Shumaker

NOVEMBER 19, 2026 | PUBLICATION

Client Alert: Privacy Rules Are Moving from the Policy Page to the Code Base: Three Recent Developments and What They Mean for Your Business

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

Mark Lehman

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Three recent developments share one message: regulators and courts determine privacy compliance by evaluating how a company's technology actually functions. California's privacy regulator has proposed rules that spell out, in technical detail, how websites must honor browser-based opt-out signals.[1] California's Attorney General penalized a major app-based company because the opt-out lived outside its app.[2] In contrast, Washington's highest court narrowed one litigation theory used against website tracking tools.[3]

1. California Proposes Detailed Rules for Browser Opt-Out Signals

California law already requires businesses that sell or share personal information to treat a web browser's qualifying opt-out preference signal as a valid request to stop selling or sharing.[4] Proposed regulatory amendments would add further consumer protections.

Under the proposed amendments, if a company sells or shares personal information for targeted advertising, California expects the company's website to detect a consumer's browser opt-out signal before any advertising or analytics tag fires. Furthermore, the company is to apply that consumer's preferences and choices to every device the company has linked to that consumer.Staff of the California Privacy Protection Agency, referred to as CalPrivacy, recommended a package of amendments for formal rulemaking.[5] The proposal would make five practical changes:

- **Global Privacy Control named.** The rule text would identify Global Privacy Control, a common browser setting, as an example of a signal businesses must honor.[6]
- **Cookie syncing.** A business that receives a signal must stop third-party trackers on its site from matching their user identifiers with one another for cross-context behavioral advertising.[7]
- **Linked devices.** A business that ties a consumer's laptop and phone into one pseudonymous profile, through fingerprinting for example, must apply a signal received on one device to every linked device. A business that keeps data in unlinked, device-specific form only needs to apply the signal to that device.[8]
- **Tag timing.** Setting advertising or analytics cookies and pixels before the consent management platform checks for the signal would violate the existing duty to stop selling or sharing "as soon as feasibly possible."[9]
- **Browser features and metrics.** Browser tools that act for a consumer may not block or override the consumer's signal. Businesses subject to metrics reporting would separately count opt-outs received through signals, and that reporting duty would extend to any business required to complete a cybersecurity audit or risk assessment.[10]

Posting a "Do Not Sell or Share" link would not be a satisfactory alternative to processing an opt-out signal.[11]

The proposed amendments are not final, and no comment deadline or hearing date has been set. Publication of the proposed amendments will start a 45-day comment period, which may be followed by revisions, Board adoption, and review by the Office of Administrative Law.[12]

Viewed within the existing legal and regulatory framework, including the new browser opt-out requirement in Civil Code section 1798.136,[13] the proposed amendments suggest that CalPrivacy is concerned that businesses fail to detect browser opt-out signals or fail to properly process opt-out requests originating from browsers. If the proposed amendments are implemented in their current form, the practical burden will fall on marketing technology, because tag managers, consent platforms, and identity-resolution services will need to be configured to work together.

2. Washington Supreme Court Limits Wiretap Claims over Website Pixels

The Washington Supreme Court's recent ruling in *Baker v. Seattle Children's Hospital* held that Washington's wiretap statute does not reach a tracking pixel that records a visitor's clicks and searches on a company's automated public website. However, the ruling left open claims involving communications with real people, such as patient messages to clinical staff.[14]

Parents alleged that Seattle Children's Hospital embedded the Meta Pixel on its public website, which sent the parents' searches and page views about their children's health to Meta for targeted advertising, and that the site's cookie notice neither named the pixel nor explained how it worked.[15] The Washington Privacy Act prohibits recording a private communication "between two or more individuals" without the consent of all participants.[16] Because the statute lists individuals separately from corporations, the court held that a visitor's exchange with a corporation's fully automated website involves only one individual and falls outside the statute.[17] The court affirmed dismissal on that ground alone and did not decide whether website searches are "private communications."[18] The majority distinguished decisions applying the federal wiretap statute and California law, citing significant differences between those schemes.[19]

