FILE
IN CLERK'S OFFICE
SUPREME COURT, STATE OF WASHINGTON
OCTOBER 8, 2026
Stephens, C. J.
CHIEF JUSTICE

THIS OPINION WAS FILED
FOR RECORD AT 8 A.M. ON
OCTOBER 8, 2026
SARAH R. PENDLETON
SUPREME COURT CLERK

IN THE SUPREME COURT OF THE STATE OF WASHINGTON

CARLY BAKER, JANSSEN RAMOS SAVOIE, and AMBER SHAVIES, individually, and on behalf of those similarly situated,	)	No. 104590-5
Petitioners,	)	
v.	)	En Banc
SEATTLE CHILDREN'S HOSPITAL, a Washington nonprofit corporation,	)	
Respondent.	)	Filed: October 8, 2026

ANGELIS, J.—The Washington privacy act (WPA) makes it unlawful 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) (emphasis added). The plaintiffs are the lead plaintiffs of a putative class action. They alleged that Seattle Children's Hospital (SCH), a corporation,

violated this provision when it used technology provided by Meta Platforms Inc. to track the plaintiffs' searches and clicks on SCH's public website and SCH's automated responses, which SCH shared with Meta. According to the plaintiffs, Meta then used the data to create targeted advertising based, at least in part, on the plaintiffs' activities on SCH's website.

We conclude that the WPA does not prohibit SCH's alleged actions. RCW 9.73.030(1)(a) governs interception or recording of "communication" between "two or more *individuals*" and therefore excludes searches and clicks that generate an automated response from SCH's website. (Emphasis added.) Accordingly, we affirm the trial court's order dismissing the plaintiffs' WPA claim.[1]

BACKGROUND

Because we are reviewing a motion to dismiss, we accept the factual allegations in the plaintiffs' complaint as true, and we determine whether they are sufficient to support a violation of the WPA.[2] SCH maintains a public website. The website provides general information, such as a directory of health care professionals with particular specialties who work at SCH, hours of operation for clinics, and descriptions of health conditions. Clerk's Papers (CP) at 18-19, 22, 25,

[1] On appeal, the plaintiffs did not raise, and we therefore do not address, the claims in their complaint that SCH's actions violated other Washington laws.

[2] *Bravo v. Dolsen Cos.*, 125 Wn.2d 745, 750, 888 P.2d 147 (1995); *Kinney v. Cook*, 159 Wn.2d 837, 842, 154 P.3d 206 (2007).

67-70. Users can navigate the website using a search bar or by clicking links. The website also uses a cookie[3] called Meta Pixel, which is free software used to track website visitors and which Meta uses to target advertisements based on visitors' activities on websites like SCH's public site. Specifically, Pixel tracks users' clicks, text searches, and page views, and it sends the data to Meta without the user's knowledge. For example, when a visitor types "depression" in the search bar of SCH's public website, the site loads a page with resources for this health condition. Pixel records and relays the content of this search to Meta, which links that information to the Facebook or Instagram account of the website visitor and which Meta uses for targeted advertising.

If a user does not have a Meta account or is not logged into an account when using SCH's website, Pixel collects and transmits the user's activity to Meta with a unique identifier. That identifier allows Meta to link the user's activity on the SCH website when that individual logs in to or creates a Meta account.

SCH's website alerts visitors, via a pop-up window, that if they accept cookies, they agree to the use of that software to store data that assist in marketing.

[3] The plaintiffs' complaint defines "cookie" as a text file that stores information about a website viewer's device that can be shared. Pixel uses first- and third-party cookies. A first-party cookie is created by the website that a user is currently visiting, and a third-party cookie can store and communicate a website user's data from one website with a different website. Pixel uses these cookies to link the data from visitors to SCH's public website with those visitors' Meta identification and profiles.

The alert does not, however, identify Pixel or explain the process by which Pixel collects and uses website data.

In 2013, Carly Baker, Amber Shavies, and Janssen Ramos Savoie filed a putative class action suit against the hospital, alleging a violation of the WPA.[4] The plaintiffs alleged that they visited SCH's public website to search for information regarding their children's medical conditions and for clinic operating hours, as well as visiting the patient portal, MyChart, to communicate with doctors and view their children's electronic records and medical histories.

