FILED
SUPREME COURT
STATE OF WASHINGTON
12/1/2025 2:13 PM
BY SARAH R. PENDLETON
CLERK

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,

Petitioners,

v.

SEATTLE CHILDREN'S HOSPITAL, a Washington nonprofit corporation,

Respondent.

ANSWER TO PETITION FOR REVIEW

Fred B. Burnside, WSBA #32491
Rachel Herd, WSBA #50339
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue Suite 3300
Seattle, WA 98104
Tel: 206.622.3150
fredburnside@dwt.com
rachelherd@dwt.com

Attorneys for Respondent
Seattle Children's Hospital

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

State Statutes

Rules

I. INTRODUCTION

This case does not present an issue meriting review under RAP 13.4. Petitioners ignore that the Court of Appeals relied almost entirely on decisions from this Court in reaching its holding and mischaracterize the breadth and import of the decision below. They suggest the Court of Appeals issued a decision limiting Washington's Privacy Act ("WPA") to one of "the *least* protective electronic surveillance laws in the country." Pet. at 1. Petitioners are wrong. The decision relies on *nine* WPA decisions from this Court spanning 42 years. Nor is there any substantial public interest at play, because the Court of Appeals "confine[d]" its narrow and unpublished ruling "to the facts of this case" and disclaimed any notion that any court or party could use the holding to "definitively construe the application of the term 'private communication' for all cases involving website or internet use." R-011. This Court should deny review of Division One's unpublished, narrow, and fact-bound ruling for the following reasons:

First, Division One's decision does not conflict with any ruling from this Court. Petitioners advance general concepts about privacy and the breadth of the WPA in an attempt to manufacture a conflict that does not exist. The Court of Appeals discussed the Washington cases Petitioners rely on and explained why they are consistent with its holding.

Second, the Court of Appeals' narrow ruling does not present an issue of substantial public importance. Division One's unpublished opinion is confined to the facts of this case, and the decision is not, as Petitioners suggest, a dramatic change in the law. As this Court has held, any statutory expansion "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.2d 255 (2002). And the legislature *has* separately addressed health-data privacy concerns—in a statute tailored to that issue—just not through the ill-suited state wire-tapping statute that is the WPA. *See, e.g.*, RCW 19.373.010.

II. RESTATEMENT OF THE ISSUES

Does Division One's holding conflict with relevant decisions from this Court, all of which the Court of Appeals discussed at length? RAP 13.4(b)(1)

Does Division One's narrow and unpublished holding, which is expressly confined to the facts of this case, and which the Court stated does *not* "definitively construe the application of the term 'private communication' for all cases involving website or internet use" present an issue of substantial public interest that this Court should determine? RAP 13.4(b)(4).

III. RESTATEMENT OF THE CASE

Petitioners spend much of their Statement of the Case discussing the Meta Pixel in the abstract and offering hypotheticals about what *could* happen if it were used nefariously on a different website (MyChart), to search for different facts (health-care related), for different people (themselves, rather than their children). In doing so, Petitioners ignore what actually *did* happen in this case.

Seattle Children's Hospital's ("SCH") Statement of the Case will open with facts about SCH's limited use of the Meta Pixel. Then, SCH will discuss Petitioners' actions, including their creation of Facebook accounts and interactions (or lack thereof) with the Pixel on SCH's website. Finally, SCH will summarize the Court of Appeals' narrow ruling.

A. Seattle Children's Hospital and its Website.

SCH is a not-for-profit hospital that provides top-ranking pediatric healthcare to children from across the nation. CP 7 (Compl. ¶ 22). SCH maintains a public-facing website at www.seattlechildrens.org. CP 2 (Compl. ¶ 2). The public website provides users with general information about health conditions, providers, clinic locations, hours of operation, etc. CP 18–19, 22–23, 25 (Compl. ¶¶ 63, 73, 79, 81). Its functionality is limited: visitors cannot (1) access medical records; (2) communicate with physicians or members of their care team; (3) schedule appointments; (4) access prescription information; or (5) access insurance information.

