

California Privacy Protection Agency

Initial Statement of Reasons: Opt-Out Preference Signals (OOPS)

California Code of Regulations

Title 11. Law

Division 6. California Privacy Protection Agency

Chapter 1. California Consumer Privacy Act Regulations

Sections Affected: California Code of Regulations (CCR), Title 11, sections 7025, 7026, 7060, 7102, 7122, 7124, 7157, 7221, and 7222.

Problem Statement

The California Privacy Protection Agency (Agency) implements and enforces the California Consumer Privacy Act (CCPA). (Civ. Code, § 1798.199.10.)¹ The CCPA provides consumers with specific privacy rights and imposes obligations on businesses to respect those rights.

Under the CCPA, businesses must recognize and honor consumers' opt-out preference signals, including Global Privacy Control (GPC), as valid requests to opt out of the sale or sharing of personal information. However, the Agency, the Attorney General's office, and stakeholders have observed inconsistent compliance across industries. Since 2020, enforcement actions by the Agency and the Attorney General's office have demonstrated that many businesses fail to detect, honor, or properly implement opt-out preference signals (OOPS) in accordance with existing law.

In November 2025, the Agency Board directed staff to conduct preliminary rulemaking on the topic area of OOPS. During preliminary rulemaking, the Agency conducted extensive stakeholder outreach, reviewed 376 pages of public comments, and performed a state-by-state analysis of laws pertaining to OOPS, or universal opt-out mechanisms, the synonymous term used by other states. This work revealed areas in which further guidance could be of assistance to the regulated community, which include how OOPS apply to pseudonymous profiles and cross-device or cross-platform tracking; the importance of determining whether a business has received an OOPS before setting cookies or other tracking technologies that facilitate the sale or sharing of personal information; and whether browser-enabled features that disclose personal information must also forward the consumer's opt-out signal. Stakeholders, including privacy-management platforms, advertising organizations, browser developers, consumer advocates, academics, and legal practitioners requested additional guidance.

For these reasons, the Agency proposes amendments to further clarify existing requirements. These amendments generally do not create new obligations; instead,

¹ All references are to the Civil Code unless otherwise indicated.



they provide additional guidance to businesses regarding what is already required by statute and regulation.

The proposed amendments to section 7025 expressly identify GPC as an OOPS and adds examples of how OOPS applies to pseudonymous profiles, cookie-syncing, and browser features that disclose a consumer's personal information. Proposed amendments to section 7026 add an example demonstrating that, to meet timing requirements, a business must determine whether it has received an opt-out preference signal before setting cookies or other tracking technologies that facilitate the sale or sharing of personal information.

The proposed amendments to section 7102 expand metrics-reporting requirements to businesses that must conduct a cybersecurity audit or risk assessment, and they require businesses subject to metrics reporting to disclose how many opt-out requests were received through OOPS. These changes enhance transparency into how businesses honor consumers' opt-out choices and support more effective oversight.

Finally, the amendments include clarity-focused revisions to sections 7060, 7122, 7124, 7157, 7221, and 7222. These revisions correct typographical errors, align terminology with existing definitions, and improve internal consistency across related provisions, making the regulations easier for businesses to interpret and implement.

Anticipated Benefits from Regulatory Action

The CCPA provides numerous benefits to California consumers and businesses. Central to these benefits are the protection of personal information and the ability for consumers to easily exercise their privacy rights. The proposed regulations provide a number of significant benefits to both Californians and businesses.

The proposed regulations improve clarity regarding how OOPS must be recognized and applied. This additional guidance helps businesses implement existing legal requirements more consistently and reduces confusion about compliance obligations. Greater clarity in the regulations also improves efficiency, reduces the likelihood of errors, and promotes fair and uniform treatment of consumer privacy choices. Businesses benefit from having clearer expectations, which reduces the risk of inadvertent noncompliance and supports more streamlined internal processes.

The metrics reporting requirements provide meaningful benefits for consumers and the public by increasing visibility into businesses' CCPA compliance, including their obligation to honor OOPS. Extending these requirements to businesses whose processing activities pose significant security or privacy risks, such as those subject to cybersecurity audits or risk assessments, strengthens accountability to the law. Consumers will be able to verify that businesses are properly honoring their requests, including those made through an OOPS. This increased transparency promotes public trust, encourages consumers to exercise their rights with confidence, and reassures Californians that OOPS are functioning as intended. Businesses also benefit from



increased trust and credibility with consumers, especially in environments where responsible data practices are essential.

By making OOPS-related metrics publicly available, the regulations allow the Agency to more effectively identify trends, target guidance, and support improved statewide compliance. Increased visibility helps reduce regulatory uncertainty for businesses and contributes to more consistent, predictable privacy protections for Californians. Businesses also benefit from clearer expectations, which supports more effective compliance planning.