The plaintiffs argued that their website searches constitute "private communication[s]" that were intercepted and recorded by Pixel, violating RCW 9.73.030(1)(a). SCH challenged the sufficiency of the allegations, arguing that Pixel was never installed on the hospital's MyChart patient portal and that the complaint should be dismissed for failure to state a claim for relief. At the close of oral argument, the trial court granted SCH's motion to dismiss with prejudice.

The plaintiffs appealed the dismissal of their WPA claim, arguing that SCH's use of Pixel on its public website violated RCW 9.73.030(1)(a). The Court of Appeals determined that the plaintiffs' searches and queries on SCH's website were not "private communication[s]" under the WPA because they alleged that the

[4] The plaintiffs also brought claims under the Washington Consumer Protection Act, ch. 19.86 RCW, and Washington Uniform Health Care Information Act, ch. 70.02 RCW, as well as invasion of privacy, breach of implied contract, conversion, and unjust enrichment.

communications were unilateral rather than a "back-and-forth" exchange of information with another party. *Baker v. Seattle Children's Hosp.*, No. 86481-1-I, slip op. at 6, 10-11 (Wash. Ct. App. Aug. 18, 2025) (unpublished), https://www.courts.wa.gov/opinions/pdf/864611.pdf. The court affirmed dismissal of the complaint. *Id.* at 11.

The plaintiffs petitioned for review in this court, which we granted. 5 Wn.3d 1025 (2026).[5] We received amici curiae briefs from the Chamber of Commerce of the United States and Washington State Hospital Association, and Interactive Advertising Bureau Inc. in support of SCH.

ANALYSIS

A trial court's ruling on a motion to dismiss for failure to state a claim is a question of law that we review de novo. *Scott v. Amazon.com, Inc.*, 6 Wn.3d 1, 8, 583 P.3d 1155 (2026) (quoting *Cutler v. Phillips Petrol. Co.*, 124 Wn.2d 749, 755, 881 P.2d 216 (1994)). We apply the facts alleged in the complaint, and we may also consider hypothetical facts "'conceivably raised by the complaint'" in support. *Bravo v. Dolsen Cos.*, 125 Wn.2d 745, 750, 888 P.2d 147 (1995) (quoting

[5] The plaintiffs did not explicitly abandon the allegation that Pixel was installed on MyChart, but they subsequently clarified that their claims targeted only the use of Pixel on SCH's publicly available website. CP at 74 n.5 (plaintiffs' statement that "MyChart . . . is relevant only to the extent that the Complaint alleges that the Pixel transmits to Meta when a patient attempts to log-in to MyChart"). We therefore limit our review to the plaintiffs' activities on SCH's public website.

Halvorson v. Dahl, 89 Wn.2d 673, 674, 574 P.2d 1190 (1978)); *Kinney v. Cook*, 159 Wn.2d 837, 842, 154 P.3d 206 (2007). We affirm dismissal if, after construing the pleaded facts in favor of the nonmoving party, we conclude there is not "'any set of facts'" that "'would justify recovery.'" *Kinney*, 159 Wn.2d at 842 (quoting *Tenore v. AT&T Wireless Servs.*, 136 Wn.2d 322, 329-30, 962 P.2d 104 (1998)).

The primary dispute in this case is the meaning of RCW 9.73.030(1)(a), specifically the statutory phrase "between two or more *individuals*." (Emphasis added.) When interpreting a statute, our review is de novo. *Dep't of Ecology v. Campbell & Gwinn, LLC*, 146 Wn.2d 1, 9, 43 P.3d 4 (2002). We begin with the statute's text and the text of related statutes: "The surest indication of the legislature's intent is the plain meaning of the statute, which we glean 'from all that the Legislature has said in the statute and related statutes which disclose legislative intent about the provision in question.'" *Five Corners Fam. Farmers v. State*, 173 Wn.2d 296, 305, 268 P.3d 892 (2011) (quoting *Campbell & Gwinn*, 146 Wn.2d at 11). If a statute is ambiguous, we may consider other guides to legislative intent, such as legislative history and circumstances of its enactment. *Id.* at 305-06.