These more sensitive functions—directly relating to medical care—are accessible on a *different* website—the SCH patient portal, also called MyChart (www.mychart.seattlechildrens.org). CP 2 (Compl. ¶ 2) (recognizing patient portal is used to communicate about "medical histories, health care providers, medical conditions and treatments, medical search queries, and other highly sensitive data"); CP 154 (showing MyChart URL). SCH used Pixel on the generic, public-facing Website, www.seattlechildrens.org, ***but as Petitioners concede, it has never used Pixel on MyChart***. CP 1-2 (Compl. ¶¶ 1–3); Pet. 11–13; CP 73; CP 95, 123, 126–29; RP 25:14–16.

B. SCH Never Uses a Pixel on its Patient Portal.

Meta's Pixel ("Pixel") is a type of software code that can be placed on any website. R-001–2. It "is designed to track website user activity." *Id*. The Pixel uses "cookies"—small files stored on a user's browser—to operate. *Id.* Relevant here are two cookies: the "_fbp" cookie and the "c_user" cookie.

_fbp Cookie. When a user visits a website where the Pixel is installed, the website places the "_fbp" cookie onto the user's web browser. CP 13–14 (Compl. ¶ 46). The combination of the Pixel and the _fbp cookie allow a user's conduct on the website to be logged (e.g., mouse-clicks, page views, etc.). Petitioners concede that any information gathered through the _fbp cookie is anonymous. CP 3 (Compl. ¶ 4), CP 16 (Compl. ¶ 57) (conceding Meta Pixel cookie "did not reveal the identity of the … users"). In other words, use of the Pixel and placement of the _fbp cookie do ***not*** reveal the identity of any website viewer to Meta or SCH—only that some internet user clicked on certain webpages on the public website. CP 69 (conceding _fbp cookie "reveals only the device, not the identity of its user").

"C User" Cookie. The Complaint alleges that in some cases, Meta—*not* SCH—has the ability to link website conduct on SCH's public website to a user's Facebook account through the c_user cookie, which SCH has nothing to do with. CP 15–

16 (Compl. ¶¶ 53, 55). Each Facebook user is assigned a Facebook ID when creating a Facebook account, which is contained within the "c_user" cookie that Meta places on each Facebook user's device. *Id.* (Compl. ¶¶ 54–55). Petitioners complained that *if* Meta combines data from these two separate cookies, it "can" theoretically learn whether a Facebook user accessed the SCH public-facing website. *Id.* (Compl. ¶¶ 53, 55–56). But they concede that absent combining these cookies, for a user logged into Facebook on the same browser, Meta "do[esn't] know who th[e] person is." RP at 27:21.

C. Petitioners Used the Public Website Only for Basic Searching and Browsing.

Carly Baker, Amber Shavies, and Janssen Ramose Savoie filed this lawsuit in their individual capacities on behalf of a purported class. CP 5–7 (Compl. ¶¶ 14–17). Only three paragraphs in the 55-page complaint discuss the Petitioners' online conduct. *Id.* None of these Petitioners alleges that: (1) they are patients at SCH; (2) they are prospective patients of

SCH; (3) they input any of their own "sensitive information" into the public website; (4) they were logged into Facebook when they visited the public website (indeed, Petitioner Baker does not even allege she ever logged into Facebook); (5) any of their own sensitive information was anonymously shared with Meta; (6) Facebook associated any of their public website activity with their Facebook accounts; or (7) they suffered any tangible, specific injury as a result of the alleged sharing of their anonymous activity on the public website.

No Petitioner identified a single private communication with another person at SCH (or any communication they even intended for another person). Instead, they engaged in conduct directed at stored information on a static server.

Stripping away generic allegations about what others may have done, or what could be done on websites without the Pixel (e.g., MyChart), Petitioners allege very little:

Petitioner Baker. Petitioner Baker alleges she visited the public website using her "personal cell phone and

computer" and that she had a "Facebook and/or Instagram account." CP 5–6 (Compl. ¶ 15). She does not allege she was logged into either platform while visiting the public website. Petitioners conceded this point at oral argument on the motion to dismiss, explaining "we didn't allege facts that she was always logged in" because "she wasn't logged in—she may have been logged in, but we don't know." RP 28:1–10; 29:5–14. As a result, Ms. Baker does not allege facts sufficient to show the c_user cookie was placed on the browser she used to access the public website. Nor does she allege facts suggesting she shared private health information (PHI) on the public website. She alleges only that she (1) used the website's search bar and (2) viewed public articles regarding generic conditions she refuses to identify. CP 5–6 (Compl. ¶ 15); Pet. 11–12.