In addition to clarifying OOPS requirements, the proposed regulations also improve the overall clarity and internal consistency of the CCPA regulatory framework. Some sections have been refined to ensure terminology is used consistently, examples are aligned with existing statutory language, and regulatory text is easier for businesses and consumers to understand. These non-substantive revisions benefits businesses by reducing ambiguity and supporting more accurate interpretation of existing obligations. It also benefits consumers by supporting more reliable and consistent implementation of their privacy rights.

Specific Purpose, Necessity, and Rational for Each Proposed Change

The Agency proposes amending sections 7025, 7026, 7060, 7102, 7122, 7124, 7157, 7221, and 7222 of Division 6 of Title 11 of the California Code of Regulations.

Article 3. Business Practices for Handling Consumer Requests

Amend § 7025. Opt-out Preference Signals.

Proposed subsection (b)(1) adds “, like Global Privacy Control,” to the regulations as an example of an HTTP header field that meets the requirements of an opt-out preference signal. This change is necessary to provide greater clarity regarding what signals must be recognized as an opt-out preference signal. Over the past five years, Global Privacy Control (GPC) has become the most widely supported opt-out mechanism across consumers, states, and browsers. Both the Attorney General’s office and the Enforcement Division of the Agency have enforced OOPS requirements involving businesses who have failed to honor GPC. Explicitly identifying it in the regulation benefits both businesses and consumers by providing greater clarity of the signals that businesses must comply with and that consumers can use to exercise their right to opt-out of sale or sharing. It also benefits consumers in other states that have reciprocal laws that recognize privacy signals from other jurisdictions by removing any ambiguity that GPC meets the requirements of California’s OOPS law.²

² See *generally*, Conn. Gen. Stat. § 42-520(e)(1)(A)(ii)(IV) (2026) (Connecticut); Del. Code Ann. tit. 6, § 12D-106(e)(1)a.2.D (2026) (Delaware); La. Rev. Stat. § 51:1780.3(E)(1)(e) (eff. Jan. 1, 2027) (Louisiana); Md. Code Ann., Com. Law § 14-4707(f)(4)(iii) (2026) (Maryland); Minn. Stat. § 325M.14,



Proposed subsection (c)(7)(F) is added to illustrate how businesses must apply OOPS to cookies used for cross-context behavioral advertising purposes. This example is necessary because the Agency has observed that cookie-syncing, where advertising companies match their respective user IDs to recognize the same consumer across browsers or devices and enrich ad-targeting profiles, is a common marketplace practice. By including this example, the Agency provides additional guidance to help businesses understand how to apply an OOPS to third-party advertising companies engaged in cookie-syncing that they permit on their website. Businesses must configure their websites to prevent those third-party tracking technologies from initiating or performing cookie-syncing whenever an OOPS is present. This example helps businesses better understand how to comply with the law in similar circumstances and ultimately ensures that consumers' rights are respected.

Proposed subsection (c)(7)(G) and (H) have been added to illustrate how businesses are to apply opt-out preference signals to pseudonymous profiles. Section 7025(c)(1) requires businesses to treat an OOPS as a valid request to opt out "for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles." This language makes clear that OOPS applies to pseudonymous profiles, such as those linked to a consumer through probabilistic or device-based identifiers (e.g., User1234). This is necessary because the Agency has observed confusion in this area and public comments have sought additional guidance on this topic.

Proposed subsection (c)(7)(G) illustrates when a business must apply the OOPS to pseudonymous profiles. When the business uses tracking technologies to recognize the same consumer across its different websites, mobile applications, and other platforms and it sells or shares that information, it must apply the consumer's OOPS with corresponding breadth. By contrast, subsection (c)(7)(H) offers a counterexample showing when a business would not be required to extend an OOPS sent from one device or browser to any others. This counterexample ensures that businesses do not mistakenly believe that they must collect or retain additional information to link browsers or devices to consumers for the purpose of applying an OOPS. Under Civil Code section 1798.145(j), businesses are not required to maintain information in identifiable, linkable, or associable form to link or associate a verifiable consumer request with personal information. Together, these examples demonstrate that the obligation to apply an OOPS to pseudonymous profiles arises from the business's existing practices.

These examples are informed by a recent CCPA enforcement action brought by the California Attorney General's office against Disney. (See *People of the State of California v. Disney DTC, LLC, et al.*, Docket No. 26STCV04425 (Cal. Super. Ct., Los Angeles Cnty.) (filed Feb. 11, 2026).) In the *Disney* case, Disney maintained extensive

subd. 3(a)(4) (2026) (Minnesota); Mont. Code Ann. § 30-14-2809(3)(b)(iv) (2026) (Montana); Neb. Rev. Stat. § 87-1111(5)(d) (2026) (Nebraska); N.H. Rev. Stat. Ann. § 507-H:6(V)(a)(1)(B)(iv) (2026) (New Hampshire); N.J. Stat. Ann. § 56:8-166.11(b)(2)(d) (2026) (New Jersey); Or. Rev. Stat. § 646A.578(5)(c)(D) (2026) (Oregon); Tex. Bus. & Com. Code § 541.055(e)(4) (2026) (Texas); Vt. Stat. Ann. tit. 9, § 2415e(d)(2)(C)(iv) (eff. Jan. 1, 2028) (Vermont).