We begin with the statutory text. RCW 9.73.030 states, in relevant part:

(1) Except as otherwise provided in this chapter, 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:
>
> (a) Private communication . . . between two or more *individuals* . . . .

(Emphasis added.)

RCW 9.73.030(1) references "individual" twice, and the statutory language distinguishes between "individual[s]," on the one hand, and other entities such as "partnership[s], corporation[s], association[s], or the state of Washington," on the other hand. When the legislature uses two different terms in the same statute, we presume lawmakers intended the terms to have different meanings. *Densley v. Dep't of Ret. Sys.*, 162 Wn.2d 210, 219, 173 P.3d 885 (2007) (citing *Koenig v. City of Des Moines*, 158 Wn.2d 173, 182, 142 P.3d 162 (2006)). Accordingly, the term "individual" in subsection .030(1)(a) does not encompass the other, separately listed institutions in subsection .030(1).

In this case, no party disputes that SCH is a corporation, and each communication involved only one of the plaintiffs and a fully automated system SCH owns and operates. Thus, under the plain language of RCW 9.73.030(1), the plaintiffs did not communicate with an "individual" when searching or clicking and receiving automated responses. The WPA provision at issue covers only private communications transmitted between "two or more individuals." RCW 9.73.030(1)(a). Because only one individual was involved in each communication, the plaintiffs do not have a claim under the WPA.

The plaintiffs argue that transmitted communications need not be between "two or more individuals" because the WPA confirms that corporations can be liable under the act. The fact that RCW 9.73.030(1) expressly states that both individuals and corporations can be liable but separately requires covered communications to be "between two or more individuals" reinforces (rather than undermines) our conclusion. Had lawmakers intended the phrase "between two or more individuals" in .030(1)(a) to encompass the full list of entities and organizations in .030(1), they could have written .030(1)(a) to mirror the preceding section or could have stated that the WPA protects communications between two or more "persons," rather than "two or more individuals." The legislature did not use such language, and courts cannot add or delete language from an unambiguous statute. *State v. J.P.*, 149 Wn.2d 444, 450, 69 P.3d 318 (2003). Accordingly, we conclude that the relevant portion of the WPA does not apply to the communications at issue, each of which involved only one of the plaintiffs and an automated server maintained by a corporate entity.

The plaintiffs also ask us to take into account that our court has characterized the WPA as "one of the most restrictive electronic surveillance laws ever promulgated," *State v. Roden*, 179 Wn.2d 893, 898, 321 P.3d 1183 (2014), and courts have denied motions to dismiss claims alleging that conduct similar to SCH's actions here violate the federal wiretap act or California's privacy act. As

we have cautioned, however, "[f]ederal cases on [the federal wiretap statute] are not instructive given the significant differences between the state and federal statutory schemes." *Id*. at 905. The same is true of California's privacy act, which likewise differs significantly from the WPA. We also have clarified that when we described the WPA as among the "most restrictive" privacy statutes, we were focused primarily on its requirement that all parties consent before a communication may be recorded, which the federal wiretap act does not require, and which most states do not require. *State v. Kipp*, 179 Wn.2d 718, 724-25, 317 P.3d 1029 (2014) (noting that "Washington is 1 of only 11 states that require that *all* parties to a private communication consent to its recording and disclosure").

In sum, RCW 9.73.030(1)(a) applies to a communication between two or more individuals and does not apply to a communication between an individual and another of the entities listed in RCW 9.73.030(1).[6] The communications at issue in this case occurred between a single member of the putative class and an automated website maintained by a corporation—SCH. The plaintiffs' activities on SCH's website do not qualify, therefore, as a communication between two or more individuals, and their WPA claim cannot succeed.[7]

---

[6] The entities listed in RCW 9.73.030(1) will often, of course, communicate through individuals. We need not, and do not, resolve whether the statute would apply when such communications are transmitted by a covered device and are between two or more individuals because those hypothetical facts are not conceivably raised by the complaint.

