); RCW 9.73.060 (victims are entitled to "actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation").

As Seattle Children's Hospital (SCH) has persuasively explained, the WPA's plain text unambiguously demonstrates that it applies only where information is exchanged between two or more *people*. *See* Seattle Children's Hospital Supplemental Brief at 6–10, *Baker v. Seattle Children's Hospital*, No. 104590 (Wash. Mar. 9, 2026). Because Plaintiffs' interactions (clicks and search requests)

with SCH's website (*i.e.*, a server) did not involve such exchanges, the data from those interactions did not constitute "communication[s]" subject to the WPA. *Id*. SCH, moreover, did not eavesdrop on any communications; the clicks and words entered in the SCH website's search bar were intended for the SCH website.

2. The WPA's surrounding provisions confirm its scope is limited to person-to-person communication.

"In discerning the plain meaning of a provision," this Court "consider[s] the entire statute in which the provision is found, as well as related statutes or other provisions in the same act that disclose legislative intent." *Velazquez Framing, LLC v. Cascadia Homes, Inc.*, 2 Wn.3d 552, 555, 540 P.3d 1170 (2024) (cleaned up). The provisions surrounding the section of the WPA Plaintiffs invoke, RCW 9.73.030, further confirm that the WPA focuses on communications between natural persons. And nothing in those provisions suggests

that it was intended to be an omnibus privacy law for the internet, as Plaintiffs' theory would require.

Section 9.73.030 was enacted in 1967 as part of a suite of provisions aimed at preventing the surreptitious interception and recording of private communications between people "by telephone, telegraph, radio, or other device." RCW 9.73.030(1)(a). By 1967, nearly every household had a telephone, James Ellison, *What Were Phones Like in the 1960s: A Glimpse into the Past Communication Technology*, BlinksandButtons (June 25, 2024), https://perma.cc/P63K-X93G, and communication between persons by telegraph and radio was long-established, Clare D. McGillem, *Telegraph*, Encyc. Britannica (Feb. 6, 2026), https://perma.cc/D74G-LGCN; *A Sonic Revolution: A Brief History of Radio,* Hist. of Every Day, https://perma.cc/HU5Z-8CUG.

The WPA's additional provisions cover the remaining common forms of interpersonal communication. Section 9.73.010, for instance, makes it a misdemeanor to read, divulge, or prohibit delivery of a telegram meant for someone else. The next section applies the same rule to sealed letters. *See* RCW 9.73.020. And the subsection following the one at issue here, applies to "[p]rivate conversation." *See* RCW 9.73.030(1)(b). Each of these provisions targets a specific method of communication (in-person, telephone, telegram, etc.) *between people*. Indeed, the 1967 Legislature would no doubt have been shocked to learn it was inadvertently criminalizing collection of signals directed from remote controls to TVs or from customers to vending machines, as Plaintiffs' theory would hold.

3. Interpreting the WPA to reach routine website data practices would create considerable tension with the health data privacy regime.

That the WPA does not cover the collection of clicks and searches challenged here makes sense, given the affirmative data privacy measures the Legislature has undertaken. In 2023, the Legislature enacted the My Health My Data Act (the "MHMDA"), RCW 19.373 *et seq.*, which comprehensively regulates the collection, sharing, and sale of consumer health-related data online. Broadly applicable to "any legal entity that conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington," RCW 19.373.010(23), the MHMDA regulates all types of "consumer health data"—that is, "personal information that is . . . reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status," RCW 19.373.010(8)(a). In doing so, the Legislature struck a

deliberate balance between protecting consumer privacy and permitting routine website operations necessary to provide users with the services they request. That calibrated scheme provides concrete guidance to *amici*'s members, along with numerous health care providers, nonprofit organizations, businesses, and other organizations in Washington that operate public-facing websites.

This Court should not ignore the Legislature's specific—and more recent—treatment of data privacy on the internet in favor of Plaintiffs' blunderbuss approach, which renders certain provisions of the MHMDA superfluous. For example, even data collection necessary to provide the services a consumer seeks, which the MHMDA permits, *see* RCW 19.373.030(1)(a)(ii), (b)(ii), could be banned under the Plaintiffs' version of the WPA absent consent. Reading a statutory exception out of the MHMDA flouts the well-established rule that "[s]tatutes must be interpreted and

construed so that all the language used is given effect, with no portion rendered meaningless or superfluous." *State v. J.P.*, 149 Wn.2d 444, 450, 69 P.3d 318 (2003) (cleaned up). And it also contravenes common sense, which dictates that the "legislature does not intend to create inconsistent statutes." *Am. Legion Post No. 149 v. Dep't of Health*, 164 Wn.2d 570, 585, 192 P.3d 306 (2008). Rather than contort the WPA to cover collection of clicks and web search terms and try to reconcile that with the MHMDA, the far more sensible understanding is that the WPA never applied to online data analytics tools like third-party pixels to begin with.[1]

[1] This view is also supported by the fact that the Legislature twice attempted to pass a statutory corollary to the California Consumer Privacy Act ("CCPA"). *See* David Strauss, *Washington Privacy Act Fails*, Byte Back Law (Mar. 12, 2020), https://perma.cc/VQX2-3WUE. These attempts reflect that the 1967 WPA did not address modern data-privacy concerns, notwithstanding Plaintiffs' effort to expand its scope retroactively through judicial interpretation.

Plaintiffs' theory has another big problem: Plaintiffs urge that data collection is a basis for *criminal* liability—even though the MHMDA relies solely on civil enforcement. *See* RCW 19.373.090, 19.86. But a dramatic shift from civil to criminal liability should not be lightly embraced, especially where civil-only liability appears in the later and more detailed statute governing sensitive personal data. Because the MHMDA reflects the Legislature's deliberate decisions with respect to internet data privacy, the Court should not twist the WPA to cover the same ground.

4. The unfair and absurd results of Plaintiffs' interpretation underscore its error.

If any ambiguity remains with respect to the interpretation of "communication . . . between two or more individuals" in RCW 9.73.030(1)(a), it should be resolved against extending the scope to include routine web functions like collection of clicks and web searches. As explained, the WPA is both a civil and criminal statute. 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 in favor of the party potentially subject to criminal penalties. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004); *City of Seattle v. Winebrenner*, 167 Wn.2d 451, 462, 219 P.3d 686 (2009). Because of the WPA's criminal nature, an appellate court recently recognized the need to "consider the statutory scheme of the privacy act as a whole" and apply a "literal and strict" interpretation to the WPA. *State v. Gates*, 28 Wn. App. 2d 1301, 2023 WL 6553863, *10 (2023) (quoting *State v. Delgado*, 148 Wn.2d 723, 727, 63 P.3d 792 (2003)).

Plaintiffs' interpretation of the WPA is anything but "strict." *Delgado*, 148 Wn.2d at 737. Under Plaintiffs' theory, a hospital could be exposed to criminal liability based on the passive loading of a third-party pixel or web cookie, conduct far removed from the surreptitious interception of

interpersonal communications that is prohibited by the WPA's terms. In fact, this Court and the Legislature engage in such conduct every day by operating websites that fire analytics technology like Fathom Analytics, Google Ads, and Google Analytics. *See* Washington Courts, courts.wa.gov; Washington State Legislature, leg.wa.gov. A regime penalizing such conduct would fail to provide fair notice of what conduct is criminally proscribed, especially considering that the MHMDA provides a privacy compliance regime specifically targeted at such actions. Accordingly, to the extent that any doubt remains about the proper interpretation of "private communication . . . between two or more individuals," the rule of lenity and the requirement for "literal and strict" interpretation demand the Court reject Plaintiffs' boundless theory of "communication" in the WPA.

The absurd results canon reinforces this conclusion, as "it will not be presumed that the legislature intended absurd

results." *J.P.*, 149 Wn.2d at 450; *see also, e.g, Pub. Citizen v. United States Dep't of Just.*, 491 U.S. 440, 453-54 (1989) (rejecting an "absurd result[]" that "Congress [could not] have meant"). Under Plaintiffs' theory, any website operator—from a doctor's clinic to a news outlet to a municipal agency to *amici*'s members—would risk criminal liability for ubiquitous internet practices. That interpretation of a 1967 wiretapping and eavesdropping law is absurd, especially in light of the MHMDA.

B. Plaintiffs' Expansive Interpretation of the WPA Would Impose Significant Burdens on *Amici*'s Members and Undermine Administrability and Predictability.

A dramatic reframing of the WPA would have numerous deleterious effects including criminalizing routine website functions and exposing *amici*'s members, along with many other businesses and medical providers, to private damages actions. Plaintiffs' theory also would impose obligations that website operators would struggle to

meaningfully operationalize and would destabilize existing compliance regimes. Determinations regarding the structuring of privacy rules are best left to the Legislature. That is especially clear where, as here, the Legislature has expressly addressed a later development with more recent legislation.

This Court should therefore reject an interpretation of the WPA that would force organizations across the State—from the *amici*'s members to other businesses, non-profit organizations and medical providers—to divert resources away from essential services and mission-critical operations to comply with an untailored and inapplicable wiretapping and eavesdropping law.

1. Casting routine website interactions as "communications . . . between two or more individuals" would create unworkable compliance obligations, impose unreasonable compliance costs, and breed uncertainty.

Plaintiffs' proposed interpretation of the WPA, which purports to transform a website click on a public website into a "private communication . . . between two or more individuals," RCW 9.73.030(1)(a), would impose sweeping and unfeasible compliance burdens on *amici*'s members and other organizations.

First, hospitals, healthcare providers, nonprofit organizations, businesses, and other public-facing institutions rely on predictable statutory frameworks to allocate limited privacy and compliance resources efficiently and effectively. Organizations like SCH must balance robust privacy stewardship with the practical need to direct the bulk of their resources toward patient care and community service. To accomplish their public health-oriented missions,

these organizations must ensure that health information can be shared effectively. And the same is true for businesses seeking to offer beneficial services to customers and clients. When compliance duties are defined clearly, organizations can structure privacy programs, train staff, and support governance frameworks with confidence that they are meeting their obligations.

Amici's members, along with other businesses and medical providers in Washington, are already subject to specialized rules governing consumer health information, like the MHMDA, which includes specific notice-and-consent obligations (*see supra* at 10–13). Under the MHMDA regime, for example, entities have concrete guidance about what conduct triggers which duties, and they can structure privacy programs and policies that meet those obligations. *See, e.g.,* RCW 19.373.030(1)(c) (delineating how consent can be obtained under the MHMDA).

Plaintiffs' broad interpretation of the WPA, in contrast, would inject uncertainty into routine digital operations and require the diversion of limited compliance resources into reengineering basic website functionality. A shift in the WPA would result in fractured and inconsistent compliance efforts, in addition to reduced capacity to advance core missions like patient care, research, and community engagement. The WPA's plain text does not cover the internet practices challenged here, and it should not be read to require institutions to play a high-stakes guessing game as to what is covered and what is not.

This unpredictability undermines not only operational planning, but also the goals at the heart of privacy law: to create rules that regulated entities can follow, consistently and transparently, in service of the public. *See, e.g., Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health and Hum. Servs., https://perma.cc/5FQP-2WEZ ("A major

goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being").

Second, accepting Plaintiffs' interpretation of the WPA would threaten *amici*'s members, along with other businesses and medical providers operating in Washington—including small businesses, *see The U.S. Lawsuit System Costs America's Small Businesses $160 Billion*, Inst. L. Reform (Jan. 4, 2024)—with potentially ruinous civil liability from class actions. That risk will grow substantially as plaintiffs increasingly rely on state privacy statutes to pursue claims seeking sizable statutory damages untethered from concrete harm. *See* Daniel Castro, Luke Dascoli & Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws,* Info. Tech. & Innovation Found. 12 (Jan.

2022), https://perma.cc/8T49-WQLZ. Privacy-related class action litigation has surged nationwide, with more than 2,500 data privacy class actions filed in 2024 alone, including lawsuits targeting routine internet tools and ordinary business operations. *US Data Privacy Litigation*, Int'l Ass'n of Priv. Pros. (Mar. 10, 2025), https://perma.cc/QUT4-F5C3. Construing the WPA to authorize similar freewheeling class-action liability in Washington would import these costs into the state, threatening entities that lack the resources to litigate or settle such claims. The 1967 Legislature did not license that result, and this Court should not embrace an interpretation of the WPA that does.

2. The Legislature is the proper body to tailor privacy protections to technological change.

This Court has long recognized that statutory expansions "in light of developments in technology" must come from the Legislature, which is "in the best position to weigh the competing policies." *State v. Townsend*, 147 Wn.2d

666, 675 n.2, 57 P.3d 255 (2002). Indeed, as explained, the Legislature has repeatedly demonstrated both its capacity and willingness to update state privacy law to address new technologies and streamline compliance for businesses and other organizations. The Legislature has not, however, amended the WPA in the manner Plaintiffs urge. The Court should not usurp the Legislature's prerogative to choose whether and how to do so by adopting Plaintiffs' interpretation here.

First, the WPA is a statute that carries criminal penalties, allocates rights and duties among private and public actors, and has significant operational consequences for institutions statewide. Decisions about whether to broaden its coverage—especially in a way that would affect every website operator in Washington—belong with the political branches, which can study the issue comprehensively, gather stakeholder input, and craft precise

rules that are built for real-world implementation. *See Baker v. Carr,* 369 U.S. 186, 217 (1962) (refusing to make "policy determination of a kind clearly for non–judicial discretion"). Indeed, the Attorney General's Office recently completed a data privacy survey to inform the State's work on these issues—a step that presumably would have been unnecessary if the WPA applied as broadly as Plaintiffs urge. *Data Privacy Hub*, Office of the Attorney General, https://perma.cc/6L68-SN7C.

And the Legislature has not been idle in responding to technological and data-use developments. When it perceives a need to extend privacy protections, it enacts targeted statutes calibrated to particular technological risks. For example, the MHMDA reflects the Legislature's capability to craft nuanced rules directed at specific sectors. The same is true of amendments enacted in 2015 governing law-enforcement use of cell-site simulators. RCW 9.73.270. Each

of these privacy protections reflect legislative judgment about where additional measures are necessary, what additional measures are appropriate, and how to implement those measures without imposing unworkable obligations on entities like hospitals, health care providers, nonprofits, businesses, and public agencies.

Equally telling is what the Legislature has *not* done. Despite heightened public awareness and ongoing national debates over website cookies, pixels, and digital analytics, and despite having amended the WPA four times, RCW 9.73.030, *amended by* Laws of 1977, 1st Ex. Sess., ch. 362 § 1; Laws of 1985, ch. 260 § 2; Laws of 1986, ch. 38 § 1; Laws of 2021, ch. 329 § 21, the Legislature has never adopted the policy Plaintiffs favor. Instead, it has left untouched the WPA's longstanding requirement that a covered communication be "between two or more individuals." RCW

9.73.030(1)(a). Plaintiffs' preferred interpretation of the statute would override that deliberate choice.

Second, in interpreting Washington law, this Court should reject Plaintiffs' invitation to add a privacy-protective judicial gloss to the WPA based on a comparison of Washington's statutes to those in other States. Plaintiffs argue that the WPA should be interpreted broadly because other states, in particular California, apply similar laws to online data collection. *See* Petitioner's Supplemental Brief at 7–8, *Baker v. Seattle Children's Hospital*, No. 104590 (Wash. Mar. 9, 2026). But that argument misunderstands both the governing principles of statutory interpretation and the proper interpretation of California privacy law.

To begin, this Court should not give the WPA a meaning it cannot bear based on the normative view that Washington intended to maximize privacy protections. *See, e.g., Pulsifer v. United States*, 601 U.S. 124, 152 (noting that

an interpretation of a statute is "not better just because it would go further" because "no law pursues its purposes at all costs"). As this Court has recognized, courts "do not add to or subtract from the clear language of a statute." *State v. Sullivan*, 143 Wn.2d 162, 175, 19 P.3d 1012 (2001). Rather, a statute's meaning is determined by its text, structure, and context—not by general reputation or aspirational policy arguments. *See Grayned v. City of Rockford*, 408 U.S. 104, 108–09 (1972) ("A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application").

The potential achievement of a broad policy aim does not change these principles. And courts should be especially wary of stretching a criminal statute to achieve regulatory outcomes better left to the legislature. *See Bittner v. United States*, 598 U.S. 85, 102 (2023) ("penal statutes are to be

construed strictly, and an individual is not to be subject to a penalty unless the words of the statute plainly impose it") (Gorsuch, J., joined by Jackson, J.); *Tiffany v. Nat'l Bank of Missouri,* 85 U.S. (18 Wall.) 409, 410 (1873) (no one should be "subjected to a penalty unless the words of the statute plainly impose it").

Moreover, even if cross-state comparisons did play a role in the analysis here, other states' statutes have no authoritative weight and should be respected only as the choice of *other* legislatures. In any event, Plaintiffs' characterization of California privacy law is incorrect. California regulates online data collection practices through its comprehensive data-privacy statutes, the California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 *et seq.*, and the California Privacy Rights Act (CPRA), Cal. Proposition 24 (2020) (amending the CCPA). California also has an older wiretap law, similar to the WPA, known as the

California Invasion of Privacy Act (CIPA), Cal. Penal Code §§ 630 *et seq*. Like the WPA, CIPA is best read not to apply to collection of online data, and several California courts have thus declined to use CIPA to regulate website analytics, instead directing litigants to the modern statutory frameworks designed specifically for online data practices. *See, e.g., Rodriguez v. Ink Am. Int'l. Grp. LLC*, 2025 WL 4034985, at *4 (Cal. Super. Ct. Dec. 10, 2025) (holding website data analytics tools were "intended by the Legislature to be covered by the CCPA and CPRA," not CIPA).

California plaintiffs' efforts to expand California privacy law beyond what the statutory text can support have led to conflicting court decisions and widespread confusion.[2]

[2] *Compare, 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.*, 2024 WL 4873370, at *2 (Cal. Super. Ct. Sept. 9, 2024) (holding that CIPA "does not

One federal judge candidly assessed that CIPA's language is a "total mess" made "bigger and bigger" by the need for courts to stretch and mold that language to suit emerging technologies. *Doe v. Eating Recovery Ctr.*, 806 F. Supp. 3d 1109, 1112 (N.D. Cal. Oct. 17, 2025). Plaintiffs' proposed expansion of the WPA would saddle Washington courts with the same analytical difficulties observed in California, while depriving businesses, nonprofits, and other entities of the fair notice, clarity, and appropriately tailored regulation that come from privacy statutes crafted specifically for the digital environment. Any expansion of Washington's privacy regime must come by legislative enactment, not judicial fiat.

---

address the privacy rights of internet users"); *Rodriguez*, 2025 WL 4034985, at *4 (holding that CIPA "indicates a deliberate choice not to sweep ordinary website analytics" within its ambit) *with Deivaprakash v. Conde Nast Digital*, 798 F. Supp. 3d 1100, 1104–06 (N.D. Cal. 2025) (holding that website operator's trackers were prohibited under CIPA); *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 933 (N.D. Cal. 2024) (holding that mere collection of IP addresses violated CIPA).

V. CONCLUSION

For the foregoing reasons, the Court should affirm the Court of Appeals' Decision.

VI. CERTIFICATE OF COMPLIANCE

Exclusive of the title sheet, table of contents, table of authorities, certificate of compliance, certificate of service, and signature blocks, this document contains 4,194 words complies with Washington Rule of Appellate Procedure 18.17.

Dated: April 10, 2026

Respectfully submitted,

/s/ *Ingrid L. Price*

Ingrid L. Price (WSBA No. 56076)
iprice@cov.com
Abby C. Wright+
awright@cov.com
COVINGTON & BURLING LLP
One CityCenter
850 10th Street, NW
Washington, DC 20001
Telephone: (202) 662 6000

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

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 Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I caused the foregoing document to be electronically filed and served on counsel of record using the Washington State Appellate Courts' e-file portal.

Declared under penalty of perjury under the laws of the state of Washington dated at Seattle, Washington, this 10th day of April.

/s/ Ingrid L. Price

Ingrid L. Price