device-linking and cross-platform advertising capabilities but failed to apply consumers' opt-out requests across all devices and streaming services associated with the consumer. This case underscores an important performative principle: "[I]f a business can associate a consumer's devices with the consumer for advertising purposes, it can and must associate those devices with the consumer for purposes of honoring the consumer's opt-out rights." (*Id.* at ¶ 3.) The proposed examples demonstrate how this principle applies to pseudonymous profiles, providing helpful guidance to businesses and addressing commenters' requests for additional guidance.

Proposed subsection (h) is added to ensure that a consumer's opt-out preference functions effectively and consistently across all browser features that disclose personal information. Modern browsers increasingly offer features and tools that actively retrieve information on behalf of the consumer. In doing so, these features may disclose or make available personal information to third parties. This can undermine the effectiveness of opt-out signals and create inconsistent privacy protections depending on how the consumer interacts with the browser.

By requiring any browser feature that discloses personal information to also forward the consumer's OOPS or privacy setting, the regulation ensures that opt-out rights remain effective across current and emerging browser technologies. As browsers continue to add new functions that retrieve information on behalf of the consumer, this requirement helps ensure that OOPS protections do not become irrelevant or obsolete as technology evolves. It benefits businesses by providing clear guidance on how to apply OOPS consistently across all browser features, and it benefits consumers by ensuring that their rights to opt out of the sale or sharing of personal information are honored even as browser capabilities expand.

Amend § 7026. Requests to Opt-out of Sale/Sharing.

Proposed subsection (f)(3)(C) is added to illustrate how businesses are to comply with the timing requirements for requests to opt-out of sale or sharing of personal information. Under section 7026(f)(1), a business must stop selling or sharing personal information as soon as feasibly possible after receiving a consumer's request to opt out, and no later than 15 business days. If a business continues selling or sharing personal information after the consumer submits the request, but before the business has fully complied with the request, the business must notify all third parties to whom it sold or shared that personal information during the interim period so that those sales or shares can be remedied. (See Cal. Code Regs., tit. 11, § 7026(f)(2).) This framework applies equally to online environments, where sales or shares of personal information routinely occur within milliseconds of a page loading or a cookie being set.

When a consumer visits a website with the GPC, the signal is transmitted to the business with the browser's initial request to access the website. The business receives that signal immediately, triggering its obligation to stop selling or sharing personal information. It is entirely feasible to configure a website to detect the GPC signal before initializing any scripts, cookies, or other technologies that facilitate the sale or sharing of



personal information as required by subsection (f)(1). Moreover, given the speed at which online sales or sharing occur, a business must determine whether it has received an OOPS before initiating these technologies; otherwise, it would face the impractical task of remedying those transmissions under section 7026(f)(2).

This example demonstrates how businesses can meet the timing requirement by ensuring their website detects the GPC signal before setting cookies or loading tracking technologies that facilitate the sale or sharing of personal information. Importantly, this example highlights a common real-world scenario in which businesses rely on both a Consent Management Platform (CMP) and a Tag Management System (TMS) to control the loading of cookies, scripts, tags, pixels, and other technologies capable of selling or sharing personal information. The CMP collects and stores the consumer's consent or opt-out preferences, while the TMS uses those preferences to determine which scripts may execute. Because both systems operate through client-side JavaScript, they must be coordinated so that any script capable of selling or sharing personal information is blocked until the consumer's GPC signal or other opt-out choice has been processed.

In the example, Business WWW configures its website so that third-party advertising and analytics scripts—implemented through cookies, pixels, or JavaScript tags managed by the TMS—initialize before the CMP and TMS determine whether the GPC signal has been received. This misconfiguration is significant because the GPC signal is received with the browser's initial HTTP request. As soon as Business WWW receives the signal, section 7026(f)(1) requires it to stop selling or sharing personal information as soon as feasibly possible. By allowing scripts that set third-party cookies or trigger data-sharing to run before checking for the GPC, Business WWW sells or shares personal information during the critical first milliseconds of the page load. This improper sequencing is not merely a technical oversight; it is a direct violation of the timing requirement.

This example is necessary because it highlights a noncompliant practice observed in the marketplace. It provides businesses guidance by demonstrating that proper compliance requires detecting GPC at the very start of the page-load sequence and blocking all advertising, analytics, or other data-transmitting scripts that would constitute the sale or sharing of personal information until that determination is made. This example also benefits consumers by ensuring that their right to opt-out of the sale and sharing of personal information is honored with greater efficacy.