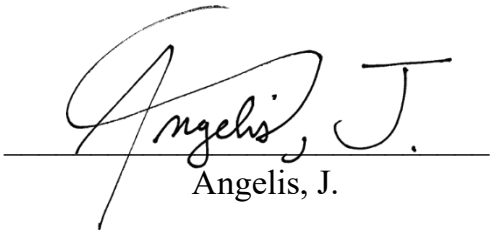
[7] Because the plaintiffs do not challenge dismissal of their other claims—alleged violations of the Washington Consumer Protection Act and the Washington Uniform Health Care Information

Because we conclude that the claims, as pleaded, do not satisfy the "between two or more individuals" requirement, we do not decide whether any communications at issue constitute a "private communication" under RCW 9.73.030(1)(a).

CONCLUSION

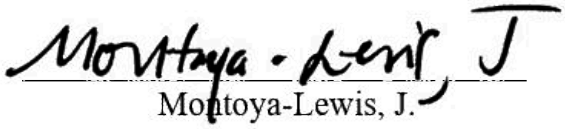
We hold that the communications at issue do not constitute a communication "between two or more individuals" under RCW 9.73.030(1)(a). Accordingly, we affirm the trial court's order dismissing the plaintiffs' complaint.

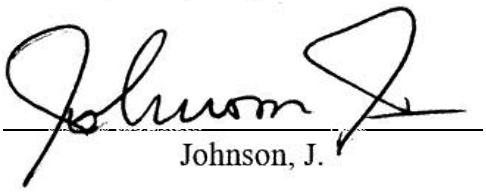
Act, and claims for invasion of privacy, breach of implied contract, conversion, and unjust enrichment—our opinion does not address the sufficiency of those claims.


Angelis, J.

WE CONCUR:


Stephens, C.J.


Montoya-Lewis, J.


Johnson, J.


Mungia, J.


Gordon McCloud, J.


Melody, J.

No. 104590-5

GONZÁLEZ, J. (concurring in result)—A group of parents allege they clicked links and typed terms into a search bar of the Seattle Children's Hospital website and software embedded in that website reported the activity to a third party in violation of Washington's privacy act. Our privacy act makes it unlawful to intercept or record a "[p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals" without first obtaining the consent of all participants. RCW 9.73.030(1)(a). I agree with the majority that the trial court properly dismissed the claims based on RCW 9.73.030(1)(a) under CR 12(b)(6).

The parents' allegations are not sufficient to overcome a motion to dismiss because they have not pleaded that their private communications were transmitted "between two or more individuals." *Id.* I write separately, however, to stress that the parents sufficiently allege private communications were transmitted.

Unlike the majority, I would also recognize that private communications transmitted between an individual and individuals working for a corporation are protected by our privacy act. Therefore, I respectfully concur in result.

Questions of statutory interpretation are reviewed de novo. *State v. Wadsworth*, 139 Wn.2d 724, 734, 991 P.2d 80 (2000). Our privacy act forbids the interception or recording of private communications and conversations under specific conditions:

> (1) Except as otherwise provided in this chapter, 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:
>
> (a) Private 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;
>
> (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation.

RCW 9.73.030. This case involves an allegedly intercepted or recorded private communication. I agree with the majority that the parents' RCW 9.73.030(1) claim does not survive because they do not allege their private communications were transmitted between two or more individuals. Because of that result, the majority does not address whether the parents sufficiently alleged a private

communication was transmitted, but I would reach that issue. In my view, the parents transmitted private communications on the hospital's website, but they directed those communications to a server that returned stored content and not to another individual.

Carly Baker alleges she used the hospital website's search bar and "Conditions" page to search for medical conditions and symptoms. Janssen Ramos Savoie alleges she used the search bar and the "Find A Doctor" page to search for health care providers and medical specialists and to conduct searches on medical conditions and symptoms. Amber Shavies alleges she searched for urgent care facilities and their hours of operation. Each parent has a child who was a patient of the hospital. Each of the parents had an account with Meta Platforms Inc., and some of the parents recall later receiving health-related advertisements on Facebook.

The parents allege that when they visited the hospital's website, their browsers sent "GET requests" to the hospital's web server and the web server returned http responses displaying the requested pages. A "GET request" is one of the two principal types of http requests a browser sends to a website's server. As the complaint describes it, a GET request identifies the requested page by its URL, can carry additional data embedded in that URL, and travels with any cookies the

browser holds for the server it addresses. A "POST request," by contrast, carries data outside of the URL.

