No. 86461-1

IN THE COURT OF APPEALS, DIVISION ONE
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.

PETITION FOR REVIEW

Kim D. Stephens
Rebecca L. Solomon
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue,
Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600

Ryan J. Ellersick
ZIMMERMAN REED LLP
14648 North Scottsdale Rd.,
Ste. 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400

Attorneys for Petitioners

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

In recent years, numerous federal courts around the country have found claims viable under the federal Wiretap Act and other state wiretap statutes when a healthcare provider deploys third-party tracking technologies on its website that allow Big Tech companies to intercept a user's health-related communications. This case presents the question whether the Washington Privacy Act ("WPA")—which is "one of the most restrictive electronic surveillance laws ever promulgated." *State v. Roden*, 179 Wn.2d 893, 898, 321 P.3d 1183 (2014), and "extends considerably greater protections" than the federal Wiretap Act, *State v. Gunwall*, 106 Wn.2d 54, 66, 720 P.2d 808 (1986)—also provides a viable claim for Washington residents.

The Court of Appeals found it did not. In doing so, the Court of Appeals interpreted the WPA in a way that renders the statute among the *least* protective electronic surveillance laws in the country—with no application whatsoever to internet-based

communications and the evolving surveillance technology used by Big Tech and other corporations to harvest consumer data at scale. The Court of Appeals decision conflicts with multiple decisions from this Court, which direct that the WPA should be interpreted "in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape." *State v. Christensen*, 153 Wn.2d 186, 197, 102 P.3d 789 (2004).

In the almost ten years since this Court interpreted the WPA, the technological landscape has evolved rapidly, and with it the methods consumers use to interact with their health care providers. Rather than pick up the phone, consumers routinely go online or download an app to their mobile phones. They research symptoms and conditions, they review doctor profiles, and they book appointments—all of which reveal intimate details about their personal and family health situations. The data is valuable, and corporations have developed sophisticated

technology to harvest that data without a consumer's knowledge or consent. Yet the Court of Appeals found that the WPA offers no protection for Washington residents who are secretly surveilled online by this technology. This Court should grant review to decide the important question whether the WPA protects against a third party's non-consensual interception and eavesdropping on a Washington resident's private web communications with their health care provider.

II. IDENTITY OF PETITIONER

Petitioners are Carly Baker, Janssen Ramos Savoie, and Amber Shavies.

III. COURT OF APPEALS DECISION

Petitioners seek review of the decision by Division One of the Court of Appeals, No. 86461-1, filed on August 18, 2025, and attached to the Appendix.

IV. ISSUES FOR REVIEW

In holding that the WPA provides no protection against third-party surveillance of website communications, did the Court of Appeals misapply this Court's precedents directing that the WPA should be interpreted to protect the private communications of Washington residents in the face of an ever-changing technological landscape? And is it a matter of substantial public interest for this Court to review whether the WPA provides the same—if not greater—protections than the federal Wiretap Act for Washington residents who are the victims of online surveillance?

V. STATEMENT OF THE CASE

Like many hospitals, one of the ways Seattle Children's Hospital ("SCH") interfaces with its patients is through its website, www.seattlechildrens.org (the "website"). Clerk's Papers ("CP") 1-2, ¶¶ 1-2. Visitors to the website can search for information about specific conditions, such as by visiting the

website's page on "depression." CP 17, ¶ 59. Users can also type specific search terms into the website search bar, such as the term "suicide," which brings up various articles and resources. CP 23, ¶ 79. Patients and prospective patients visiting the website can also search for physicians based on the doctor's specialty and other pre-populated search criteria. CP 25, ¶ 81. A search for doctors with experience in "eating disorders," for example, brings up a list of physicians with experience treating those conditions. *Id.*

Despite warnings from federal regulators regarding the privacy concerns of tracking technologies on healthcare websites, CP 34-35, ¶¶ 110-11, SCH chose to deploy one of the most invasive website tracking technologies on the market today—the Meta Pixel. The Meta Pixel is a piece of software code that Meta makes available for companies to use on their websites for free. CP 12, ¶ 43. The purpose of the Meta Pixel is to track people who visit websites—including pages they view

and search terms they input into search bars—and retarget those people with ads on Facebook and Instagram so they return to the website to buy goods and services. CP 12, 17, ¶¶ 43, 58.

The Meta Pixel works by eavesdropping on web communications between individuals and SCH. When a person types in the web address for SCH's website, the person's browser sends a web communication called a "GET request" to the server where SCH hosts its website. CP 13-14, 17, ¶¶ 46-47, 59. In response to the GET request, the SCH server sends a web communication called an "HTTP Response" that displays the webpage on the person's browser. CP 13-14, 18, ¶¶ 46-47, 60.

Because SCH deploys the Meta Pixel on its website, SCH's HTTP Response contains more just than the content of the webpage—it also contains the Meta Pixel, which secretly infiltrates the person's browser, triggering the interception of the person's web communications with SCH from that point forward. CP 14-15, 18, ¶¶ 49-50, 60-61. For example, if a person

requested to see the "depression" page on SCH's website, Meta would also receive the identical request showing that the person loaded the "depression" page, as reflected in ***Figures 1*** and ***2*** below. CP 17-18, ¶¶ 59-61.

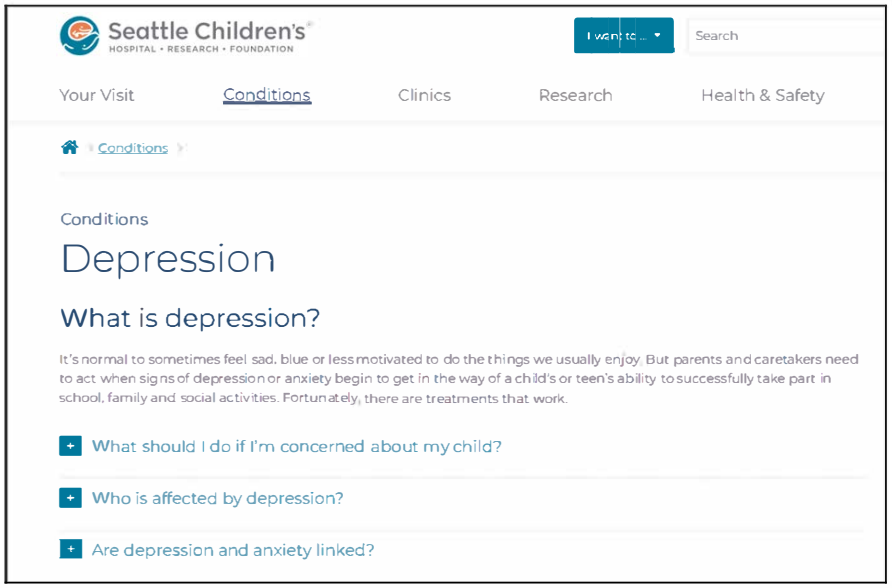

Figure 1: Example of webpage SCH server loads when person selects "depression" on SCH website's "Condition" webpage (CP 17, ¶ 59)