Article 5. Verification of Requests

Amend § 7060. General Rules Regarding Verification.

Proposed subsection (a) has been revised to add “or request to appeal ADMT” to clarify that verification requirements also apply to the request to appeal ADMT. This revision is necessary to align with the existing requirement in section 7221, subsection (b)(1)(B), which states that businesses must comply with the verification requirements set forth in Article 5 when a consumer submits an appeal. This revision also benefits businesses by



clarifying that existing verification processes for other CCPA rights may also be used for requests to appeal ADMT. Consumers will also benefit from the increased compliance by businesses.

Article 8. Training and Record-Keeping

Amend § 7102. Metrics Reporting Requirements for Businesses.

Proposed subsection (a) has been revised to extend the requirement to publicly disclose metrics about CCPA requests in the privacy policy to businesses that must conduct a cybersecurity audit or risk assessment. Proposed subsection (a)(1)(E) has also been revised to require businesses to identify, from the total number of requests to opt-out of sale or sharing received, how many requests were submitted through an OOPS.

Current regulations require businesses that process the personal information of at least 10,000,000 California consumers to annually disclose, in their privacy policies, their CCPA request metrics, including metrics related to opt-out requests. Businesses that are required to conduct a cybersecurity audit or risk assessment are already identified as entities whose processing activities pose significant security or privacy risks to consumers. Expanding the reporting obligation to these businesses ensures that transparency requirements apply where the potential harms are greatest. In addition, specifying that businesses must disclose the number of opt-out requests submitted through OOPS, including those initiated via GPC, provides clearer insight into industry-wide compliance with the opt-out requirements.

This proposed regulation benefits businesses and consumers because it strengthens consumer trust by creating a single, consistent location in the privacy policy where consumers can verify large-scale compliance with OOPS-based opt-out mechanisms. It also enhances enforcement and accountability by making key CCPA metrics readily available for corroboration by regulators and the public. Finally, by applying reporting obligations to all businesses whose processing activities present significant security or privacy risks, the regulation ensures that transparency expectations are appropriately aligned with the CCPA's risk-based approach.

Additionally, non-substantive changes, including adjustments to punctuation have been made throughout the section. The title has been amended to better reflect the content of the regulation.

Article 9. Cybersecurity Audits

Amend § 7122. Thoroughness and Independence of Cybersecurity Audits.

Proposed subsection (a) has been revised to replace “Accountability” with “Accounting.” This change is necessary to correct a typographical error and is a non-substantive change.



Amend § 7124. Certification of Completion.

Proposed subsection (d)(4) has been revised to remove “n electronically” as unnecessary; and to add “to the best of my knowledge” to align the penalty of perjury requirement with similar language in the Agency’s Data Broker Registration requirements. This change is necessary to remove unnecessary language, clarify businesses’ responsibilities under the proposed regulation, and promote consistency across the Agency’s related regulations.

Article 10. Risk Assessments

Amend § 7157. Submission of Risk Assessments to the Agency.

Proposed subsection (b)(5) has been revised to add “signed a” to align with the language in section 7124, subsection (d)(4); and to add “to the best of my knowledge” to align the penalty of perjury requirement with similar language in the Data Broker Registration requirements. This change is necessary to clarify businesses’ responsibilities under the proposed regulation and promote consistency across the Agency’s regulations.

Article 11. Automated Decisionmaking Technology

Amend § 7221. Requests to Opt-Out ADMT.

Proposed subsection (b)(2)(A) has been revised to replace “ability to perform at work or in an educational program” to “performance at work or performance in an educational program.” This change is necessary to use the defined terms in section 7001, subsections (cc) and (dd), and to clarify businesses’ responsibilities under the proposed regulation and to consistently use the defined terms.

Amend § 7222. Requests to Access ADMT.

Proposed subsection (b)(1) has been revised to replace “improve our services” to “make a significant decision,” to align the language in the example with when a business’s use of ADMT is subject to the requirements of Article 11. This change is necessary to ensure that the example is consistent with the legal threshold at which Article 11 applies. This also prevents businesses from using vague language about their use of ADMT, which undermines consumers’ exercise of their access ADMT right and undercuts consumers’ ability to understand why ADMT was used with respect to them.

Incorporation By Reference

No documents have been incorporated by reference.



Economic and Fiscal Impact

Business impact

The proposed regulations newly affect only those businesses that are required under the CCPA to submit a cybersecurity audit or a risk assessment. Approximately 53,791 businesses fall within this category. For businesses already subject to these statutory and regulatory requirements, any costs associated with the clarifying amendments are expected to be subsumed within the ordinary costs of complying with existing regulations, as the amendments do not impose new substantive obligations.

Estimated Costs to Businesses

The only proposed amendments expected to result in any measurable cost to businesses are those expanding metrics-reporting requirements to businesses that must conduct a cybersecurity audit or risk assessment, including reporting the number of requests to opt-out of sale or sharing received through OOPS. All other proposed amendments merely provide examples, clarify existing requirements, and improve internal consistency and readability of the regulations. They do not impose new obligations or require new systems or create additional costs for businesses.

Businesses subject to the metrics-reporting requirement—both those that currently report them and those who would be newly required to report them under the proposed amendments—already generate the underlying metrics as part of existing processes and requirements. Because all businesses must update their privacy policies annually under existing law, preparing and posting these high-level metrics should require no more than an initial half an hour of administrative or software-developer time. Using the Agency's blended wage rate of \$62.93 per hour, the estimated cost for a typical business is approximately \$31.47. As businesses already maintain the underlying information, the overall cost impact is minimal and does not represent a significant statewide financial burden.

Estimated Benefits of Regulation

The proposed regulations provide several benefits for consumers and businesses. Clarifying how opt-out signals must be recognized and applied helps businesses implement existing legal requirements more consistently and reduces confusion about compliance. This improves efficiency, reduces the likelihood of errors, and promotes fair and uniform treatment of consumer privacy choices across the industry.

The metrics reporting requirements also create broader benefits by improving statewide visibility into privacy practices. By requiring businesses that engage in processing activities posing significant security or privacy risks, such as those triggered for cybersecurity audits or risk assessments, to disclose information about their receipt and process of CCPA requests, the regulations enhance transparency and support enforcement efforts. Consumers and the public will benefit from being able to confirm that businesses are honoring CCPA requests, including those submitted through an



OOPs. This transparency strengthens public trust, provides meaningful insight into whether CCPA requests and OOPS are being respected, gives consumers greater confidence in exercising their rights, and supports the Agency's enforcement work.

Results of Economic Impact Assessment

The Agency has conducted an economic impact assessment and concluded:

Creation or Elimination of Jobs: The proposal would not result in the creation or elimination of jobs.

Creation or Elimination of Businesses: The proposal would not result in an elimination of businesses.

Expansion of Businesses: The proposal would not result in an expansion of businesses.

Worker Safety: The proposal would not benefit worker safety as the provisions do not pertain to, nor impact, worker safety.

Environment: The proposal would not benefit the state's environment as the provisions do not pertain to, nor impact, the state's environment.

Health, Safety and Welfare: The proposal would benefit the health, safety, and welfare of California residents by strengthening protections for personal information. The proposal improves how businesses honor consumers' privacy choices and how they report on key compliance activities. The regulations make it easier for consumers to confirm that businesses are honoring their opt out of the sale or sharing of their personal information through OOPS, and they give businesses additional guidance on how to apply these signals. Together, the regulations improve clarity for businesses and enhance Californians' control over their personal information.

Evidence Supporting Finding of No Significant Statewide Adverse Impact

Although the proposed regulations will directly impact businesses statewide, including small businesses, the Agency concludes that the economic impact will not be significant. Businesses already must comply with opt-out requirements under the CCPA, and the proposed changes provide additional guidance rather than impose new obligations, meaning they are unlikely to increase costs. The metrics reporting requirements rely on information businesses already gather for compliance purposes, limiting additional burden.

The Agency also found that the regulations will not create or eliminate jobs or businesses, nor materially affect California's competitiveness. No specific technologies or equipment are required, further reducing potential costs. Overall, the regulations strengthen privacy protections while avoiding major economic impacts.



Fiscal Effect on State Government

No fiscal impact exists. These regulations do not affect any State agency or program.

Disclosures Regarding the Proposed Action

The Agency has made the following initial determinations:

Local mandate: None.

Cost to any local agency or school district requiring reimbursement pursuant to Government Code section 17500, et seq: None.

Any other non-discretionary cost or savings imposed upon local agencies: None.

Cost or savings to any state agency: None.

Cost or savings in federal funding to the state: None.

Effect upon housing: None.

Specific Technologies or Equipment

The proposed regulations do not require any specific technologies or equipment.

Consideration of Alternatives to the Proposed Action

The Agency has determined that there is no reasonable alternative to the proposed regulations that would better achieve its purposes or achieve them with less burden on businesses while still ensuring full compliance with the law. Below are the alternatives the Agency considered and the reasons each one was rejected.

Alternative 1: Extend metrics requirements in section 7102 to all businesses.

The Agency considered and ultimately rejected the first alternative because implementing it would add reporting and operational obligations for all businesses, increasing their overall compliance burden. While expanding these requirements could provide additional information to support oversight and enforcement, the Agency determined that an incremental approach is more appropriate. Focusing the added financial and administrative responsibilities on businesses whose activities present a significant privacy or security risk allows the Agency to address the most pressing needs while minimizing broader impacts. For these reasons, the Agency concluded that this alternative was not the right approach at this time.

Alternative 2: Remove businesses that process the personal information of 10,000,000 or more consumers and require only those businesses that must conduct a



cybersecurity audit or risk assessment to comply with the metrics requirements in section 7102.

The Agency considered and rejected the second alternative because limiting the metrics requirement only to businesses that must conduct a cybersecurity audit or risk assessment could leave gaps in coverage. Although it is likely that businesses processing the personal information of 10 million or more consumers would fall within the added cybersecurity audit and risk assessment obligations, there remains a possibility that some businesses meeting the original threshold might not. Maintaining the existing threshold avoids that risk and ensures consistent reporting without adding any new costs, since those businesses are already subject to the requirement. For these reasons, the Agency determined that this alternative was not appropriate at this time.

Performance Standard as Alternative

The proposed regulations do not mandate the use of specific technologies or equipment or prescribe specific actions or procedures. While the regulations prescribe certain requirements, the proposed regulations give businesses discretion as to how to meet those requirements. A performance standard would not accomplish the goal of providing transparency with CCPA compliance.

Technical, Theoretical, or Empirical Studies, Reports, or Similar Documents Relied Upon

The following documents were relied on for this rulemaking:

1. 4 Colo. Code Regs. 904-3 §§ 5.01–5.09 (2025), accessed at: <https://www.coloradosos.gov/CCR/GenerateRulePdf.do?ruleVersionId=12259&fileName=4%20CCR%20904-3>.
2. Colo. Rev. Stat. §§ 6-1-108(1), 6-1-1306, 6-1-1313 (2026), accessed at: <https://olls.info/crs/crs2026-title-06.pdf>.
3. Conn. Gen. Stat. § 42-520 (2025), accessed at: https://www.cga.ct.gov/current/pub/chap_743dd.htm.
4. Del. Code Ann. tit. 6, § 12D-106 (2026), accessed at: <https://delcode.delaware.gov/title6/Title6.pdf>.
5. H.B. 4, 88th Leg., Reg. Sess. (Tex. 2023), accessed at <https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB4>.
6. H.B. 154, 152d Gen. Assemb., Reg. Sess. (Del. 2023), accessed at <https://legiscan.com/DE/text/HB154/id/2832228/Delaware-2023-HB154-Engrossed.html>.



7. H.F. 4757, 93d Leg., Reg. Sess. (Minn. 2024), accessed at <https://www.revisor.mn.gov/bills/93/2024/0/HF/4757/versions/4/pdf/>.
8. L.B. 1074, 108th Leg., 2d Sess. (Neb. 2024), accessed at <https://nebraskalegislature.gov/FloorDocs/108/PDF/Final/LB1074.pdf>.
9. La. Stat. Ann. §§ 51:1780.1–1780.5 (2027), accessed at: <https://www.legis.la.gov/legis/ViewDocument.aspx?d=1475339>.
10. Md. Code Ann., Com. Law § 14-4707 (2025), accessed at: https://mgaleg.maryland.gov/2027RS/Statute_Web/gcl/14-4707.pdf.
11. Minn. Stat. § 325M.14 (2025), accessed at: <https://www.revisor.mn.gov/statutes/cite/325M.14/pdf>.
12. Mont. Code Ann. § 30-14-2809 (2025), accessed at: https://leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0280/section_0090/0300-0140-0280-0090.html.
13. N.H. Rev. Stat. Ann. § 507-H:6 (2027), accessed at: <https://www.gencourt.state.nh.us/rsa/html/NHTOC/NHTOC-LV-507-H.htm>.
14. N.J. Stat. Ann. § 56:8-166.11 (2025), accessed at: <https://law.justia.com/codes/new-jersey/title-56/section-56-8-166-11/>.
15. Neb. Rev. Stat. § 87-1111 (2025), accessed at: <https://nebraskalegislature.gov/laws/statutes.php?statute=87-1111>.
16. Or. Rev. Stat. § 646A.578 (2025), accessed at: <https://law.justia.com/codes/oregon/volume-16/chapter-646a/section-646a-578/>.
17. Public Act 22-15, S.B. 6, Gen. Assemb., Reg. Sess. (Conn. 2022), accessed at <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF>.
18. S.B. 255, 2023 Gen. Ct., Reg. Sess. (N.H. 2023), accessed at https://legiscan.com/NH/text/SB255/id/2660738/New_Hampshire-2023-SB255-Introduced.html.
19. S.B. 332, 220th Leg., Reg. Sess. (N.J. 2023) (enacted as P.L. 2023, c. 266), accessed at https://legiscan.com/NJ/text/S332/id/2865878/New_Jersey-2022-S332-Amended.html.



20. S.B. 384, 68th Leg., Reg. Sess. (Mont. 2023), accessed at <https://legiscan.com/MT/text/SB384/id/2791095/Montana-2023-SB384-Enrolled.pdf>.
21. S.B. 541, 2024 Leg., Reg. Sess. (Md. 2024), accessed at <https://legiscan.com/MD/text/SB541/id/2998119/Maryland-2024-SB541-Chaptered.pdf>.
22. S.B. 619, 2023 Leg., Reg. Sess. (Or. 2023), accessed at <https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled>.
23. Tex. Bus. & Com. Code § 541.055 (2024), accessed at: <https://tcss.legis.texas.gov/resources/BC/pdf/BC.541.pdf>.
24. H.121, 2024 Gen. Assemb., Reg. Sess. (Vt. 2024), accessed at: <https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0121/H-0121%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf>.
25. Brock Dahl et al., *OOPS! States Crack Down on Opt-Out Preference Signal Compliance*, Lexology (Nov. 4, 2025), accessed at: <https://www.freshfields.com/en/our-thinking/blogs/a-fresh-take/oops-states-crack-down-on-opt-out-preference-signal-compliance-102ls1x#page=1>.
26. California Department of Justice, Protecting Our Kids from Social Media Addiction Act (SB 976): Public Notice and Related Documents (May 15, 2026), accessed at: <https://oag.ca.gov/sb976>.
27. California Privacy Protection Agency, Board Meeting: Meeting Agenda, Meeting Materials, and Transcripts (Nov. 7, 2025), accessed at: <https://cppa.ca.gov/meetings/materials/20251107.html>.
28. California Privacy Protection Agency, Board Meeting: Meeting Agenda, Meeting Materials, and Transcripts (Aug. 6 – 7, 2026), accessed at: https://cppa.ca.gov/meetings/materials/20260806_07.html.
29. California Privacy Protection Agency, CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Regulations: Documents (Jan. 1, 2026), accessed at https://cppa.ca.gov/regulations/ccpa_updates.html.
30. California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments (2026), accessed at: https://cppa.ca.gov/regulations/pdf/public_comments_reduce_friction_oops.pdf.



31. Chung Peng Lee et al., *How Do Data Owners Say No? A Case Study of Data Consent Mechanisms in Web-Scraped Vision-Language AI Training Datasets*, AAAI'26/IAAI'26/EAAI'26: Proceedings of the Fortieth AAAI Conference on Artificial Intelligence and Thirty-Eighth Conference on Innovative Applications of Artificial Intelligence and Sixteenth Symposium on Educational Advances in Artificial Intelligence (2026), accessed at: <https://arxiv.org/pdf/2511.08637>.
32. Duc Bui, Brian Tang & Kang G. Shin, *Do Opt-Outs Really Opt Me Out?*, Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (2022), accessed at: <https://dl.acm.org/doi/epdf/10.1145/3548606.3560574>.
33. Eryn Ma & Eleanor Birrell, *Prospective Consent: The Effect of Framing on Cookie Consent Decisions*, CHI Conference on Human Factors in Computing Systems Extended Abstracts (2022), accessed at: <https://dl.acm.org/doi/epdf/10.1145/3491101.3519687>.
34. *In the Matter of: 2080 Media, Inc. D/B/A PlayOn Sports* (California Privacy Protection Agency, Feb. 27, 2026), Order of Decision, accessed at: https://privacy.ca.gov/wp-content/uploads/sites/357/2026/03/Order-of-Decision_PlayOn_Enforcement.pdf.
35. *In the Matter of: Ford Motor Company* (California Privacy Protection Agency, Feb. 27, 2026), Order of Decision, accessed at: <https://privacy.ca.gov/wp-content/uploads/sites/357/2026/03/Order-of-Decision-Ford-Motor-Co.pdf>.
36. *In the Matter of: LocateSmarter, LLC* (California Privacy Protection Agency, Aug. 10, 2026), Order of Decision, accessed at: https://privacy.ca.gov/wp-content/uploads/sites/357/2026/08/Order-of-Decision-and-Stipulated-Order_LocateSmarter-LLC-.pdf.
37. *In the Matter of: Tractor Supply Company* (California Privacy Protection Agency, Sept. 26, 2025), Order of Decision, accessed at https://privacy.ca.gov/wp-content/uploads/sites/357/2026/01/20250930_tractor_supply_bd_sfo.pdf.
38. Jan Charatan & Eleanor Birrell, *Two Steps Forward and One Step Back: The Right to Opt-out of Sale under CPRA*, Proceedings of the 2024 ACM Conference on Privacy, Security, and Trust (PoPETs) (2024), accessed at: <https://arxiv.org/pdf/2312.15094>.
39. Matt Schwartz et al., *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports (Apr. 1, 2025), accessed at: <https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf>.