As a result of the ruling, companies that operate in Washington gained meaningful protection against class claims premised solely on standard analytics on public pages. However, that protection is narrow. The plaintiffs' claims under the Washington Consumer Protection Act and the Uniform Health Care Information

Act, along with common-law theories, were dismissed below and not appealed, so the court did not test their sufficiency.[20] The ruling also does nothing to limit regulatory or litigation exposure in states whose courts read their statutes differently.[21]

3. California Attorney General Settles with Lyft over In-App Opt-Out

If customers use a service through an app, the opt-out must be in the app, take effect immediately and with minimal steps, and not ask a logged-in user to prove identity again. Lyft agreed to pay $1.8 million and accept a multi-year compliance program for falling short of that standard.[22]

The action against Lyft grew out of a 2025 investigative sweep focused on geolocation data.[23] The California Attorney General alleged that, beginning in mid-2023, Lyft disclosed device identifiers, IP addresses, and coarse location data to third parties to target ads to Lyft passengers, but offered no in-app opt-out.[24] Consumers instead had to follow links from the in-app privacy policy to a mobile web page and then log in again and verify their identity, even though they were already signed in to the Lyft application.[25]

The stipulated judgment requires Lyft to:

- Provide a clear and conspicuous in-app opt-out that takes effect immediately across all Lyft services.[26]
- Apply opt-outs, including those sent by browser signal, across every service tied to a logged-in account; for logged-out users, tell them that logging in or providing minimal information may be needed and, if they do not, apply the opt-out to the browser, application, or device and any associated profile, including pseudonymous profiles.[27]
- Let consumers confirm their opt-out and avoid choice architecture that confuses cookie or marketing settings with the opt-out.[28]
- Send a one-time notice of opt-out rights within 60 days to consumers who used the Lyft app between January 1, 2020, and the effective date and have not opted out, and complete risk assessments within 180 days covering sales and sharing, sensitive personal information, and location data used for advertising.[29]
- Maintain a monitoring program, beginning within 180 days, and submit annual reports to the Attorney General for three years.[30]

The theory is simple and broadly applicable: existing rules require that at least one opt-out method reflect how the business primarily interacts with consumers, that methods require minimal steps, and that a business not demand identity verification to opt out.[31] The judgment also tracks some of CalPrivacy's proposed regulatory amendments discussed above.[32]

Conclusion

Taken together, these developments show regulators are moving from asking whether an opt-out exists to testing whether it works, quickly and everywhere the business can recognize the consumer. California is building that expectation into both rules and enforcement, while Washington has signaled that its wiretap statute is not the right tool for policing automated website analytics.[33] Companies should therefore treat opt-out engineering as a core compliance function and should not read the Washington decision as a general safe harbor.

If you have questions or would like more information, please contact Mark Lehman or another member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line.

This article is for general informational purposes and does not constitute legal advice.

[1]Cal. Privacy Prot. Agency, Proposed Text of Regulations: Opt-Out Preference Signals (OOPS) (Oct. 8, 2026) (proposing amendments to Cal. Code Regs. tit. 11, §§ 7025, 7026, 7060, 7102, 7122, 7124, 7157, 7221, 7222) [hereinafter Proposed OOPS Text], https://cppa.ca.gov/meetings/materials/20261105_06_09_text.pdf.

[2]Press Release, Cal. Off. of the Att'y Gen., Privacy Rights Can't Be Left in the Rearview: Attorney General Bonta Secures $1.8 Million Settlement with Lyft (Oct. 29, 2026) [hereinafter Lyft Press Release], https://oag.ca.gov/news/press-releases/privacy-rights-can%E2%80%99t-be-left-rearview-attorney-general-bonta-secures-18-million.

[3]*Baker v. Seattle Children's Hosp.*, 597 P.3d 763, 765, 767 & n.6 (Wash. 2026).

[4]Cal. Code Regs. tit. 11, § 7025(b)-(c) (2026); *see also* Cal. Civ. Code § 1798.135(b), (e) (West 2026).