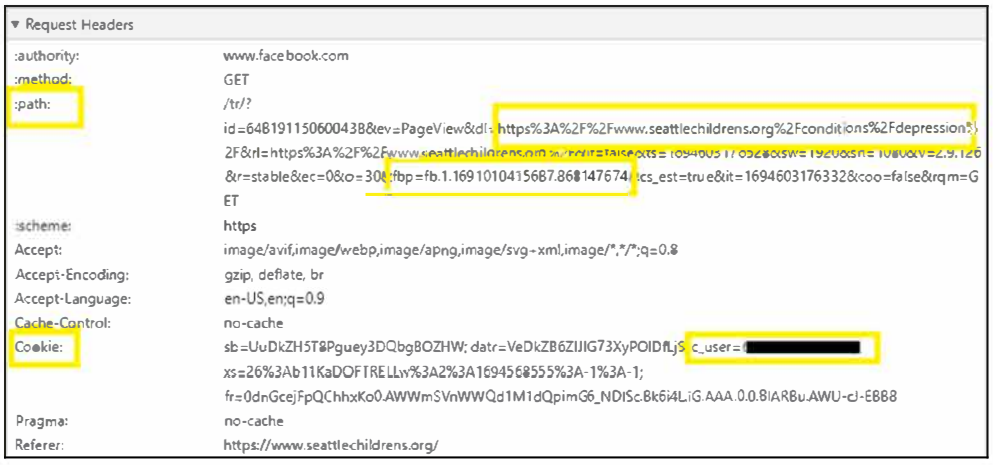

Figure 2: Information transmitted to Meta via the Pixel (CP 18, ¶ 61).

As shown in ***Figure 2***, in addition to relaying the contents of the individual's communications with SCH—that the person searched for "depression"—the Pixel also triggers the transmission of unique identifiers that Meta uses to link the communications to a particular person or Facebook account holder. CP 15, ¶ 53. One of those identifiers is the "c_user" cookie, which Facebook places on the device of every Facebook user when they establish their account. CP 15-16, ¶ 55. When that person later visits a website like SCH's where

the Meta Pixel is embedded, the Pixel triggers the person's browser to send Meta the "c_user" cookie associated with the person's device. *Id.* Because the "c_user" cookie is unique to each Facebook account holder, Facebook is able to link the person's web communications—in this case, that the person searched for "depression"—with the person's Facebook account.[1] *Id.*

Meta then uses that data to sell targeted advertising to entities like SCH interested in retargeting specific web users with ads. CP 7, 17, ¶¶ 19, 58. Based on the above search, for example, Meta could sell advertising to a mental health company seeking to target a Facebook user (and others like that person) who live in the Seattle area, who have children or teenagers struggling

[1] The Pixel also triggers the transmission of other data Meta can use to identify the person communicating with the SCH website, such as the person's IP address, device ID, and other unique cookies. CP 4, 15, 19, 22, ¶¶ 8, 52-53, 63, 71.

with mental health issues, and who recently searched for mental health resources or "depression." CP 27, ¶ 85.

Petitioners are among the SCH website users who conveyed sensitive information about their family medical needs to SCH not knowing that SCH had deployed the Meta Pixel to intercept their communications. Petitioner Baker alleged that she used the SCH website to "search for medical conditions and symptoms, including by utilizing the Website's 'search' bar and 'Conditions' webpage," to communicate information regarding her minor daughter's health conditions. CP 5-6, ¶ 15. Petitioner Shavies alleged she "conducted searches to locate urgent care facilities and identify their hours of operation" and to log in to the patient portal for her two underage children. CP 6, ¶ 16. And Petitioner Savoie alleged she used the SCH website to "search for health care providers and medical specialists, including by utilizing the Websites 'search' bar and 'Find a Doctor' webpage," on behalf of her underage son who was a patient of

SCH. CP 6, ¶ 17. Savoie further alleged she "conducted searches on medical conditions and symptoms." *Id.* All three Petitioners had Facebook and/or Instagram accounts when they visited the SCH website, and they alleged that SCH intercepted this sensitive health information and disclosed it to Meta for purposes of ad targeting. CP 5-7, 19 ¶¶ 15-17, 64. Indeed, some Petitioners "recall receiving health-related advertisements on Facebook after using Defendant's Website, including ads related to specific symptoms communicated to [SCH] on the Website"—indicating the Meta Pixel served its intended purpose. CP 7, ¶ 19.

After learning about this practice, Petitioners filed a complaint bringing claims individually and on behalf of other Washington residents whose communications with the SCH website were intercepted via the Meta Pixel without consent. CP 40, ¶ 129.

On January 5, 2024, SCH moved to dismiss the Complaint for failure to state a claim under CR 12(b)(6). CP 114. On

February 23, 2024, the Superior Court entered an Order Granting Defendant's Motion to Dismiss, dismissing the claims with prejudice. CP 102-04.

Petitioners timely filed their notice of appeal on March 22, 2024. CP 107-113. Petitioners limited their appeal to the trial court's dismissal of the WPA claim.

The Court of Appeals affirmed the dismissal, holding that Plaintiffs' website communications alleged in the Complaint did not constitute "communications," as covered by the WPA.

VI. THIS COURT SHOULD GRANT REVIEW UNDER RAP 13.4(b)(1) and (4)

This Court has never addressed whether the WPA applies to the type of web-based communications that increasingly define how consumers interact with their healthcare providers and other corporate actors. In the almost ten years since this Court last interpreted the WPA, communications and surveillance technology have evolved rapidly. Review is

warranted to correct the Court of Appeals' cabined interpretation of the WPA and to answer the important question whether the WPA applies to web-based communications.

A. The WPA is One of the Most Protective Wiretap Statutes in the Country

The WPA provides that,

> it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington . . . to intercept, or record any . . .
>
> [p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.

RCW 9.73.030(1)(a).

The WPA creates a private right of action, providing that "[a]ny person who, directly or by means of a detective agency or

any other agent,[2] violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation." RCW 9.73.060. The WPA also entitles victims 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." *Id.*

This Court has repeatedly emphasized that the WPA "is one of the most restrictive electronic surveillance laws ever promulgated." *Roden*, 179 Wn.2d at 898; *State v. Faford*, 128 Wn.2d 476, 481, 910 P.2d 447 (1996) ("Washington's privacy act is one of the most restrictive in the nation."); *State v.*

[2] Petitioners alleged that SCH is liable under the WPA for using Meta as its "agent" to intercept Petitioners' website communications.

Townsend, 147 Wn.2d 666, 672, 57 P.3d 255 (2002) (observing that the WPA "is considered one of the most restrictive in the nation"); *State v. Kipp*, 179 Wn.2d 718, 724, 317 P.3d 1029 (2014) ("Washington State's privacy act is considered one of the most restrictive in the nation.").

In comparison to the federal Wiretap Act, for example, the WPA provides significantly more protection for Washington residents. *Roden*, 179 Wn.2d at 898 ("Overall, the [WPA] significantly expands the minimum standards of the federal statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520, and offers a greater degree of protection to Washington citizens.") (citation modified); *Gunwall*, 106 Wn.2d at 66 (observing that the WPA "is broad, detailed and extends considerably greater protections to our citizens in this regard than do comparable federal statutes and rulings thereon").

The fact that the WPA "significantly expands the minimum standards of the federal [wiretap] statute" and "offers a greater degree of protection to Washington citizens," *Roden*, 179 Wn.2d at 898, is important given the growing trend among federal courts finding that use of the Meta Pixel to intercept health-related web communications states a viable claim under the federal Wiretap Act. *See Castillo v. Costco Wholesale Corp.*, No. 2:23-CV-01548-JHC, 2024 WL 4785136, at *7 (W.D. Wash. Nov. 14, 2024) (collecting cases); *Sweat v. Houston Methodist Hospital*, No. CV H-24-775, 2024 WL 3070184, at *4 (S.D. Tex. June 20, 2024) (denying motion to dismiss under federal wiretap statute based on healthcare provider's use of Meta Pixel on website); *R.C. v. Walgreen Co.*, No. EDCV 23-1933 JGB (SPX), 2024 WL 2263395, at *16 (C.D. Cal. May 9, 2024) (same); *Hartley v. Univ. of Chicago Med. Ctr.*, No. 22 C 5891, 2024 WL 1886909, at *3 (N.D. Ill. Apr. 30, 2024) (same); *Mekhail v. N. Mem'l Health Care*, No. 23CV00440KMMTNL,

2024 WL 1332260, at *5 (D. Minn. Mar. 28, 2024) (same); *Kane v. Univ. of Rochester*, No. 23-CV-6027-FPG, 2024 WL 1178340, at *7 (W.D.N.Y. Mar. 19, 2024) (same); *B.K. v. Desert Care Network et al*, No. 223CV05021SPGPDX, 2024 WL 1343305, at *6 (C.D. Cal. Feb. 1, 2024) (same); *In re Group Health Plan Litigation*, No. 23-CV-267 (JWB/DJF), 2023 WL 8850243, at *8 (D. Minn. Dec. 21, 2023) (same); *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (same).

Courts have allowed these claims to proceed despite the more rigorous federal pleading standards and the highly technical definitions under the federal Wiretap Act—neither of which are implicated by the WPA. *See Roden*, 179 Wn.2d at 905 (highlighting that "[t]he federal statute defines terms with greater technical specificity," whereas "[t]he Washington statute does not include technical definitions . . . and [the Court has] consistently interpreted its terms broadly"); *McCurry v. Chevy*

Chase Bank, FSB, 169 Wn.2d 96, 102-03 (2010) (rejecting *Twombly/Iqbal* pleading standard).

Similarly, multiple courts have allowed claims related to the Meta Pixel on healthcare providers' websites to move forward under California's Invasion of Privacy Act ("CIPA") and other state wiretap statutes. *See Toy v. Life Line Screening of Am. Ltd.*, No. 23-CV-04651-RFL, 2024 WL 1701263, at *1 (N.D. Cal. Mar. 19, 2024) (finding that allegations that Life Line "aided Google and Facebook in intercepting users' interactions with Life Line's website, including her private health information, by installing Pixel and Google Analytics on its website," stated a claim under CIPA); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1080 (N.D. Cal. 2023) (denying motion to dismiss CIPA claim based on Meta's interception of health information from hospital websites through Meta Pixel); *Cousin v. Sharp Healthcare*, No. 22-CV-2040-MMA-DDL, 2023 WL 8007350, at *5 (S.D. Cal. Nov. 17, 2023) (denying

motion to dismiss CIPA claim based on use of Meta Pixel on hospital website); *W.W. v. Orlando Health, Inc.,* No. 6:24-CV-1068-JSS-RMN, 2025 WL 722892, at *6 (M.D. Fla. Mar. 6, 2025) (denying motion to dismiss under Florida Security of Communications Act where healthcare organization installed Meta Pixel on website); *Doe v. Post Acute Med., LLC*, No. 1:24-CV-547, 2025 WL 511069, at *5 (M.D. Pa. Feb. 14, 2025) (denying motion to dismiss under Pennsylvania's Wiretapping and Electronic Surveillance Control Act where health care provider installed Meta Pixel and other tracking tools on website). Indeed, a federal jury in California recently found Meta liable under CIPA for its role in tracking the activity of users on a mobile health app.[3]

In sum, courts around the country applying the federal Wiretap Act and other state wiretap statutes have found claims

[3] https://www.cnbc.com/2025/08/07/jury-rules-meta-violated-law-in-period-tracking-app-data-case.html

viable based on the same fact pattern presented in this case. As "one of the most restrictive electronic surveillance laws ever promulgated," *Roden*, 179 Wn.2d at 898, the WPA at a minimum should provide equal protection to Washington residents against non-consensual interceptions of their health-related communications.

B. The WPA is Interpreted Broadly to Protect Washington Residents as Communications Technology Evolves

Washington State "has a long history of statutory protection of private communications and conversations." *State v. Clark*, 129 Wn.2d 211, 222, 916 P.2d 384 (1996). "Since 1909, the privacy act [] protected sealed messages, letters, and telegrams from being opened or read by someone other than the intended recipient." *Christensen*, 153 Wn.2d at 198. Then, "[i]n 1967, the legislature amended the act in order to keep pace with the changing nature of electronic communications and in

recognition of the fact that there was no law that prevented eavesdropping." *Id.*

Since 1967, this Court has repeatedly interpreted the WPA broadly to stay current with technological innovation. The Court has explained that it "must interpret the privacy act in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape," and that "[t]his must be done so as to ensure that new technologies cannot be used to defeat the traditional expectation of privacy." *Christensen*, 153 Wn.2d at 197; *see also Faford*, 128 Wn.2d at 485–86 ("The sustainability of our broad privacy act depends on its flexibility in the face of a constantly changing technological landscape."); *State v. Hinton*, 179 Wn.2d 862, 872, 319 P.3d 9 (2014) ("[T]his court has consistently extended statutory privacy in the context of new communications technology, despite suggestions that we should reduce the protections because of the possibility of intrusion.").

Thus, when faced with a new communications technology that did not exist in 1967, this Court interprets the WPA in a flexible, non-technical manner that furthers the WPA's broad underlying purpose of protecting the privacy of communications. *See Roden*, 179 Wn.2d at 906.

In *Faford*, for example, the Court rejected the trial court's narrow definition of the term "transmit" in the WPA and instead interpreted the statute consistent with the "breadth of the act's purpose" in holding that the WPA protects against the use of a police scanner to intercept communications over a cordless telephone. *Faford*, 128 Wn.2d at 483. Similarly, in *Roden*, the Court held that the WPA protects private communications via text messages despite the "possibility that an unintended party can intercept a text message due to his or her possession of another's cell phone." *Roden*, 179 Wn.2d at 901. In *Townsend*, the Court likewise concluded that email and instant messages

were protected under the WPA even though "interception of [the] messages was a possibility." *Townsend*, 147 Wn.2d at 674.

In today's digital age, web communications are increasingly the default method for navigating day-to-day activities. In 1967, a person seeking information from their medical provider about health conditions, symptoms, or physician availability might pick up a landline phone and speak directly with a hospital employee. Today, those communications occur over the internet, with individuals going to their medical provider's website.

Recognizing this fact, courts across the country have applied federal and state wiretap statutes to safeguard the privacy of an individual's website communications, even beyond the healthcare context. *See Brown v. Google LLC*, 685 F. Supp. 3d 909, 936 (N.D. Cal. 2023) (observing that "URLs, by virtue of including the particular document within a website that a person views . . . divulge a user's personal interests, queries, and habits"

and are protected from interception under the federal wiretap statute); *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) [of CIPA] applies to Internet communications.").

"[T]o keep pace with the changing nature of electronic communications," *Christensen*, 153 Wn.2d at 198, this Court should grant review to clarify that the WPA protects against unknown third parties eavesdropping on the web communications of Washington residents. *See Faford*, 128 Wn.2d at 486 ("This type of intentional, persistent eavesdropping on another's private affairs personifies the very activity the privacy act seeks to discourage.").

C. The Court of Appeals' Highly Technical and Narrow Interpretation of the WPA Conflicts with this Court's WPA Jurisprudence

Despite guidance from this Court that (1) lower courts should interpret the WPA broadly to effectuate its purpose of

safeguarding the privacy of communications as technology evolves, (2) the WPA's terms are flexible and non-technical, and (3) the WPA provides considerably more protection than the federal Wiretap Act, the Court of Appeals here imposed a highly technical and narrow interpretation of the WPA in a manner that renders the WPA considerably *less* protective than the federal Wiretap Act and other state wiretap statutes. This Court should grant review to clarify that the WPA, like other wiretap statutes, provides protection to Washington residents against unwanted corporate surveillance online.

To state a claim under the WPA, a plaintiff must show that "(1) a private communication [was] transmitted by a device, which was (2) intercepted or recorded by use of (3) a device designed to record and/or transmit (4) without the consent of all parties to the private communication." *Roden*, 179 Wn.2d at 899.

The Court of Appeals reached only the first element under the WPA and concluded that Petitioners failed to allege that their

online interactions with SCH through the website constituted "communications."

The WPA prohibits the interception of a "private *communication* transmitted by a telephone, telegraph, radio, or other device." RCW 9.73.030(1)(a) (emphasis added). The WPA does not define "communication," but this Court has observed that "[a] nontechnical statutory term may be given its dictionary meaning," consistent with the WPA's "legislative intent to safeguard the private conversations of citizens from dissemination in any way." *State v. Smith*, 189 Wn.2d 655, 662, 405 P.3d 997 (2017). This Court has stated that "[t]he ordinary meaning of 'communication' is "the act . . . of imparting or transmitting' or 'facts or information communicated.'" *State v. Riley*, 121 Wn.2d 22, 33, 846 P.2d 1365 (1993) (quoting Webster's Third New International Dictionary 460 (1986)); *see also* Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/communication

(last visited Sept. 6, 2025) (defining "communication," as "a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior," or "information transmitted or conveyed").

In interpreting the WPA, this Court has eschewed narrow, hyper-technical approaches that run contrary to the WPA's purpose of protecting private communications. *See Faford*, 128 Wn.2d at 483-84 ("As Defendants point out, the trial court selectively chose the narrowest definitions of 'transmit' available. In light of the breadth of the act's purpose, we prefer Defendants' alternative definitions from Webster's Third New International Dictionary, such as 'disseminate' or 'communicate.'"); *Roden*, 179 Wn.2d at 905--06 (explaining that, unlike the federal wiretap statute, the WPA "does not include technical definitions or independent provisions for stored communications, and we have consistently interpreted its terms broadly").

The broad scope of the term "communication" under the WPA is evident when comparing the WPA to the federal Wiretap Act and other state wiretap statutes. For example, the federal Wiretap Act and CIPA are narrower and only protect against the interception of "contents." Under the federal Wiretap Act, "'the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication.'" *Walgreen*, 2024 WL 2263395, at *16 (quoting *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)). "URLs which disclose search terms that reveal website users' personal interests, queries, and habits are 'contents' of communications under CIPA and [the federal Wiretap Act]." *Id.* (citation modified). "So, too, are search queries such as those for 'specialty healthcare providers and treatments for medical conditions.'" *Id.* (quoting *Cousin*, 2023 WL 8007350, at *5).

The WPA sweeps broader than the federal Wiretap Act and CIPA and protects against the interception of even *non-content* record data. For example, in *Gunwall*, the Court held that a pen register, which records outgoing telephone dialing information but not the actual *contents* of the calls, had unlawfully intercepted a "communication." *See Gunwall*, 106 Wn.2d at 69.

Despite the WPA's broader scope, Petitioners alleged in their Complaint that they communicated substantive content regarding health conditions, symptoms, and physicians—thus meeting the stricter requirement for "contents" under the federal Wiretap Act. CP 5-7, ¶¶ 15-17. The Complaint also detailed how substantive search queries on the SCH website related to "depression," "suicide," and "eating disorders" are intercepted by Meta and linked to the particular individual who transmitted the communications. CP 17-18, 23-26, ¶¶ 59-62, 79-82. Courts applying the federal Wiretap Act and CIPA routinely find that

the same allegations satisfy the "contents" requirements under those statutes. *See, e.g., Castillo*, 2024 WL 4785136, at *5, * 10.

Because the WPA provides more protection than the federal Wiretap Act (and presumably more than CIPA given this Court's view that the WPA is among the *most* protective wiretap statutes ever), it should follow that satisfying the "content" element under those statutes would easily satisfy the "communication" element under WPA. But the Court of Appeals found otherwise. According to the Court of Appeals:

> plaintiffs' complaint did not allege that they navigated SCH's public website to transmit a message to or exchange information with another party. Rather, they merely allege to have clicked and entered search terms to retrieve publicly displayed information and webpages. Distinguishable from 'back-and-forth' messaging that is plainly protected by the act, SCH's alleged interception of plaintiffs' click-and-search activity did not affect other parties or involve multiple invasions of privacy. Because plaintiffs do not plead facts to establish that communication occurred on SCH's public website under the plain terms of RCW 9.73.030(1)(a), we conclude their claim must fail.

The Court of Appeals' decision misses the mark on both the law and the facts. First, by defining "communication" to only mean "back-and-forth messaging" that affects "other parties or involve[s] multiple invasions of privacy," the court drastically narrowed the scope of the WPA, making the "communication" element even more strict than the "contents" requirement under the federal Wiretap Act and CIPA, neither of which demand "back-and-forth messaging" to trigger a violation. By "selectively cho[osing] the narrowest definition[] of ['communication'] available," the Court of Appeals failed to account for "the breadth of the [WPA's] purpose,"—namely, to protect the privacy of communications as technology evolves. *Faford*, 128 Wn.2d at 483, 486.

Further, to say that Petitioners merely engaged in "click-and-search" activity ignores the substantive content relayed by a consumer taking such actions on the SCH website. In the same way that "thumb movements" on a cell phone or "finger strokes"

on a keyboard can convey the content of a message, clicking on the "Eating Disorders" webpage or typing the word "depression" into the SCH website search bar—all of which was intercepted by Meta—necessarily involved "transmit[ing]" or "convey[ing]" "information," and therefore constituted a "communication." *See* Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/communication (last visited Sept. 6, 2025); *see also Walgreen*, 2024 WL 2263395, at *16 (observing that "URLs which disclose search terms that reveal website users' personal interests, queries, and habits are 'contents' of communications under [CIPA] and [the federal Wiretap Act]") (citation modified).

The Court of Appeals decision cannot be squared with this Court's WPA precedents. Either the WPA is among the most protective wiretap statutes in the country and provides significantly more protection than the federal Wiretap Act—as this Court has repeatedly emphasized—or, as the Court of

Appeals found, the WPA provides considerably *less* protection than the federal Wiretap Act and other state wiretap statutes. Because the Court of Appeals decision is irreconcilable with this Court's prior interpretation of the WPA, this Court should grant review to clarify the act's proper scope.

D. Whether the WPA Applies to Web-Based Communications is an Issue of Substantial Public Interest

At least two federal courts have recognized the need for this Court to offer guidance on the WPA's proper scope in the context of web-based communications. *In re Meta Pixel Tax Filing Cases*, No. 22-CV-07557-PCP, 2024 WL 1251350, at *8 (N.D. Cal. Mar. 25, 2024) (noting the absence of "a relevant construction of the Washington Privacy Act by the Washington Supreme Court or any Washington Court of Appeals," in the context of web-based communications); *Castillo*, 2024 WL 4785136, at *9, n.6 (observing the lack of "clear authority from Washington courts" on whether the WPA applies to

communications with a company via the company website but noting that the parties could "move to certify a question to the Washington Supreme Court").

In today's digital age, much of a person's interactions with the outside world occur over the internet through web-based communications. Indeed, this case presents just one example of the type of online communications that millions of Washington residents engage in every day. Whether the WPA has any role in preventing online surveillance of such activities presents an issue of substantial public interest that warrants this Court's review.

VII. CONCLUSION

Because the decision of the Court of Appeals conflicts with this Court's WPA precedents, and the proper scope of the WPA presents an issue of substantial public interest, review is warranted under RAP 13.4(b)(1) and (4).

I certify that this memorandum contains 4,968 words, in compliance with the Rules of Appellate Procedure.

DATED this 17th day of September, 2025.

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Rebecca L. Solomon*
Kim D. Stephens, P.S. WSBA #11984
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
kstephens@tousley.com
csolomon@tousley.com

Ryan J. Ellersick, WSBA # 43346
ZIMMERMAN REED LLP
14648 North Scottsdale Rd., Ste. 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
ryan.ellersick@zimmreed.com

Certificate of Service

I hereby certify that on the 17th day of September, 2025, I caused to be served true and correct copies of the foregoing to all parties registered via Court of Appeals Efiling system.

I certify under penalty of perjury under the laws of the United States and the state of Washington that the foregoing is true and correct.

s/Linsey M. Teppner
Linsey M. Teppner, Legal Assistant

TOUSLEY BRAIN STEPHENS PLLC

September 17, 2025 - 3:35 PM

Transmittal Information

Filed with Court:	Court of Appeals Division I
Appellate Court Case Number:	86461-1
Appellate Court Case Title:	Carly Baker, Et Al, Appellant v. Seattle Childrens Hospital, Respondent

The following documents have been uploaded:

- 864611_Other_20250917153415D1079158_8061.pdf
  This File Contains:
  Other - Appendix to Petition for Review
  The Original File Name was 2025.09.17 - Appendix to Petition for Review.pdf
- 864611_Petition_for_Review_20250917153415D1079158_0166.pdf
  This File Contains:
  Petition for Review
  The Original File Name was 2025.09.17 - Petition for Review.pdf

A copy of the uploaded files will be sent to:

- FredBurnside@dwt.com
- astanton@tousley.com
- francescareifer@dwt.com
- kstephens@tousley.com
- lisamerritt@dwt.com
- lteppner@tousley.com
- megangalloway@dwt.com
- mpeterson@tousley.com
- rachelherd@dwt.com
- ryan.ellersick@zimmreed.com

Comments:

Sender Name: Linsey Teppner - Email: lteppner@tousley.com
Filing on Behalf of: Rebecca Luise Solomon - Email: rsolomon@tousley.com (Alternate Email: lteppner@tousley.com)

Address:
1200 Fifth Avenue
Suite 1700
Seattle, WA, 98101
Phone: (206) 682-5600

Note: The Filing Id is 20250917153415D1079158

No. 86461-1

IN THE COURT OF APPEALS, DIVISION ONE
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.

APPENDIX TO PETITION FOR REVIEW

Kim D. Stephens
Rebecca L. Solomon
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue,
Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600

Ryan J. Ellersick
ZIMMERMAN REED LLP
14648 North Scottsdale Rd.,
Ste. 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400

Attorneys for Petitioners

No.	Document	Page
1.	Unpublished Opinion on Appeal	R-001

DATED this 17th day of September, 2025.

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Rebecca L. Solomon*
Kim D. Stephens, P.S. WSBA #11984
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
kstephens@tousley.com
csolomon@tousley.com

Ryan J. Ellersick, WSBA # 43346
ZIMMERMAN REED LLP
14648 North Scottsdale Rd., Ste. 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
ryan.ellersick@zimmreed.com

Certificate of Service

I hereby certify that on the 17th day of September, 2025, I caused to be served true and correct copies of the foregoing to all parties registered via Court of Appeals Efiling system.

I certify under penalty of perjury under the laws of the United States and the state of Washington that the foregoing is true and correct.

s/Linsey M. Teppner
Linsey M. Teppner, Legal Assistant

FILED
8/18/2025
Court of Appeals
Division I
State of Washington

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

CARLY BAKER, JANSSEN RAMOS SAVOIE, AND AMBER SHAVIES, individually, and on behalf of those similarly situated, Appellants, v. SEATTLE CHILDREN'S HOSPITAL, a Washington nonprofit corporation, Respondent.	No. 86461-1-I DIVISION ONE UNPUBLISHED OPINION

COBURN, J. — Plaintiffs filed a putative class action lawsuit against Seattle Children's Hospital (SCH), alleging in part that SCH used third-party technology to intercept their activities on SCH's public website in violation of Washington's privacy act, chapter 9.73 RCW. The trial court dismissed the plaintiffs' complaint for failure to state a claim under CR 12(b)(6). We affirm.

FACTS

SCH owns and controls the public website www.seattlechildrens.org.[1] The website allows visitors to search for information about medical conditions, health care providers, and services. SCH uses Meta Platforms, Inc.'s "Pixel" software code on its

[1] The facts are taken from the allegations in plaintiffs' complaint. When reviewing a trial court's dismissal under CR 12(b)(6), we presume that the complaint's factual allegations are true. Jackson v. Quality Loan Serv. Corp., 186 Wn. App. 838, 843, 347 P.3d 487 (2015).

public website. Pixel is designed to track website user activity by capturing how visitors interact with the website, including clicks, text searches, page views, and the webpage addresses that the user visits. SCH uses the information to support its advertising efforts.

Pixel, as used by SCH, also shares the tracked data with Meta. This data is often linked with the individual website user's Meta-owned Facebook account. "Meta uses both first- and third-party cookies[2] in Pixel to link Facebook IDs and Facebook profiles, and [SCH] sends these identifiers to Meta." For example, if the website user is logged into their Facebook account when they visit SCH's public website, Pixel sends third-party cookies to Meta. The cookies allow Meta to link website activity data collected by Pixel to the user's unique Facebook account. Even if the website user does not have a Facebook account or is not logged in to Facebook when browsing SCH's public website, Pixel transmits the user's website activity to Meta with a unique identifier associated with a cookie that Meta can use to link the user's activity with their current or later-created Facebook account. After linking user's website activity to a specific Facebook account, Meta can use that information for its own targeted advertising purposes.

In October 2023 plaintiffs Carly Baker, Janssen Ramos Savoie, and Amber Shavies filed a putative class action against SCH, alleging in part that SCH violated RCW 9.73.030(1)(a) of Washington's privacy act by intentionally deploying Pixel on the

[2] The complaint defines "cookies" as "a text file that website operators and others use to store information on the website visitor's device," which can be later communicated to a server. When a user visits one website, "third-party cookies" store and communicate data to an entirely different website. "First-party cookies" are created by the website the user is visiting.

hospital's website to secretly intercept and record their sensitive health information.[3] See ch. 9.73 RCW. Plaintiffs defined the intercepted and recorded website activity as including an HTTP request, which

> is an electronic communication a website visitor sends from her device's browser to the website's server. … In this case, a patient's HTTP Request would be asking [SCH's] Website to get certain information, such as a list of urgent clinic locations or health care providers with a particular specialization.
>
> …
>
> A [website] user's HTTP Request essentially asks [SCH's] Website to retrieve certain information (such as the "Find a Provider or Researcher" webpage). [An] HTTP Response then renders or loads the requested information in the form of … pages, images, words, buttons, and other features that appear on the patient's screen as they navigate [SCH's] Website.

Specifically, Baker used SCH's public website to search for medical conditions and symptoms on behalf of her minor daughter, including using the website's search bar and conditions webpage. Savoie used the website to search for information on medical conditions, symptoms, and health care providers for her minor son by using the website's search bar and "Find A Doctor" webpage. Shavies searched on the website for operating hours for urgent care facilities. Plaintiffs did not expect their website activity to be shared with third parties without their express consent. Each of the

[3] Plaintiffs defined the proposed class as, "All individuals residing in Washington whose Sensitive Information was disclosed to a third party through [SCH's] Website without authorization or consent during the Class Period." The complaint defines "Sensitive Information" as "patients' and prospective patients' highly sensitive Personal Health Information ('PHI') and Personally Identifiable information ('PII')."

In their complaint, the plaintiffs collectively refer to SCH's public website at www.seattlechildrens.org and its "patient portal" at seattlechildrens.org/patients-families/mychart/ as the "Website." Plaintiffs, however, limit their appeal to the trial court's dismissal of their privacy act claim regarding plaintiffs' alleged use of SCH's public website at www.seattlechildrens.org. We recite facts in the plaintiffs' complaint accordingly.

plaintiffs had a Facebook and/or Instagram[4] account when they used SCH's public website. Some plaintiffs recall receiving health-related advertisements on Facebook after using SCH's website, including advertisements "related to specific symptoms communicated to" SCH on the website."[5]

SCH acknowledges the use of cookies on its website with a pop-up that appears "upon navigating to [SCH's] website," which states,

> By clicking 'Accept All Cookies,' you agree to the storing of cookies on your device to enhance site navigation, analyze site usage and assist in marketing efforts. For more information, see Website Privacy [link].

In January 2024 SCH moved to dismiss plaintiffs' lawsuit for failure to state a claim under CR 12(b)(6). Plaintiffs filed a response, to which SCH replied. After the trial court held a hearing in February, the court granted SCH's 12(b)(6) motion and dismissed plaintiffs' complaint with prejudice.[6]

Plaintiffs appeal.

DISCUSSION

Standard of Review

Plaintiffs argue that the trial court erred by dismissing their claim under Washington's privacy act, chapter 9.73 RCW. We review de novo an order granting a motion to dismiss under CR 12(b)(6). FutureSelect Portfolio Mgmt., Inc. v. Tremont Grp.

[4] The complaint states that Instagram is a social media company owned by Meta.

[5] As a result of SCH's alleged use of Pixel in violation of the privacy act, plaintiffs asserted that they and putative class members were injured by the "interference with their control over their personal data, intrusion into their private affairs, the highly offensive publication of private facts, and other losses of privacy related to the secret interception and disclosure of their private and sensitive health information."

[6] The trial court also dismissed plaintiffs' claims under Washington's Consumer Protection Act, chapter 19.86 RCW; Washington's Uniform Healthcare Information Act, chapter 70.02 RCW; as well as plaintiffs' invasion of privacy, breach of implied contract, conversion, and unjust enrichment claims. Plaintiffs limit their appeal to their claim under the privacy act.

Holdings, Inc., 180 Wn.2d 954, 962, 331 P.3d 29 (2014).

A CR 12(b)(6) motion challenges the legal sufficiency of the allegations in the complaint. McAfee v. Select Portfolio Servicing, Inc., 193 Wn. App. 220, 226, 370 P.3d 25 (2016). The rule "weeds out complaints where, even if what the plaintiff alleges is true, the law does not provide a remedy." McCurry v. Chevy Chase Bank, FSB, 169 Wn.2d 96, 102, 233 P.3d 861 (2010). "Dismissal under CR 12(b)(6) is appropriate in those cases where the plaintiff cannot prove any set of facts consistent with the complaint that would entitle the plaintiff to relief."[7] Jackson, 186 Wn. App. at 843. In considering a motion to dismiss under CR 12(b)(6), we take all facts alleged in the complaint as true. FutureSelect Portfolio Mgmt., Inc., 180 Wn.2d at 962. Though we may consider hypothetical facts, "'[i]f a plaintiff's claim remains legally insufficient even under his or her proffered hypothetical facts, dismissal pursuant to CR 12(b)(6) is appropriate.'" Id. at 963 (alteration in original) (quoting Gorman v. Garlock, Inc., 155 Wn.2d 198, 215, 118 P.3d 311 (2005)). We must determine whether the plaintiffs can prove any set of facts, consistent with their complaint,[8] that would entitle them to relief. Orwick v. City of Seattle, 103 Wn.2d 249, 254, 692 P.2d 793 (1984).

Washington privacy act, chapter 9.73 RCW

Washington's privacy act protects private communication and conversation.

[7] A court may dismiss a petitioner's claim under CR 12(b)(6) for "failure to state a claim upon which relief can be granted."

[8] Plaintiffs incorrectly assert that a court must consider whether all possible facts could sustain a claim for relief, including hypothetical facts that are not pleaded in the complaint. The cases that plaintiff cites do not stand for this proposition. See Burton v. Lehman, 153 Wn.2d 416, 422, 103 P.3d 1230 (2005); Halvorson v. Dahl, 89 Wn.2d 673, 674-75, 574 P.2d 1190 (1978); McCurry, 169 Wn.2d at 102. While a court may consider hypothetical facts outside of the record when ruling on a CR 12(b)(6) motion, see Haberman v. Wash. Pub. Power Supply Sys., 109 Wn.2d 107, 120, 744 P.2d 1032 (1987), a court may generally not go beyond the face of the pleadings. Jackson,186 Wn. App. at 844.

RCW 9.73.030. One of the most restrictive electronic surveillance laws in the nation, "[t]he act prohibits anyone not operating under a court order from intercepting or recording certain communications without the consent of all parties."[9] State v. Roden, 179 Wn.2d 893, 898, 321 P.3d 1183 (2014) (citing RCW 9.73.030, .040, .090(2)); State v. Faford, 128 Wn.2d 476, 481, 910 P.2d 447 (1996). The act provides in relevant part:

> it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any … [p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals ... without first obtaining the consent of all the participants in the communication[.]

RCW 9.73.030(1)(a).[10] Violation of this provision may result in both civil and criminal liability. RCW 9.73.060, .080.

A violation of the privacy act requires "(1) a private communication transmitted by a device, which was (2) intercepted or recorded by use of (3) a device designed to record and/or transmit (4) without the consent of all parties to the private communication." Roden, 179 Wn.2d at 899 (citing Christensen, 153 Wn.2d at 192) (citing RCW 9.73.030).

Communication

Plaintiffs assert that their click-and-search activity on SCH's public website constitutes "private communication" under RCW 9.73.030(1)(a). Because plaintiffs' alleged navigation of SCH's public website is not "communication" as contemplated by

[9] The Washington Supreme Court observed that "[a]rguably, the most significant piece of evidence about the extent to which the legislature intended to restrict eavesdropping is the all-party consent requirement." State v. Christensen, 153 Wn.2d 186, 198 n.3, 102 P.3d 789 (2004) (citing RCW 9.73.030).

[10] This opinion cites to decisions that refer to prior versions of RCW 9.73.030. Throughout its various amendments, the relevant language of the statute has remained the same.

the privacy act, we reject plaintiffs' argument.

In determining the meaning of a statutory phrase, the fundamental goal is to give effect to the legislature's intent. Kadoranian v. Bellingham Police Dep't, 119 Wn.2d 178, 185, 829 P.2d 1061 (1992). A statute's meaning that is clear from its plain language is not subject to judicial construction. State v. Sullivan, 143 Wn.2d 162, 175, 19 P.3d 1012 (2001). Courts may determine the plain meaning of a nontechnical statutory term that is undefined in the statute from its dictionary definition. HomeStreet, Inc. v. Dep't of Revenue, 166 Wn.2d 444, 451, 210 P.3d 297 (2009); Columbia Riverkeeper v. Port of Vancouver USA, 188 Wn.2d 421, 435, 395 P.3d 1031 (2017).

Because the privacy act does not define "private communication," our state Supreme Court has adopted the dictionary definition for "communication." State v. Riley, 121 Wn.2d 22, 33, 846 P.2d 1365 (1993). Under RCW 9.73.030(1)(a), communication is "'the act ... of imparting or transmitting' or 'facts or information communicated.'" Id. (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 460 (1986)).[11]

In Riley, the Supreme Court held that a line trap that traced computer hacking activity to Riley's home did not record communication under the terms of RCW 9.73.030(1)(a) because the line trap merely recorded Riley's phone number rather than an exchange of information from one party to another party. Id. at 32-34. The court distinguished the information discovered by the line trap from a pen register's discovery of the dialing of one telephone number to another as contemplated in its decision in

[11] The state Supreme Court has also interpreted the plain meaning of "private" according to its dictionary definition of "'belonging to oneself ... secret ... intended only for the persons involved <a ~ conversation> ... holding a confidential relationship to something ... a secret message: a private communication ... secretly: not open or in public.'" State v. Kipp, 179 Wn.2d 718, 729, 317 P.3d 1029 (2014) (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1804-05 (1969), quoted in State v. Clark, 129 Wn.2d 211, 224-25, 916 P.2d 384 (1996)).

State v. Gunwall, 106 Wn.2d 54, 720 P.2d 808 (1986), stating:

> In Gunwall, this court held that a pen register records a "private communication" under RCW 9.73. … Although a pen register does not intercept spoken words, it does record an exchange of information—the dialing from one telephone number to another. A pen register is thus "comparable in impact to electronic eavesdropping devices in that it … may affect other persons and can involve multiple invasions of privacy". In contrast, all that is learned from a tracer is the telephone number of one party, the party dialing. A pen register may therefore be reasonably viewed as recording a "private communication", whereas a tracer may not.

Id. at 34 (emphasis added) (second alteration in original) (citation omitted) (quoting Gunwall, 106 Wn.2d at 69).

In State v. Wojtyna, we applied the Riley court's reasoning to the display of Wojtyna's phone number on a suspected drug dealer's pager that Wojtyna contacted. 70 Wn. App. 689, 694-96, 855 P.2d 315 (1993). Upon the suspected dealer's arrest, police seized the pager and monitored it for incoming calls. Id. at 691. After the pager received an incoming call, a detective called the phone number and arranged a meeting with Wojtyna for an undercover drug deal. Id. Like in Riley, "all that was learned from the pager was the telephone number of one party, the party dialing." Id. at 695. Because the interception of the telephone number did not affect other parties, involve multiple invasions of privacy, or record the exchange of information, we concluded the display of the telephone number did not establish communication under the privacy act. Id. (citing Riley, 121 Wn.2d at 33-34).

In Roden, the Supreme Court considered whether Roden's text messages to an alleged drug dealer's cell phone constituted private communications under the act. 179 Wn.2d at 896-97, 899-03. The court discussed Wojtyna and observed that "a simple informational statement that is sent to a pager'' is distinguishable from "back-and-forth"

text messaging, which is "much more like e-mail exchanges and telephone calls" and is plainly protected by the privacy act.[12] Id. at 901; see also State v. Smith, 85 Wn.2d 840, 846, 540 P.2d 424 (1975) ("We are convinced that the events here involved do not comprise 'private conversation' within the meaning of the statute. Gunfire, running, shouting, and … screams do not constitute 'conversation' within that term's ordinary connotation of oral exchange, discourse, or discussion.").[13]

Plaintiffs assert that we should broadly interpret the privacy act to include their navigation of SCH's public website, citing to our Supreme Court's instruction that courts "must interpret the privacy act in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape." Christensen, 153 Wn.2d at 197. This mandate pertains to evolving technology used to record or intercept conversation or communication protected by the act, see Christensen, 153 Wn.2d at 197-98, as well as technology that is used to communicate. See Faford, 128 Wn.2d at 485-86; Roden, 179 Wn.2d at 901-03. Nonetheless, a communication must occur to support a viable claim under RCW 9.73.030(1)(a).[14] Plaintiffs offer no authority to support their broader interpretation of

[12] Notably, the test for determining whether "[a] communication is private" under the privacy act indicates that a communication requires an exchange of information from one party to another recipient party. See Kipp, 179 Wn.2d at 729. Private communication is "(1) when [the] parties manifest a subjective intention that it be private and (2) where that expectation is reasonable." Id. "A communication is not private where anyone may turn out to be the recipient of the information or the recipient may disclose the information." Clark, 129 Wn.2d at 227 (citing Wojtyna, 70 Wn. App. at 695-96); see also, e.g., Kadoranian, 119 Wn.2d at 189-91 (holding that brief conversation regarding general information that was "inconsequential, non-incriminating and made to a stranger" is "not the kind of communication that the privacy act protects").

[13] The court in Smith considered the former "private conversation" provision of the privacy act, which is identical in wording to the current version. Compare former RCW 9.73.030(2) (1967) with RCW 9.73.030(1)(b). The same applies to the "private communication" provision. Compare former RCW 9.73.030(1) (1967) with RCW 9.73.030(1)(a).

[14] Plaintiffs also cite the rule that "[w]hen an area of the law involved is in the process of development, courts are reluctant to dismiss an action on the pleadings alone by way of a CR

communication under the privacy act.[15] See DeHeer v. Seattle Post-Intelligencer, 60 Wn.2d 122, 126, 372 P.2d 193 (1962) ("Where no authorities are cited in support of a proposition, the court is not required to search out authorities, but may assume that counsel, after diligent search, has found none."). We are otherwise controlled by the definition that our Supreme Court adopts in Riley. State v. Gore, 101 Wn.2d 481, 487 681 P.2d 227 (1984) (stating that once the Washington Supreme Court "has decided an issue of state law, that interpretation is binding on all lower courts until it is overruled by [the state Supreme Court]").

In the present case, plaintiffs' complaint did not allege that they navigated SCH's public website to transmit a message to or exchange information with another party. Rather, they merely allege to have clicked and entered search terms to retrieve publicly displayed information and webpages. Distinguishable from "back-and-forth" messaging that is plainly protected by the act, SCH's alleged interception of plaintiffs' click-and-search activity did not affect other parties or involve multiple invasions of privacy. See Roden, 179 Wn.2d at 901-02. Because plaintiffs do not plead facts to establish that communication occurred on SCH's public website under the plain terms of RCW

12(b)(6) motion." Haberman, 109 Wn.2d at 120. Plaintiffs cite to Bravo v. Dolsen Cos., 125 Wn.2d 745, 751, 888 P.2d 147 (1995), wherein the court held that dismissal under CR 12(b)(6) was "inappropriate ... because there is no prior state court decision setting forth the elements of [the claim]." Because the elements of a privacy act claim are well-established, Bravo is inapposite. See, e.g., Roden, 179 Wn.2d at 899-906 (discussing elements).

[15] Plaintiffs cite federal and foreign state court decisions for discussions of the federal wiretap statute, 18 U.S.C. §§ 2510-2522, and other state privacy acts or wiretap statutes. We do not find these non-binding decisions persuasive on this issue of Washington law. See Brown v. Old Navy, LLC, No. 102592-1, slip op. at 5 (Wash. Apr. 17, 2025), https://www.courts.wa.gov/opinions/pdf/1025921.pdf; West v. Thurston County, 168 Wn. App. 162, 183 n.22, 275 P.3d 1200 (2012) (citing State v. Lord, 161 Wn.2d 276, 289, 165 P.3d 1251 (2007)); see also Gore, 101 Wn.2d at 487 (stating that once our state Supreme Court "decide[s] an issue of state law, that interpretation is binding on all lower courts until it is overruled by [the Washington Supreme Court].").

9.73.030(1)(a), we conclude their claim must fail.

We acknowledge plaintiffs' concern regarding the privacy of health-related internet activity and privacy concerns related to web-based communications. Indeed, our sister division recently observed "that the laws in Washington demonstrate a public policy that recognizes there is value in the security of our personal information" and cites various statutes that regulate the handling of personal and health care information. Nunley v. Chelan-Douglas Health Dist., 32 Wn. App. 2d 700, 723-24, 558 P.3d 513 (2024). This includes the Washington My Health My Data Act, chapter 19.373 RCW, that requires "additional disclosures and consumer consent regarding the collection, sharing, and use of [health data]." RCW 19.373.005(3). But the issue before us is a narrow one related only to our state's privacy act. Further, our holding should not be read to definitively construe the application of the term "private communication" for all cases involving website or internet use. We confine our holding to the facts of this case and decide that the plaintiffs' alleged click-and-search navigation of SCH's public website does not fall within the statutory prohibition of RCW 9.73.030(1)(a).[16]

We affirm.

Coburn, J.

WE CONCUR:

Díaz, J.

[16] Because our holding is dispositive, we need not address other arguments raised by the parties that could be pertinent if the complaint involved a private communication.

TOUSLEY BRAIN STEPHENS PLLC

September 17, 2025 - 3:35 PM

Transmittal Information

Filed with Court:	Court of Appeals Division I
Appellate Court Case Number:	86461-1
Appellate Court Case Title:	Carly Baker, Et Al, Appellant v. Seattle Childrens Hospital, Respondent

The following documents have been uploaded:

- 864611_Other_20250917153415D1079158_8061.pdf
  This File Contains:
  Other - Appendix to Petition for Review
  The Original File Name was 2025.09.17 - Appendix to Petition for Review.pdf
- 864611_Petition_for_Review_20250917153415D1079158_0166.pdf
  This File Contains:
  Petition for Review
  The Original File Name was 2025.09.17 - Petition for Review.pdf

A copy of the uploaded files will be sent to:

- FredBurnside@dwt.com
- astanton@tousley.com
- francescareifer@dwt.com
- kstephens@tousley.com
- lisamerritt@dwt.com
- lteppner@tousley.com
- megangalloway@dwt.com
- mpeterson@tousley.com
- rachelherd@dwt.com
- ryan.ellersick@zimmreed.com

Comments:

Sender Name: Linsey Teppner - Email: lteppner@tousley.com
Filing on Behalf of: Rebecca Luise Solomon - Email: rsolomon@tousley.com (Alternate Email: lteppner@tousley.com)

Address:
1200 Fifth Avenue
Suite 1700
Seattle, WA, 98101
Phone: (206) 682-5600

Note: The Filing Id is 20250917153415D1079158