

FILED
SUPREME COURT
STATE OF WASHINGTON
4/10/2026 2:47 PM
BY SARAH R. PENDLETON
CLERK

Supreme Court No. 1045905

**IN THE 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.

**BRIEF OF AMICUS CURIAE
INTERACTIVE ADVERTISING BUREAU, INC.
IN SUPPORT OF DEFENDANT/RESPONDENT**

Marc R. Shapiro (N.Y. SBN 4403606)
Christopher J. Cariello (N.Y. SBN
5176821)
Ned Hirschfeld (N.Y. SBN 5281829)
51 West 52nd St
New York, NY 10019
Telephone: (212) 506-5000
mrshapiro@orrick.com
ccariello@orrick.com
nhirschfeld@orrick.com

Robert M. McKenna
(WSBA #18327)
Aravind Swaminathan
(WSBA #33883)
401 Union Street, Suite 3300
Seattle, WA 98101
Telephone: (206) 839-4415
rmckenna@orrick.com
aswaminathan@orrick.com

Ian Hawkes (D.C. Bar #90012466)
2100 Pennsylvania Ave NW
Washington, DC 20037
Telephone: (202) 339-8400
ihawkes@orrick.com

Counsel for Amicus Interactive Advertising Bureau, Inc.

TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	1
II. INTEREST OF THE <i>AMICI CURIAE</i>	2
III. STATEMENT OF THE CASE.....	3
IV. ARGUMENT	3
A. Plaintiffs’ Overbroad Definition Of “Private Communications ... Between Two Or More Individuals” Would Encompass All Internet Activity.....	3
B. Plaintiffs’ Overbroad Construction Would Disrupt Internet Activity In Ways The Washington Legislature Never Contemplated Or Intended.....	9
V. CONCLUSION	17

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Animal Legal Def. Fund v. United States Dep’t of Agric.</i> , 933 F.3d 1088 (9th Cir. 2019)	7
<i>Mohamad v. Palestinian Auth.</i> , 566 U.S. 449 (2012).....	7
<i>State v. Riley</i> , 121 Wash. 2d 22 (1993).....	7, 8
<i>United States v. Farrell</i> , 2016 WL 705197 (W.D. Wash. Feb. 23, 2016).....	8, 10
<i>United States v. Forrester</i> , 512 F.3d 500, 510 (9th Cir. 2008)	8
<i>Vita v. New England Baptist Hosp.</i> , 494 Mass. 824 (2024)	8
Statutes	
RCW 9.73.030.....	7, 15
RCW 19.373.005.....	2, 15, 16
Other Authorities	
Chitraa V., Davamani A., A Survey on Preprocessing Methods for Web Usage Data, International Journal of Computer Science and Information Security, Vol. 7, No. 3, 82 (2010).....	9
Codecademy, Understanding HTTP Requests, https://www.codecademy.com/article/what-is-http ;	5, 6
Connected Commerce Council, Small Business Find Big Value in Digital Ads, available at https://tinyurl.com/bdd65uur ;	13
Garett R, Chiu J, Zhang L, Young SD. A Literature Review: Website Design and User Engagement. Online J Commun Media Technol, 6(3):1 (July 2016).....	10
Jerry V. Glowniak, An Introduction to the Internet, Part 1: History, Organization and Function, 23 J. Nucl. Med. Technol. 56, 59 (1995).....	5

John Naughton, The Evolution of the Internet: From Military Experiment to General Purpose Technology, 1 J. Cyber Pol’y 5, 9 (2016).....	5
Laws of 1967, Ch. 93, § 1.....	14
Laws of 1977, Ch. 36, § 1.....	14
Laws of 1985, Ch. 260, § 1.....	14
Laws of 1986, Ch. 38, § 1.....	14
Laws of 2001, Ch. 329, § 3.....	14
Oxford English Dictionary 880 (2d ed. 1989)	7
SBE Council, The Digital Boost to Startups and Small Business: Online Advertising Delivers BIG Benefits, available at https://tinyurl.com/bp538hax	13
Web Performance Working Group Charter, available at https://tinyurl.com/wdhke8nk	10, 11
Webster’s Third New International Dictionary 460 (1986)	7

I. INTRODUCTION

Plaintiffs misleadingly warn that the Court of Appeals' decision leaves the WPA "with no application whatsoever to internet-based communications." Pet. for Rev. at 1-2. That is wrong: As the Court of Appeals' narrow ruling recognized, the WPA may play an important role in regulating personal exchanges over the internet that mirror the telephone calls and text messages long covered by the statute.

