

Tracking Pixels on Automated Website Held Not to Violate Washington Privacy Act

OCTOBER 16, 2026

Authors: [Laura E. Kogan](#), [James E. von der Heydt](#), [Hannah Laubach](#)

Featured Practices: [Litigation](#), [Consumer Protection & Class Actions](#), [Intellectual Property](#)

Featured Industries: [Retail & E-Commerce](#)

Key Takeaways

- In *Baker v. Seattle Children's Hospital*, the Washington Supreme Court held that consumers' clicks and searches on a fully-automated website are not communications "between two or more individuals" under the Washington Privacy Act.
- The decision substantially limits WPA claims based on website tracking technologies, providing businesses with a strong defense against a growing wave of pixel-tracking litigation.
- Businesses should continue to evaluate their use of tracking tools, particularly on customer-facing forms, chat functions, and logged-in platforms, as questions remain regarding how the WPA applies to other types of online interactions.

Earlier this week, the Washington Supreme Court unanimously affirmed dismissal of a putative class action alleging that Seattle Children's Hospital violated the Washington Privacy Act (WPA), RCW 9.73.030, by using Meta Pixel on its public website. *Baker v. Seattle Children's Hosp.*, No. 104590-5, 2026 WL 3023818 (Oct. 8, 2026).

In *Baker*, the Court held that a user's clicks and searches on an automated website operated by a corporation do not qualify as communications "between two or more individuals" for purposes of the statute. See RCW 9.73.030(1)(a). The ruling significantly narrows WPA exposure for companies that use website tracking technologies, but it leaves important questions open, including when consumers' website interactions might constitute "private communications" under the WPA.

Background

Washington is one of a minority of states that require all-party consent to record communications. The WPA makes it unlawful for any individual, partnership, corporation, association, or the State to intercept or record a "private communication" transmitted by a device "between two or more individuals" without first obtaining the consent of all participants.

The plaintiffs, parents of children treated at Seattle Children’s Hospital, alleged that they used the hospital’s public website to search for information on medical conditions, physicians, and clinic hours. They further alleged that the Meta Pixel code embedded in the site captured their clicks, text searches, and page views and transmitted them to Meta, which then fed the data to their Facebook or Instagram accounts for targeted advertising. For example, a visitor’s search for “depression” was allegedly relayed to Meta. The site displayed a cookie pop-up stating that accepting cookies meant agreeing to data storage for marketing, but the notice did not identify Meta Pixel or explain how it worked.

The trial court dismissed the WPA claim with prejudice, and the Court of Appeals affirmed in an unpublished August 2025 opinion, reasoning that the plaintiffs’ one-way searches were not “communications” because they lacked a back-and-forth exchange.

The Court’s Decision

Writing for seven justices, Justice Angelis anchored the Court’s holding in the statutory text. RCW 9.73.030(1) separately lists “individual[s]” and entities such as corporations, and the Court presumed the Legislature intended those terms to carry different meanings. Because each alleged communication involved only one plaintiff and a fully-automated system owned by a corporation, there were not “two or more individuals,” and the plaintiffs’ claim failed. The Court noted that the Legislature could have protected communications between “persons” but did not.

The Court rejected the plaintiffs’ reliance on decisions allowing similar pixel claims to proceed under the federal Wiretap Act and the California Invasion of Privacy Act, explaining that those statutes differ significantly from the WPA. It also clarified that its prior description of the WPA as among the “most restrictive” surveillance laws referred chiefly to the all-party consent requirement.

The majority made clear that it was not deciding (1) whether website clicks and searches can be “private communications,” or (2) whether the WPA applies where a corporation communicates through individuals, such as employees who might respond to website inquiries.

Concurring in the result, Justice González addressed the first of those questions. In an opinion joined by Justice Whitener, he explained his view that the parents’ interactions with the website were adequately alleged to be “private communications” for purposes of the statute. Under prior WPA case law, this term applies when communicating parties subjectively hold a reasonable expectation of privacy—a test he found to be satisfied at the pleading stage in *Baker* despite the hospital’s pop-up banner securing user consent for cookies to support marketing. According to the concurrence, the banner would not necessarily dispel users’ expectation of privacy created by the hospital’s notice that it “would not share [users’] health information beyond [certain] disclosures [not] related to advertising.”

Justices González and Whitener nonetheless agreed with the *Baker* majority’s grounds for dismissal. As the concurrence summarized, although the plaintiffs’ interactions with the website were “private” for purposes of the WPA, they were “directed at a server that returned stored content and not at another individual,” and therefore were not covered by the statute.

Implications

Baker is most relevant to organizations operating websites, apps, or online portals that are used by Washington residents and that deploy third-party tracking tools such as Meta Pixel, analytics tags, and advertising cookies. Healthcare providers and hospitals are clearly protected by many aspects of the ruling, but its reasoning applies equally to retailers, financial institutions, insurers, and other consumer-facing businesses. For such organizations, *Baker* provides a strong defense to WPA claims based on visitors' clicks and searches on public, fully-automated web pages, because those interactions do not involve communications between two or more individuals.

That protection has limits. Businesses whose employees communicate with customers or patients through live chat, secure messaging, contact forms, or voicemail remain exposed, because the ruling did not address whether the Act applies when a company communicates through individuals. Likewise, organizations that use tracking on patient portals or other logged-in environments should not rely on *Baker*, since the Court only addressed activity on the hospital's public website, which was not alleged to be targeted at an individual on the hospital staff.

Baker addresses only one provision of the WPA. It did not address the scope of Washington's Consumer Protection Act and Uniform Health Care Information Act, or of common-law privacy and contract claims. Further, companies with users outside Washington continue to face active pixel-tracker litigation under federal and other state law, especially in California.

Recommended Next Steps

Washington-facing businesses should inventory the pixels and analytics tags on their sites and apps to identify the data each shares. Since it left several questions about the WPA's scope unresolved, *Baker* does not change the recommendation to keep third-party code out of consumer-inquiry forms routed to employees and chat or messaging interfaces; to restrict tracking on logged-in portals and health-related pages; and to update cookie banners and privacy notices with disclosure of tracking tools and ad-related sharing, obtaining consent where appropriate. For the reasons explained in Justice González's concurrence, even a public-facing website may be reasonably seen as a platform for "private communications" covered by the WPA.

For questions about state privacy statutes and assistance evaluating your company's tracking practices and litigation exposure, please contact a member of Benesch's Litigation Practice Group or Consumer Protection & Class Action team.