40. Maximilian Hils, Daniel W. Woods & Rainer Böhme, *Privacy Preference Signals: Past, Present and Future*, Proceedings on Privacy Enhancing Technologies (2021), accessed at: <https://arxiv.org/pdf/2106.02283v1>.
41. Muhammad Abu Bakar Aziz & Christo Wilson, *Johnny Still Can't Opt-out: Assessing the IAB CCPA Compliance Framework* (2024), Proceedings on Privacy Enhancing Technologies, accessed at: <https://cbw.sh/publications/aziz-pets24.pdf>.
42. *People of the State of California v. Healthline Media, LLC* (Super. Ct. San Francisco Cnty., July 1, 2025, No. CGC25626794), Complaint for Injunction, Civil Penalties, and other Equitable Relief, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/People%20v.%20Healthline%20Media%20Complaint.pdf>.
43. *People of the State of California v. Jam City, Inc.* (Cal. Super. Ct. L.A. Cnty. Nov. 21, 2025, No. 25STCV34029), Complaint for Injunction, Civil Penalties, and other Equitable Relief, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20%28People%20v%20Jam%20City%20Inc%29.pdf>.
44. *People of the State of California v. Sephora USA, Inc.* (Cal. Super. Ct. San Francisco Cnty. Aug. 23, 2022, No. CGC22601380), Complaint for Injunction, Civil Penalties, and other Equitable Relief, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20%288-23-22%20FINAL%29.pdf>.
45. *People of the State of California v. Sling TV L.L.C.; Dish Media Sales L.L.C* (Cal. Super. Ct. L.A. Cnty. Oct. 30, 2025, No. 25STCV31561), Complaint for Injunction, Civil Penalties, and other Equitable Relief, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20For%20Injunction%2C%20Civil%20Penalties%2C%20And%20Other%20Equitable%20Relief.pdf>.
46. *People of the State of California v. The Walt Disney Co.* (Cal. Super. Ct. L.A. Cnty. Feb. 11, 2026, No. 26STCV04425), Complaint for Injunction, Civil Penalties, and other Equitable Relief, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/1%20-%20Complaint%20%28Disney%29.pdf>.
47. *People of the State of California v. Healthline Media, LLC* (Cal. Super. Ct. San Francisco Cnty. July 28, 2025, No. CGC25626794), Final Judgment and Permanent Injunction, accessed at: https://oag.ca.gov/system/files/attachments/press-docs/Signed%20Judgment_0.pdf.



48. *People of the State of California v. Jam City, Inc.* (Cal. Super. Ct. L.A. Cnty. Nov. 21, 2025, No. 25STCV34029), Final Judgment and Permanent Injunction, accessed at: https://oag.ca.gov/system/files/attachments/press-docs/CA_SUP_LAX_25STCV34029_Signed_Order_Final_Judgment.pdf.
49. *People of the State of California v. Sephora USA, Inc.* (Cal. Super. Ct. San Francisco Cnty. Aug. 24, 2022, No. CGC22601380), Final Judgment and Permanent Injunction, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/Filed%20Judgment.pdf.pdf>.
50. *People of the State of California v. Sling TV L.L.C; Dish Media Sales L.L.C* (Cal. Super. Ct. L.A. Cnty. Oct. 30, 2025, No. 25STCV31561), Final Judgment and Permanent Injunction, accessed at: <https://oag.ca.gov/system/files/attachments/press-docs/Final%20Judgment%20and%20Permanent%20Injunction%20%28People%20v%20Sling%20TV%29.pdf>.
51. *People of the State of California v. The Walt Disney Co.* (Cal. Super. Ct. L.A. Cnty. Feb. 11, 2026, No. 26STCV04425), Final Judgment and Permanent Injunction, accessed at: https://oag.ca.gov/system/files/attachments/press-docs/CA_SUP_LAX_26STCV04425_Final_Judgment_and_Permanent_Injunction.pdf.
52. Ron Wyden, Letter to Rob Bonta, Phil Weiser, Jennifer M. Urban, William Tong, Kathy Jennings, Anthony G. Brown, Austin Knudsen, Mike Hilgers, John Formella, Jennifer Davenport & Ken Paxton (Aug. 3, 2026), accessed at: https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_ags_on_gpc.pdf.
53. Sebastian Zimmeck et al., *Usability and Enforceability of Global Privacy Control* (2023), Proceedings on Privacy Enhancing Technologies, accessed at: <https://sebastianzimmeck.de/zimmeckEtAlGPC2023.pdf>.
54. Van Hong Tran et al., *Dark Patterns in the Opt-out Process and Compliance with the California Consumer Privacy Act (CCPA)*, CHI '25 Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (Apr. 26 – May 1, 2025), accessed at: <https://dl.acm.org/doi/epdf/10.1145/3706598.3714138>.
55. webXray, *California Privacy Audit: A Legal Minefield That Puts Users at Risk* (Mar. 2026), accessed at: <https://globalprivacyaudit.org/2026/california%20Privatea>.
56. Wesleyan University Editorial Staff, *New Study Probes If Online Retailers Follow Privacy Opt Outs*, Wesleyan University (Apr. 11, 2025), accessed at: <https://www.wesleyan.edu/about/news/2025/04/sebastian-zimmeck-consumer-reports-privacy-research.html>.