The real risk lies squarely in the other direction. Plaintiffs are urging this Court to endorse an overbroad construction of the WPA's phrase "private communications ... between two or more individuals" that would encompass *every internet connection*, full stop. The Interactive Advertising Bureau, Inc. ("IAB") submits this amicus brief to provide the technical context necessary to understand the full sweep of Plaintiffs' erroneous construction—and the extent to which it would disrupt fundamental internet functions that benefit Washington residents.

The Washington Legislature already regulates the collection and sharing of data over the internet through internet-specific privacy statutes like the My Health My Data Act, RCW 19.373, which restricts how websites may use health-related information. Plaintiffs' overbroad reading of the WPA would trample the Legislature's carefully honed choices, transforming a decades-old wiretapping statute into a dangerously blunt instrument that would threaten civil and even criminal liability for routine internet functionality. This Court should reject that construction and instead reinforce sensible limits on the WPA's application to the internet.

II. INTEREST OF THE *AMICI CURIAE*

IAB is a leading trade association for the digital advertising industry in the United States. IAB's membership includes media companies, brands, agencies, and technology firms that collectively depend on standard digital analytics tools—including pixel tracking technology—to deliver, optimize, and measure digital advertising campaigns and

improve user experiences. The outcome of this case will directly affect IAB's members and their consumers.

III. STATEMENT OF THE CASE

IAB relies on the facts presented in the brief of Respondent Seattle Children's Hospital ("SCH").

IV. ARGUMENT

A. Plaintiffs' Overbroad Definition Of "Private Communications ... Between Two Or More Individuals" Would Encompass All Internet Activity.

Two individuals may, of course, communicate privately over the internet. A telephone call placed using a Voice Over Internet Protocol service, text messages exchanged on an internet messaging application, a live website chat with technical support—all of those examples involve two people communicating, and the WPA protects their privacy. But this case has nothing to do with that. Indeed, SCH purposefully designed the website at issue *not to enable* users to communicate with a doctor or other care team member. Those internet communications between individuals are confined to a separate

website with particularly rigorous privacy protections. Ans. to Pet. at 5.

Instead, this case implicates a categorically different type of interaction—the technological transmissions that undergird any internet connection. Plaintiffs allege only that they accessed materials that SCH had previously posted on its public website. *E.g.*, Compl. ¶¶ 59, 79-81. That conduct bears no resemblance to telephone calls or text messages; it is the electronic equivalent of solitary research, like browsing pamphlets pinned to a public library bulletin board. How, then, do Plaintiffs frame their activity as private communication between two individuals? By delving into the nuts and bolts of internet access. Plaintiffs emphasize that in order to use SCH’s public website, the user’s “browser sends a web communication called a ‘GET request’ to the server where SCH hosts its website,” which responds with “an ‘HTTP Response’ that displays the webpage on the person’s browser.” Pet. for Rev. 6. That is the interaction that, in

Plaintiffs’ telling, constitutes a communication between individuals within the meaning of the WPA.

It is critical to understand how fundamentally Plaintiffs’ theory would affect internet activity. The technological interaction that Plaintiffs highlight—a browser’s GET request followed by a server’s HTTP response, formatted as packets for transmission—is how **any** computer accesses **any** information on **any** website. It is thus “the foundation of the World Wide Web.”¹ Someone standing in front of a library bulletin board can physically grab a pamphlet posted there. An internet user reaches the same material by accessing a publicly available server. That access happens when the user’s browser sends the

¹ Codecademy, What is HTTP? Understanding HTTP Requests, <https://www.codecademy.com/article/what-is-http>; see Jerry V. Glowniak, An Introduction to the Internet, Part 1: History, Organization and Function, 23 J. Nucl. Med. Technol. 56, 59 (1995) (explaining that all internet communications use the TCP/IP protocol suite, under which data is broken into packets with headers containing IP addresses and routing instructions that are passed through a series of routers and networks until they reach their destination); John Naughton, *The Evolution of the Internet: From Military Experiment to General Purpose Technology*, 1 J. Cyber Pol’y 5, 9 (2016) (describing how the Internet’s TCP/IP architecture was designed so that the network “should take in data packets at one end and do its best to deliver them to their destination” and “would be entirely agnostic about the contents or purpose of the packets”).

server an “HTTP request,” which is a “structured message” used “to request a resource or trigger an action.”² A “GET request” is the type of HTTP request that “[r]etrieves data from the server (e.g., loading a webpage).”³ The server then “responds with an HTTP response that contains” specific bits of code.⁴

Under Plaintiffs’ construction, therefore, every time anyone visits any website for any reason, they engage in a private communication with another individual (the website’s server) under the WPA, and the website would be potentially liable for collecting the data necessary to form an internet connection. Indeed, Plaintiffs urge that the WPA “protects against the interception of even non-content record data,” including the most barebones HTTP browser request and server response. Pet. for Rev. at 29. The particular allegations in this case include users’ purported navigation to public webpages related to health conditions. *E.g.*, Compl. ¶¶ 59, 79. But Plaintiffs’ legal theory is

² Codeacademy, *supra* n.1.

³ *Id.*

⁴ *Id.*

not confined to those, or any other, particular facts. If the Court adopted Plaintiffs’ reading of the WPA, **any** internet connection to a website would instantly form the basis for a potential WPA claim.

Fortunately, that is not what the WPA says. The statute sensibly regulates only “private communication[s] ... between two or more **individuals**.” RCW 9.73.030(1)(a) (emphasis added). This Court has already ruled, relying on common dictionary definitions, that “communication” means “the act ... of imparting or transmitting” “facts or information.” *State v. Riley*, 121 Wash. 2d 22, 33 (1993) (quoting Webster’s Third New International Dictionary 460 (1986)). The dictionary meaning of “individual,” in turn, is “[a] human being, a person.” *Mohamad v. Palestinian Auth.*, 566 U.S. 449, 454 (2012) (quoting 7 Oxford English Dictionary 880 (2d ed. 1989)); see *Animal Legal Def. Fund v. United States Dep’t of Agric.*, 933 F.3d 1088, 1094 (9th Cir. 2019) (the word “individual ordinarily refers to a single human being.” (quotation marks omitted)).

The WPA thus applies when two human beings exchange facts or information. Such an exchange may occur in person or over the telephone. *See Riley*, 121 Wash. 2d at 34 (1993). It may also occur over the internet, including in the examples provided above: a Voice Over Internet Protocol call, messaging application exchange, or live website chat. In those circumstances, the internet facilitates a conversation between humans, and the WPA provides privacy protections for the conversation. But the mere interaction between a browser and server, connecting a website user to publicly posted content, is something else entirely. It is an automated interaction between devices, not an exchange between individuals.⁵ The Court should confirm that commonsense boundary on the WPA’s application to internet activity. *See Vita v. New England Baptist Hosp.*, 494

⁵ As a separate matter, automated interactions between devices that establish an internet connection, like the conveyance of an IP address, are not “private.” *See, e.g., United States v. Farrell*, 2016 WL 705197, at *1 (W.D. Wash. Feb. 23, 2016) (“Internet users have no expectation of privacy in ... the IP address of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.” (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008))).

Mass. 824, 826 (2024) (reading Massachusetts’s equivalent of the WPA to “prohibit new and evolving technological means of secret electronic eavesdropping on ... person-to-person conversations or messaging” over the internet, but not “a website user’s browsing of, and interaction with, information published on a website”).

B. Plaintiffs’ Overbroad Construction Would Disrupt Internet Activity In Ways The Washington Legislature Never Contemplated Or Intended.

It is hard to overstate how dramatically Plaintiffs’ misreading of the WPA would disrupt internet activity in Washington. Websites and their service providers intercept or record connections with users for a wide range of reasons, many vital to the internet’s basic functionality. For example, website operators may analyze records of user connections to fix technological snags or identify ways to improve connection quality. Or when troubleshooting user complaints.⁶ Or when

⁶ Chitraa V., Davamani A., A Survey on Preprocessing Methods for Web Usage Data, International Journal of Computer Science and Information Security, Vol. 7,

assessing and ameliorating security concerns.⁷ Or when analyzing the relative popularity of a website's various resources in order to develop new content in line with public interest.⁸

Those sorts of functions have grown even more essential as the internet has evolved. "As Web browsers and their underlying engines include richer capabilities and become more powerful, web developers are building more sophisticated applications where application performance is increasingly important."⁹ That has heightened website operators' "need ... to assess and understand the performance characteristics of their applications" by collecting data about user interactions.¹⁰

No. 3, 82 (2010) ("System Improvement is done by understanding the web traffic behavior by mining log data so that policies are developed for Web caching, load balancing, network transmission and data distribution. Patterns for detecting intrusion fraud, attempted break-ins are also provided by mining. Performance is improved to satisfy users.")

⁷ *See id.*

⁸ *See* Garrett R, Chiu J, Zhang L, Young SD. A Literature Review: Website Design and User Engagement. *Online J Commun Media Technol*, 6(3):1 (July 2016) (explaining how "a well-designed website with high usability has been found to positively influence visitor retention" while a "[p]oorly designed websites may frustrate users and result in a high 'bounce rate,' or people visiting the entrance page without exploring other pages within the site.")

⁹ Web Performance Working Group Charter, available at <https://tinyurl.com/wdhke8nk>.

¹⁰ *Id.*

Recording that information enables websites “to measure and improve aspects of application performance,” including basic metrics like the “end to end latency associated with loading a webpage.”¹¹ It also facilitates “error logging” and detection of “memory leaks.”¹²

These activities are essential to a well-functioning and safe internet. And all of them inescapably require recording basic data about user connections to the website; otherwise, website operators would lack *any* information about website usage and could not respond with meaningful troubleshooting, security, or content improvement. Under Plaintiffs’ reading, all of that would constitute the interception or recording of private communications between two individuals and so could give rise to WPA liability.

To be sure, Plaintiffs have not focused on those forms of interception or recording. But that is precisely the danger this

¹¹ *Id.*

¹² *Id.*

case presents. Plaintiffs are still relying on a ***statutory construction*** that would encompass all of that activity, by urging that the WPA’s phrase “private communication ... between two or more individuals” covers not merely conversations between people but also the packet transmissions between browsers and servers that facilitate every website visit on earth. If the Court were to endorse that construction here, it would threaten civil and even criminal consequences in future cases for all sorts of innocuous website troubleshooting, security, and analytics.

Plaintiffs’ overbroad reading would also imperil the foundations of digital advertising. For example, websites must record and transmit to measurement vendors basic technical information about whether users view or click on an advertisement in order to quantify its reach. Advertisers demand that sort of measurement and would not pay for advertisements without it. But Plaintiffs’ reading of the WPA could disrupt the collection and disclosure of even the simplest data. Plaintiffs try to marginalize that disruption by casting aspersions on so-called

“surveillance technology used by Big Tech.” Pet. for Rev. 2. But advertising revenue is the lifeblood of countless small-scale publishers across the internet, enabling them to make content freely available to consumers. Surveys have also confirmed that a vast majority of small businesses rely on digital advertising to “compete with larger companies.”¹³ Plaintiffs’ construction of the WPA could unduly chill those economic frameworks for freely available, diverse internet content.

To be sure, Plaintiffs’ construction would not *automatically* impose liability in all of these circumstances. In theory, user consent would remain a statutory defense. But it would plainly be unworkable for website operators to secure consumer consent for every single packet transmission that facilitates internet connectivity, just as telephone operators could not feasibly secure consumer consent for every

¹³ Connected Commerce Council, *Small Business Find Big Value in Digital Ads*, available at <https://tinyurl.com/bdd65uur>; see SBE Council, *The Digital Boost to Startups and Small Business: Online Advertising Delivers BIG Benefits*, available at <https://tinyurl.com/bp538hax> (“The smaller the business, the more important online advertising is to growth and survival[.]”).

electromechanical signal that facilitates telephone connectivity. Recording transmissions like GET requests is the technological architecture of the internet. If websites had to request, and consumers reaffirm, consent every time that occurred, using the internet would become an interminable slog.

There is no indication whatsoever that the Washington Legislature contemplated such dramatic applications of the WPA. The statute was enacted in 1967 to regulate wiretapping of telephone communications between callers. *See Laws of 1967, ch. 93, § 1.* The Legislature subsequently made four rounds of narrow amendments, but none entailed any discussion of regulating the internet.¹⁴ The Legislature certainly has never expressed any intent to impose liability for the foundational

¹⁴ The first set of amendments, in 1977, added one-party consent exceptions for emergencies, threats of extortion, and anonymous calls. *Laws of 1977, ch. 363, § 1.* Further amendments in 1985 added an exception for hostage and barricade situations. *Laws of 1985, ch. 260, § 1.* Additional amendments a year later expanded the emergency exception to include medical emergencies and added emergency service personnel. *Laws of 1986, ch. 38, § 1.* The most recent changes, in 2021, addressed the electronic recording of custodial interrogations. *Laws of 2021, ch. 329, § 3 (House Bill No. 1223).*

packet transmissions that power all websites, absent consumer consent for every single one of those transmissions.

What the Washington Legislature *has* shown is a focus on regulating internet data collection, and addressing related privacy concerns, through more modern, specialized statutes. The My Health My Data Act is a particularly relevant example for this case. The Legislature there recognized that “apps and websites” may collect “health information” over the internet. RCW 19.373.005(2). So it enacted a statute “to provide heightened protections for Washingtonian’s health data” on the internet by “[r]equiring additional disclosures and consumer consent regarding the collection, sharing, and use of such information.” RCW 19.373.005(3). The Act strikes a careful balance, requiring distinct consumer consent “for such sharing” in many circumstances, but not where companies use it as “necessary to provide a product or service that the consumer to whom such consumer health data relates has requested.” RCW 19.373.030(1)(b). That sort of consent requirement is relatively

manageable precisely because it applies only to select transmissions, not every conceivable GET request.

The internet's unique technology and functionality demand these sorts of tailored statutes. Plaintiffs urge something entirely different: Transforming the WPA into a blunt regulatory instrument that could subject websites to civil and criminal liability for making a record of **any** underlying packet transmission, absent consumer consent at a scale that would be untenable in practice. Endorsing that construction would not merely wreak havoc on website functionality for Washington residents—it would effect, through judicial decision, a statutory framework that Washington's Legislature never chose, while trampling more nuanced laws (and embedded consent regimes) like the My Health My Data Act. The Court should avoid that outcome by hewing to the Court of Appeals' sensibly cabined ruling.

V. CONCLUSION

For the foregoing reasons, amicus curiae IAB respectfully urges this Court to affirm the decision of the Court of Appeals.

This document contains 2726 words, excluding the parts of the document exempted from the word count by RAP 18.17.

Respectfully submitted this 10th day of April 2026.

/s/ Robert M. McKenna

Robert M. McKenna

Marc R. Shapiro (N.Y. SBN
4403606)
Christopher J. Cariello (N.Y.
SBN 5176821)
Ned Hirschfeld (N.Y. SBN
5281829)
51 West 52nd St
New York, NY 10019
Telephone: (212) 506-5000
mrshapiro@orrick.com
ccariello@orrick.com
nhirschfeld@orrick.com

Robert M. McKenna
(WSBA #18327)
Aravind Swaminathan
(WSBA #33883)
401 Union Street, Suite 3300
Seattle, WA 98101
Telephone: (206) 839-4415
rmckenna@orrick.com
aswaminathan@orrick.com

Ian Hawkes (D.C. Bar
#90012466)
2100 Pennsylvania Ave NW
Washington, DC 20037
Telephone: (202) 339-8400
ihawkes@orrick.com

Counsel for Amicus Interactive Advertising Bureau, Inc.

CERTIFICATE OF SERVICE

I hereby certify that I caused the foregoing **Brief of Amicus Curiae** to be served on counsel for all other parties in this matter via this Court's e-filing platform.

Dated April 10, 2026.

/s/ Robert M. McKenna

ORRICK, HERRINGTON & SUTCLIFFE LLP

April 10, 2026 - 2:47 PM

Transmittal Information

Filed with Court: Supreme Court
Appellate Court Case Number: 104,590-5
Appellate Court Case Title: Carly Baker, et al. v. Seattle Childrens Hospital

The following documents have been uploaded:

- 1045905_Briefs_20260410144350SC629505_3845.pdf
This File Contains:
Briefs - Amicus Curiae
The Original File Name was IAB - Baker Amicus Brief.pdf
- 1045905_Motion_20260410144350SC629505_1924.pdf
This File Contains:
Motion 1 - Amicus Curiae Brief
The Original File Name was IAB - Motion for Leave to File Baker Amicus Brief.pdf

A copy of the uploaded files will be sent to:

- FredBurnside@dwt.com
- andreadombovari@dwt.com
- aswaminathan@orrick.com
- ccariello@orrick.com
- francescareifer@dwt.com
- ihawkes@orrick.com
- jamessigel@dwt.com
- kstephens@tousley.com
- lisamerritt@dwt.com
- lpeterson@orrick.com
- lteppner@tousley.com
- megangalloway@dwt.com
- mpeterson@tousley.com
- mrshapiro@orrick.com
- nhirschfeld@orrick.com
- rachelherd@dwt.com
- rmckenna@orrick.com
- rsolomon@tousley.com
- ryan.ellersick@zimmreed.com

Comments:

Motion for Leave to file Amicus Curiae Brief; Amicus Brief

Sender Name: Malissa Tracey - Email: mtracey@orrick.com

Filing on Behalf of: Robert M. McKenna - Email: rmckenna@orrick.com (Alternate Email: sea_wa_appellatefilings@orrick.com)

Address:

701 Fifth Avenue, Suite 5600
Seattle, WA, 98104
Phone: (206) 839-4309

Note: The Filing Id is 20260410144350SC629505