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	No. 86461-1-I DIVISION ONE UNPUBLISHED OPINION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.

Coleman, 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.