Petitioner Shavies. Petitioner Shavies's allegations are similarly thin. She alleges having a Facebook account and that she "generally remained logged into her account." CP 6 (Compl. ¶ 16). But as to website use, she alleges only that she

visited the public website to "locate urgent care facilities and identify their hours of operation." *Id.*

Petitioner Savoie. Petitioner Savoie alleges she had "a Facebook account and generally remained logged into her account." CP 6–7 (Compl. ¶ 17). Petitioner Savoie alleges she used the '"search' bar" and "Find A Doctor webpage." *Id.* Petitioner Savoie also alleges she "conducted searches on" undisclosed "medical conditions and symptoms." *Id.*

Petitioners' Complaint devoted a substantial portion of the three paragraphs to discussing their actions on MyChart—where the Pixel was ***not*** installed. For example, Petitioner Savoie alleges having "scheduled urgent care appointments," on the SCH website. *Id.* But that functionality is only available through MyChart. CP 128–29; *see also* RP 25:14–16 (conceding no Pixel information provided on MyChart). The Pixel does not exist on MyChart. No information provided or reviewed in MyChart is (or could be) shared with Meta.

Despite Petitioners' attempts to conflate the two, the distinction between the Website and MyChart is important. As both the HIPAA guidance and (now vacated) HHS advisory incorporated into Petitioners' Complaint explain, using tracking technologies on public websites (or what they term "unauthenticated websites") is a common practice because, as HHS confirmed in an article cited by Plaintiffs, "many unauthenticated webpages"—like SCH's here—"do not have access to individuals' [Private Health Information]," and thus "use of such tracking technologies is not regulated by the HIPAA Rules." CP 34 (Compl. ¶ 110 n.54) (citing https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html) (last visited November 26, 2025). It becomes potentially problematic solely when tracking technology is used on user-authenticated webpages—i.e., requiring a login with a username and a password—as with MyChart, which can contain PHI. *Id.*

The Complaint is short on factual allegations about ***these*** Petitioners and completely devoid of allegations about ***any*** SCH patient. On the facts alleged, SCH has no knowledge of any website viewer's, clicks and searches on its public website. CP 16 (Compl. ¶ 57) ("Meta does not reveal the identity of the matched Meta users" to the Website operator.).

Petitioners go to great length to distract from the core facts that (1) Pixel was never installed on the patient portal (MyChart); (2) Petitioners identify no PHI they shared on the Website; (3) Petitioners thus do not (and cannot) allege any of their private conduct was ever shared with Meta; and (4) under their theory, any logged-in Facebook users who choose to research any information they deem sensitive on any public website states a WPA claim—with potential criminal liability—if that data is anonymously transmitted to Meta.

D. Procedural History.

Plaintiffs originally filed a 55-page complaint in King County Superior Court on October 6, 2023, alleging seven state

law claims. CP 1–56. SCH moved to dismiss the case under CR 12(b)(6) for failure to state a claim. CP114–60. In response, Plaintiffs did not seek leave to amend, choosing to stand on their Complaint. After briefing and argument, Judge Jason Holloway granted the motion and dismissed with prejudice. CP 102–05 Shortly after, Petitioners appealed.

On appeal Petitioners abandoned six of their seven claims; challenging only the Superior Court's ruling on their WPA claim. *See* R-004 n.6. Division One affirmed. In its unpublished opinion, the court explained: (1) there are already "various statutes that regulate the handling of personal and health care information"; (2) based on the facts alleged, Petitioners' conduct on SCH's public website did not constitute a communication under the WPA; (3) the holding is a "narrow one" and should "not be read to definitively construe the application of the term 'private communication' for all cases involving website or internet use"; and (4) the holding is confined "to the facts of this case." R-010-011.

IV. ARGUMENT

Petitioners seek review under sections 1 and 4 of Rule of Appellate Procedure 13.4 (b). Neither applies here, and the Court should deny their Petition.

A. Division One's Decision Does Not Conflict with this Court's Prior Decisions.

The WPA is a wiretap statute, not an all-encompassing privacy law. It bars interception and recording of a "[p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state … without first obtaining the consent of all the participants in the communication." RCW 9.73.030(1)(a). This Court has outlined a four-prong test to establish a violation of the wiretap statute. Under that test, a plaintiff must prove: "(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." *State v. Roden*, 179 Wn.2d 893, 899, 321 P.3d 1183 (2014).

In affirming, the Court of Appeals reached only the first prong, holding Petitioners failed to "plead facts to establish that communication occurred on SCH's public website" when the only conduct identified was "click-and-search activity." R-010. In the almost nine pages Petitioners spend discussing this issue, they never identify with specificity any decision by this Court at odds with Division One's holding. Indeed, the Court of Appeals' decision cites and relies on eight of the ten Washington state court WPA decisions Petitioners cite. Petitioners tacitly concede there is no conflict, arguing that one of the reasons the Court should accept review is to "offer guidance on the WPA's proper scope in the context of web-based communications." Pet. at 33. Petitioners cannot have it both ways. For the following reasons, the Court of Appeal's interpretation of "communication" does not conflict with any prior decision by this Court and review is improper under Rule 13.4 (b)(1).

1. Division One's decision does not conflict with *Gunwall, Roden,* or *Faford*.

Petitioners' argument is that courts should broadly interpret the WPA, so the court should expand the definition of "communication" under the WPA to include unilateral conduct taken on a website with no expectation that any person will ever receive that "communication." *See generally* Pet. 21–33. But they of course forget that this Court has already defined communication under the WPA, relying on a dictionary definition that Petitioners concede requires "information … exchanged between individuals." Pet. at 26-27 (citing *State v. Riley*, 121 Wn.2d 22, 846 P.2d 1365 (1993); Mirriam Webster definition of "Communication"). No such information exchange occurred here.

To support their argument, Petitioners rely heavily on *State v. Roden*, 179 Wn.2d at 898, *State v. Gunwall*, 106 Wn.2d 54, 66, 720 P.2d 808 (1986), and *State v. Faford*, 128 Wn.2d 476, 483, 910 P.2d 447 (1996). The Court of Appeals

addressed all three cases and none conflicts with its holding—indeed each supports the Court of Appeals' decision.

In *State v. Gunwall*, this Court held "that a pen register intercept comes within the definition of a 'private communication transmitted by telephone.'" 106 Wn.2d at 69. In reaching its holding, this Court recognized that the pen register intercept constitutes a communication because it was "continuing in nature, may affect other persons[,] and can involve multiple invasions of privacy." *Id.* Stated differently, it involves an "exchange of information." *Riley*, 121 Wn.2d at 34 (citing *Gunwall*).

In this case, the Court of Appeals properly considered and addressed *Gunwall*, explaining that unlike *Gunwall* where "back-and-forth" messaging occurred, "plaintiffs' complaint did not allege that they navigated SCH's public website to transmit a message to or exchange information with another party." R-010. As a result, *Gunwall* is distinguishable.

As to *State v. Roden*, Petitioners cite it repeatedly for the notion that courts should construe the WPA more broadly than its federal counterpart. But *Roden* and the cases that followed are *all* criminal cases and involve different applications that are not before the Court, involving issues relating probable cause and a Court Order. 179 Wn.2d at 898. *Roden's* reference to the breadth of the WPA relates to the fact that Washington is one of only a handful of states that otherwise requires *all-party* consent, absent probable cause and a court order. *Id.* (citing *State v. O'Neill*, 103 Wn.2d 853, 878–89, 700 P.2d 711 (1985) (Dore, J. concurring in part, dissenting in part)); *State v. Kipp*, 179 Wn.2d 718, 725, 317 P.2d 1032 (2014) (noting that it is Washington's "'all-party' consent rule" that makes the WPA broader than other state and federal laws). "The state act requires both one-party consent and probable cause, whereas the federal wiretap statute simply provides that it is not unlawful to intercept communications where one party consents to the interception." *O'Neill*, 103 Wn.2d at 879 (Dore, J.

concurring in part and dissenting in part). But again, the breadth of the WPA relates to the fact that two-party consent is required, not that the other elements are broader or easier to satisfy than any federal counterparts. *State v. Christenson*, 153 Wn.2d 186, 198 n.3, 102 P.3d 789 (2004) ("all party consent requirement" is the basis for holding that WPA provides significant restrictions on the public). Indeed, because of the criminal overlap, Washington courts reject "novel and expansive application of the privacy act." *State v. Bilgi*, 19 Wn. App. 2d 845, 859, 496 P.3d 1230 (2021). Beyond all-party consent, the WPA is narrower than federal law because it requires any communication take place between two people: "With respect to subsection (a) [of the WPA], unlike the federal [wiretap statutes], the WPA requires a communication between at least two individuals." *Cousineau v. Microsoft*, 992 F. Supp. 2d 1116, 1129 (2012). Thus, as *Roden* confirms, the WPA requires the potential for a "back-and-forth" exchange between people, rather than "a simple informational statement that is

sent to" a static device, as Petitioners did here. *Roden*, 179 Wn.2d at 901. *Roden* supports SCH.[1]

Petitioners' reliance on *State v. Faford*, 128 Wn.2d at 483, fares no better. *Faford* involved radio-scanner interception of private conversations between two people on a handheld phone. *Id.* at 479–80. The scanner owner overheard and relayed the contents of those private conversations to the police. *Id.* at 480. The Court in *Faford* cautioned against adopting the "narrowest definition," but not of a "communication," as Petitioners suggest, but of the word "transmit." *Id.* at 483–84.

[1] This is consistent with other WPA cases, which recognize that the statute covers communications between people, not conduct. Here, Petitioners allege conduct, not a communication directed to a doctor, a nurse, or anyone else. *See, e.g.*, CP 14 (Compl. ¶ 47) (Petitioners' website activity actions "essentially ask the Defendant's *Website* to retrieve certain information") (emphasis added); CP 2–3 (Compl. ¶ 3) (pixel logs "activity"); CP 12 (Compl. ¶ 43) (pixel "measure[s] certain actions," such as clicks, and page views). *Compare State v. Clark*, 129 Wn.2d 211, 214 & n.1, 916 P.2d 384 (1996) (WPA did not cover video recordings of illegal conduct) (citing *Haymond v. Dep't of Licensing*, 73 Wn. App. 758, 761–62, 872 P.2d 61 (1994) (soundless recording of conduct does not violate WPA); *State v. Raymer*, 61 Wn. App. 516, 519, 810 P.2d 1383 (1991) ("soundless recording of conduct is not prohibited by the [WPA]")); *State v. Smith*, 85 Wn.2d 840, 846, 540 P.2d 424 (1975) (WPA did not bar recording of "[g]unfire, running, shouting, [] scream[ing]"; not a communication).

It did not announce some change in the law, it simply held that courts should not allow new technology (radio scanners) to intercept what has always been protected by the statute (private conversation between two or more individuals). *Id*. 485–86. Division One recognized this distinction, noting that *Faford* and cases like it include a mandate pertaining to "evolving technology" but say nothing to support the broad interpretation of "communication" that Petitioners advance. R-009–010.

Petitioners attempt to muddy the waters, claiming the Court of Appeals got it wrong because in reality, they "communicated substantive content regarding health conditions, symptoms, and physicians." Pet. at 27 (citing CP 5–7 (Compl. ¶¶ 15–17)). But they made no such allegations. The cited paragraphs explain Petitioner Baker (who never alleges she was logged into Facebook) used the public-facing website to generically "search for medical conditions and symptoms" using the "search bar" and "Conditions" page, CP 5 (Compl. ¶ 15); that Petitioner Shavies looked up urgent care

facilities and hours, CP 6 (Compl. ¶ 16); and that Petitioner Savoie searched for doctors and undisclosed medical conditions and symptoms, CP 6-7 (Compl. ¶ 17). No named plaintiff alleges searching for any specific condition or viewing the page of any particular provider on the public website, let alone communicating any such information to another person. *See* CP 6–7. And Petitioners' alleged conduct on MyChart is irrelevant because they do not allege Pixel was ever installed on MyChart (and conceded below it was not).

2. Federal courts interpreting WPA have similarly held that browsing data is not a "communication" under the Act.

Petitioners repeatedly invoke federal courts' interpretations of the WPA, but ignore their conclusion that browsing and search history information is not a "communication" covered by the WPA (it is at most, conduct). *See Cousineau*, 992 F. Supp. 2d at 1129 (WPA claim fails because, "[w]ithout an individual on the other end of her communication (other than Microsoft), the transmission of

Cousineau's data cannot be considered a communication under the WPA"). Courts considering the issue have ruled that mouse clicks, page views, and URLs created by typing into a search bar are not "communications" under the WPA because "this data was not transmitted as part of a communication between individuals but instead directed to an automated system." *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1093 (N.D. Cal. 2015); *see also In re Meta Pixel Tax Filing Cases*, 743 F. Supp. 3d 1118, 1121–22 (N.D. Cal. 2024) (data sent via Meta Pixel were not "communications" under the WPA because they were between an individual and a website).

B. The Petition Does Not Present Issues of Substantial Public Importance.

This case does not present "an issue of substantial public interest that should be determined by the Supreme Court." RAP 13.4(b)(4). In two paragraphs, Petitioners summarily argue that because we are living in a "digital age" there is substantial "public interest" in "[w]hether the WPA has any

role in preventing online surveillance" of online "communications." Pet. at 33–34. This broad framing misstates the narrow case before the Court.

The Court of Appeals issued a narrow and unpublished "holding" that was expressly "confine[d] … to the facts of this case." R-011. Petitioners' only support for a strong public interest is their argument that "[a]t least two federal courts have recognized the need for this Court to offer guidance" on this issue. Pet. at 33. Petitioners are mistaken. In *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 1007 (N.D. Cal. 2024) the court analyzed whether corporations qualified as individuals under a specific WPA provision. *Id.* The court held that corporations were not individuals under that WPA clause, and dismissed a WPA claim rooted in an online exchange between an individual and a "business entity's automated system." *Id.* It did not analyze what qualifies as a "communication" under the WPA or request guidance from this court.

Petitioners similarly misrepresent the court's analysis in *Castillo v. Costco Wholesale Corp*., 2024 WL 4785136 (W.D. Wash. 2024)—a case in which their counsel were involved. In *Castillo*, the Western District of Washington grappled with whether a corporation is an individual under a particular WPA provision. *Id.* at *9. It did not discuss whether clicks on public websites qualified as "communications."

Although not directly offered in support of their public interest argument, throughout their brief, Petitioners make broad policy arguments as to why the Court should grant review. For the following reasons, each argument fails:

First, Petitioners argue that because similar claims have been recognized under the federal Wiretap Act, they must also be cognizable under Washington's "more protective" wiretap statute. Pet. at 16–17. But as Petitioners' cited case recognizes, the statutes are different as a textual matter: "For textual reasons specific to the WPA … the Court concludes that the WPA does not protect the personal health data here." *Castillo*,

2024 WL 4785136, at *3. That textual difference means that even if certain conduct is protected under the federal Wiretap Act, '"browsing history data is not a 'communication' protected by the WPA." *Id.* at *7. Moreover, the cases Petitioners rely on have different facts with more specific allegations about the information alleged to be intercepted. *See id.* at *7 ("Plaintiffs do not merely allege that Costco collected information about their searches for general medical treatment options."). Finally, as the Court of Appeals recognized, federal and foreign state law is not binding on this Court's interpretation of Washington Law. *See* R-010, n.15 (citing *Brown v. Old Navy, LLC*, 4 Wn.3d 580, 585, 567 P.3d 38 (2025)).

Second¸ Petitioners' suggestion that the WPA is the only mechanism courts have to protect the privacy of Washington citizens is incorrect. The legislature is more than capable of enacting statutes protecting consumers from web-based privacy violations, including those that do not involve communication. Indeed, as the Court of Appeals recognized, the Legislature did

just that for health-related data privacy. R-011 (citing Washington My Health My Data Act). Washington's My Health My Data Act provides broad protections for "consumer health data," which is defined to include "personal information that is linked or 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). The My Health My Data Act is enforceable by both the attorney general and through a private right of action. RCW 19.373.090 (establishing violations of the act "an unfair method of competition"); RCW 19.86.093 (providing a private right of action for a statutory violation that constitutes an unfair method of competition). If the WPA already protected this data, there would have been no reason for the legislature to enact that law.

And this Court has repeatedly held that any expansion of the WPA must come from the legislature, not the Court. The Legislature is "in the best position to weigh competing policies" about whether "to [] amend[] [WPA] in light of developments

of technology." *Townsend*, 147 Wn.2d at 675 n.2); *O'Neil*, 103 Wn.2d at 861–62 (discussing WPA amendments enacted to "deal with specific problems perceived by the legislature"; because "legislative policies do change").[2] The legislature *has* acted over the last ten years to amend the WPA—long after the invention of the internet and data analytics—but has chosen not to enact the changes Petitioners would prefer. *See, e.g.*, RCW 9.73.030(5) (2021) (addressing recording of custodial investigations); RCW 9.73.270 (2015) (barring collection of meta-data from cell-site simulators).

Third, Petitioners' arguments ignore the criminal nature of the WPA. In addition to civil liability, the WPA establishes

[2] And the Courts of Appeal have likewise recognized that any expansion to the WPA to cover conduct (e.g., video recording) or based on public policy objectives relating to disclosure of private information, must come from the legislature. *State v. Clayton*, 11 Wn. App. 2d 172, 180, 452 P.3d 548 (2019) ("The Privacy Act does not address police body cameras. It is up to the legislature to extend the protections of the act to the use of those cameras if it so desires."); *Kearney v. Kearney*, 95 Wn. App. 405, 414, 974 P.2d 872 (1999). ("His argument that this reading of the statute eviscerates important policies underlying the privacy act should be directed to the Legislature, which over 20 years ago removed 'divulge' from the list of proscriptions in order to aid law enforcement").

criminal liability for eavesdroppers. RCW 9.73.080. The rule of lenity mandates that courts construe any ambiguity in a criminal statute construed against liability. Washington courts adopt the rule of lenity in civil cases where the statute has parallel criminal effect. *Gray v. Twitter, Inc.*, 2021 WL 11086642, *8 (W.D. Wash. 2021) (interpreting RCW 18.04 and applying rule of lenity). "Because our legislature criminalized violations of the privacy act, its applicability should be viewed as we view the applicability of criminal laws, to which we give a 'literal and strict interpretation.'" *State v. Gates*, 28 Wn. App. 2d 1301, 2023 WL 6553863, *10 (2023) (unpublished) (citing *State v. Delgado*, 148 Wn.2d 723, 727, 63 P.3d 792 (2003)). *See also State v. Clark*, 96 Wn.2d 686, 690, 638 P.2d 572 (1982) (penal statutes strictly construed); *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) ("Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies.").

Petitioners' view of the wiretap statute would impose sweeping new civil and criminal liability on large swaths of public website operators without meaningful notice.

V. CONCLUSION

For the foregoing reasons, the Court should deny the Petition for Review.

This document contains 4,946 words, excluding the parts of the document exempted from the word count by RAP 18.17.

RESPECTFULLY SUBMITTED this 1st day of December, 2025.

DAVIS WRIGHT TREMAINE LLP

/s/ Fred B. Burnside

Fred B. Burnside, WSBA #32491
Rachel Herd, WSBA #50339
920 Fifth Ave, Suite 3300
Tel: 206.622.3150
fredburnside@dwt.com
rachelherd@dwt.com

Attorneys for Respondent
Seattle Children's Hospital

DAVIS WRIGHT TREMAINE LLP

December 01, 2025 - 2:13 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_Answer_Reply_20251201141114SC580821_5537.pdf
  This File Contains:
  Answer/Reply - Answer to Petition for Review
  The Original File Name was Baker_Answer to Petition to Review.pdf

A copy of the uploaded files will be sent to:

- anitamiller@dwt.com
- francescareifer@dwt.com
- kstephens@tousley.com
- lisamerritt@dwt.com
- lteppner@tousley.com
- mpeterson@tousley.com
- rachelherd@dwt.com
- rsolomon@tousley.com
- ryan.ellersick@zimmreed.com

Comments:

Sender Name: Fred Burnside - Email: fredburnside@dwt.com
Address:
920 5TH AVE STE 3300
SEATTLE, WA, 98104-1610
Phone: 206-757-8016

Note: The Filing Id is 20251201141114SC580821