Because the hospital had embedded Meta Platforms' Pixel code in its website, the parents allege that the hospital's http response delivered that code to the browser, and the code then caused the browser to duplicate each GET request and send the copy to Meta. A "cookie" is a text file stored on the visitor's device that can later be transmitted to a server. The parents allege that the Pixel places an _fbp cookie on the device of every visitor to the hospital's website, which permits Meta to group that visitor's requests under a single device identifier, and that Meta separately placed a c_user cookie containing the numeric identifier for the visitor's Facebook account. They allege the Pixel transmits both cookies to Meta, and that the c_user cookie is what allows Meta to attribute the request to a named account rather than to an unidentified device.[1]

"There are four prongs we consider when analyzing alleged violations of the privacy act." *State v. Roden*, 179 Wn.2d 893, 899, 321 P.3d 1183 (2014). "There must have been (1) a private communication transmitted by a device that was (2)

[1] In responding to the hospital's motion to dismiss, the parents disclaimed reliance on any Pixel activity occurring after a user signs in to the MyChart patient portal, stating that whether the Pixel continues to operate inside the portal "has no bearing on the adequacy of the allegations." Clerk's Papers at 74 n.5. I therefore do not address the complaint's allegations that the hospital intercepted, recorded, and disclosed information exchanged inside the portal, including test results, messages to providers, and prescription refill requests. The parents did not abandon their allegation that the Pixel discloses a user's patient status when the user navigates to the portal's sign-in page.

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." *Id*. (citing *State v. Christensen*, 153 Wn.2d 186, 192, 102 P.3d 789 (2004)). The first prong is at issue here. Importantly, the circumstances of this case require clarifying that the first prong's private communication transmitted by a device must be "between two or more individuals." RCW 9.73.030(1)(a).

A "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) (alteration in original) (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 460 (1986)). Under this definition, back-and-forth interactions are not required. *See also State v. Townsend*, 147 Wn.2d 666, 670, 57 P.3d 255 (2002) ("These communications from Townsend [to a fictitious child] were stored automatically on [Detective] Keller's computer. This enabled Keller to read the messages at his leisure and to print them for later use as evidence."). A communication is private (1) when parties manifest a subjective intention that it be private and (2) where that expectation is reasonable. *Id*. at 673; *see also Christensen*, 153 Wn.2d at 193.[2]

[2] In determining whether a communication is private, it is generally sufficient to show the person communicated with a single recipient. *See, e.g.*, *Roden*, 179 Wn.2d at 897 (private exchange of text messages); *State v. Faford*, 128 Wn.2d 476, 481-88, 910 P.2d 447 (1996) (private cordless telephone calls); *Townsend*, 147 Wn.2d at 671-79 (private e-mails and instant messages). A person claiming the protections of the act may need to show more than that to establish communications with a larger group are private. But private communications transmitted between more than two

Although the technological setting is different, the private communications on a website are analogous to the private communications in *State v. Gunwall*, 106 Wn.2d 54, 720 P.2d 808 (1986). In *Gunwall*, this court held that the numbers captured by a "pen register" were a private communication under RCW 9.73.030(1)(a). *Id.* at 69. A "pen register" is a device attached to telephone lines or connections to identify local and long-distance numbers dialed. *Id.* at 63. The court recognized that a pen register was "comparable in impact to electronic eavesdropping devices" because it is "continuing in nature, may affect other persons and can involve multiple invasions of privacy." *Id.* at 69. In contrast, we later held that a "line trap" did not intercept a private communication. *Riley*, 121 Wn.2d at 33-34. A "line trap" is a device placed by a telephone company to trace telephone calls to their source. *Id.* Unlike a pen register, which recorded an exchange of information (the dialing of one telephone number to another), a tracer reveals only the telephone number of the dialing party. *Id.*; *see also Roden*, 179 Wn.2d at 901 (distinguishing a phone number displayed on a pager from a text message sent on a mobile device, which is more like an e-mail exchange and telephone call). The numbers captured in *Gunwall* were dialed to reach a person on the other end of the line. That distinction matters here.

As presented, this case involves a public website's links and search bar. A

---

individuals are protected by our privacy act. *See* RCW 9.73.030(1)(a).

click and a typed query each impart information: the user's question or concern. The server returns content responsive to it. Those clicks and queries could convey what condition or symptom a parent was researching and which physician they were looking for. The parents allege they expected these communications to remain private. That expectation was reasonable on this record. The hospital's notice told patients it would not share their health information beyond the disclosures it listed, and none of those disclosures are related to advertising. *See* Clerk's Papers (CP) at 9, 36. Whether a general cookie banner defeated that expectation is not resolved by the pleadings. I would therefore hold that the parents' clicking and searching could constitute a private communication.

Nevertheless, like the majority, I would affirm the trial court's CR 12(b)(6) dismissal because the private communications were not transmitted between two or more individuals. We take the complaint's factual allegations as true and may consider hypothetical facts supporting the claim. *FutureSelect Portfolio Mgmt., Inc. v. Tremont Grp. Holdings, Inc.*, 180 Wn.2d 954, 962, 331 P.3d 29 (2014). While I would normally be reluctant to dismiss a case presenting an issue of first impression in a novel technological setting, no development of the record would change the answer here. As argued, the parents' private communications were

directed at a server that returned stored content and not at another individual.[3] It is not enough to allege, as the parents have, that "a physical person can review the communication at some point after it is received." CP at 78.

Unlike the majority, I would recognize that private communications transmitted between an individual and individuals working for a corporation are protected by our privacy act. I agree with the parents that the structure of our privacy act "leaves no room for a corporate carveout of liability." Pet'r's Suppl. Br. at 22. A corporation acts only through individuals, and the corporate status of the hospital does not tell us whether a private communication was transmitted between two or more individuals.

A private communication sent or received by the hospital's clinical staff from a patient is protected by our privacy act because two or more individuals would be involved in that exchange. Similarly, a message left by the patient on a health provider's voice mail or internal messaging system would be protected by the privacy act even if it was not left for a specific staffer.

---

[3] The parents allege source code "commands the website visitor's browser to take certain actions when the webpage loads." CP at 14. The transmission occurs "quietly in the background without notifying the web browser's user." *Id*. Meta's code "sends secret instructions back to the individual's browser, without alerting the individual." *Id*. at 18. The hospital thereby "commandeer[s] the user's computing device." *Id*. at 23. Nowhere does the complaint allege that anyone read a parent's query or that any query was directed to an individual.

Importantly, neither the majority nor I define the term "individual." "[W]e have consistently interpreted [our privacy act's] terms broadly." *Roden*, 179 Wn.2d at 906. I note that the term "individual" may well include more than a natural person.

Further, I am dubious of the majority's application of the presumption that the legislature intended different meanings when it uses two different terms in the same statute here. Majority at 7-9. The majority draws on the enumeration in subsection (1), which makes our privacy act's prohibition applicable to "any individual, partnership, corporation, association, or the state of Washington." RCW 9.73.030. But that list identifies who may violate the act. It does not tell us who may be a party to the communication the act protects.

RCW 9.73.030 uses a variety of interrelated words. Subsection (1)(a) uses "individuals" and then "participants." Subsections (2) and (3) use "party" and "parties engaged in the communication or conversation." Subsection (4) uses "speakers." In such circumstances, the "different meanings" presumption loses force. Likewise, subsection (1)(b) conditions lawfulness on the consent of "all the persons engaged in the conversation." If the term "person" extends to a corporation, then the legislature contemplated a corporate consent-provider and a corporate consent-provider-participant. The majority does not explain why a corporation may consent to the recording of a conversation under subsection (1)(b) but cannot be on one end of a communication under subsection (1)(a).

Whether the hospital owns and maintains the website is not part of the analysis. Our privacy act does not ask who owned the equipment that carried the communication. We need decide only whether the parents alleged that a private

communication was transmitted between two or more individuals. Having disclaimed reliance on what occurred inside the patient portal, the parents are left with clicks and searches typed into a public webpage. A message to a member of a care team is not before us, nor is the application of our privacy act to a system that does more than return stored content.

With these observations, I concur in result.

González, J.

Whitener, J.