[5]Memorandum from Lisa Kim, Senior Privacy Counsel & Advisor, et al., Cal. Privacy Prot. Agency, to Members of the Board, Cal. Privacy Prot. Agency, Agenda Item No. 9: Discussion and Possible Action on Proposed Amendments to Regulations, Sections 7025, 7026, 7060, 7102, 7122, 7124, 7157, 7221, and 7222, Regarding Opt-Out Preference Signals and Other Regulatory Updates, Including Possible Advancement to Formal Rulemaking, at 2 (Nov. 6, 2026) [hereinafter OOPS Staff Memo], https://cppa.ca.gov/meetings/materials/20261105_06_09.pdf.

[6]Proposed OOPS Text, *supra* note 1, at 1 (proposed § 7025(b)(1)).

[7]*Id.* at 4-5 (proposed § 7025(c)(7)(F)).

[8]*Id.* at 5 (proposed § 7025(c)(7)(G)-(H)).

[9]*Id.* at 10 (proposed § 7026(f)(3)(C)).

[10]*Id.* at 7 (proposed § 7025(h)); *id.* at 13 (proposed § 7102(a)).

[11]*Id.* at 5-6 (proposed § 7025(e)).

[12]OOPS Staff Memo, *supra* note 5, at 2; Cal. Privacy Prot. Agency, Laws & Regulations, https://cppa.ca.gov/regulations/ (last visited Nov. 17, 2026) (listing the opt-out preference signal package under preliminary rulemaking activities).

[13]Cal. Civ. Code § 1798.136 (West 2026) (added by 2025 Cal. Stat. ch. 465, § 2 (A.B. 566), eff. Jan. 1, 2026, operative Jan. 1, 2027).

[14]*Baker*, 597 P.3d at 765, 767 & n.6; *see also id.* at 770-71 (González, J., concurring in result).

[15]*Baker*, 597 P.3d at 765.

[16]Wash. Rev. Code § 9.73.030(1)(a) (2026).

[17]*Baker*, 597 P.3d at 766-67.

[18]*Id.* at 768.

[19]*Id.* at 767.

[20]*Id.* at 765 nn.1, 4; *id.* at 767 n.7.

[21]*Id.* at 767.

[22]Final Judgment & Permanent Injunction ¶¶ 25, 34, 36, *People v. Lyft, Inc.*, No. CGC-26-641775 (Cal. Super. Ct. S.F. Cnty. Oct. 29, 2026) [hereinafter Lyft Judgment], https://oag.ca.gov/system/files/attachments/press-docs/caseinfo.pdf.

[23]Complaint for Injunction, Civil Penalties & Other Equitable Relief ¶ 9, *People v. Lyft, Inc.*, No. CGC-26-641775 (Cal. Super. Ct. S.F. Cnty. filed Oct. 28, 2026) [hereinafter Lyft Complaint], https://oag.ca.gov/system/files/attachments/press-docs/people-v-lyft-file-stamped-complaint.pdf; *see also* Lyft Press Release, *supra* note 2 (describing the March 2025 sweep).

[24]Lyft Complaint, *supra* note 23, ¶¶ 7, 9.

[25]*Id.* ¶¶ 10-11.

[26]Lyft Judgment, *supra* note 22, ¶ 25(a).

[27]*Id.* ¶ 25(b)-(c).

[28]*Id.* ¶¶ 26-27.

[29]*Id.* ¶¶ 30, 32.

[30]*Id.* ¶ 34.

[31]Cal. Code Regs. tit. 11, §§ 7026(a)-(d), 7060(b) (2026).

[32]*Compare* Lyft Judgment, *supra* note 22, ¶ 25(b)-(c), *with* Proposed OOPS Text, *supra* note 1, at 5 (proposed § 7025(c)(7)(G)-(H)).

[33]Proposed OOPS Text, *supra* note 1; Lyft Judgment, *supra* note 22; *Baker*, 597 P.3d at 766-68.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer