AAAnow

54 Poland St, Soho,
London W1F 7NJ
United Kingdom

US State Privacy Laws:
Targeted Advertising and Profiling Opt-Out Rights (2026)

Cross-context behavioural advertising (cookies, pixels, trackers)
+ profiling in furtherance of legal or similarly significant effects decisions

Document Version: 1.2
Document Status: Client release
Dated: 21st February 2026

Contents

1 Purpose and scope

This provides a state-by-state assessment of US comprehensive consumer privacy laws (in force or taking effect) that create consumer controls over (1) targeted advertising, including cross-context behavioural advertising implemented via cookies, trackers, pixels, SDKs, or similar technologies, and (2) profiling in furtherance of decisions that produce legal or similarly significant effects. It is designed for policy, product, and compliance presentation use, with a master grid suitable for report insertion.

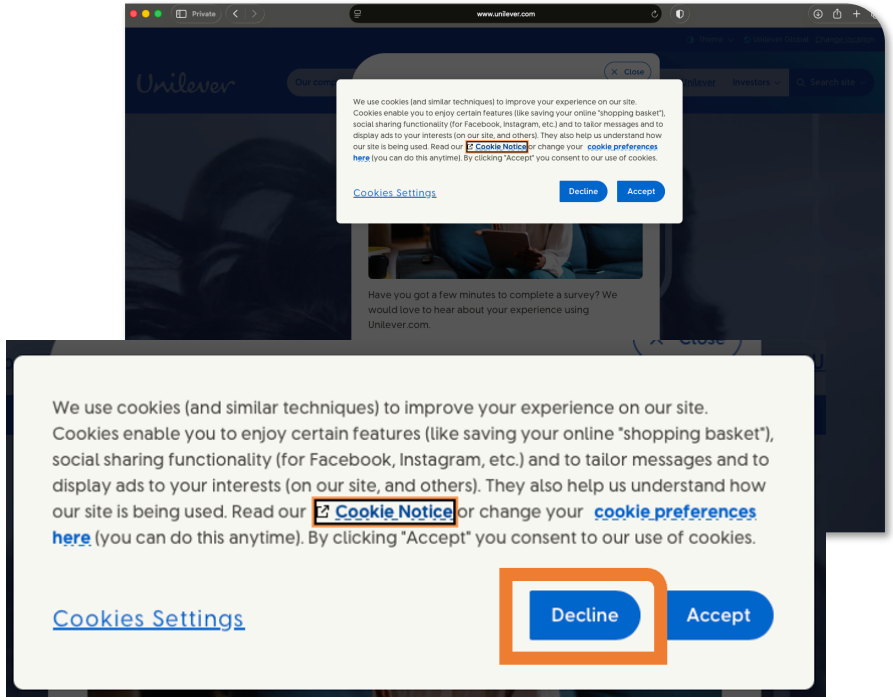
This paper does not attempt to summarise each state law in full. It focuses only on targeted advertising, cross-context behavioural advertising constructs, profiling / automated decision-making opt-outs tied to significant effects, and related opt-out mechanisms, including universal opt-out signals where applicable.

Online privacy compliance is under increasing scrutiny due to adtech practices, enforcement activity, and litigation and reputational exposure. This paper provides a state-by-state review of enacted comprehensive US consumer privacy laws as of January 2026, based on primary statute sources, regulator guidance, and reputable legal trackers.

1.1 illusion of choice

The central focus of this paper is the risk posed where tracking technologies (cookies, trackers, pixels, SDKs, or similar tools) operate before a consumer can exercise choice or continue despite a reject selection. This creates an “illusion of choice”: the user is presented with control, but data has already been collected and potentially disclosed to third parties, and the reject option does not function as expected.

Example
A website displays a cookie notice offering a “Reject” option. A user selects “Reject” expecting that tracking will not occur. If data collection or disclosure has already occurred before the selection is applied, or continues after rejection due to configuration or vendor behaviour, the user’s control is not effective and the notice may create an ***“illusion of choice.”***



2 Definitions and legal framing

2.1 Targeted advertising (cross-context behavioural advertising)

In most US state privacy laws, targeted advertising refers to displaying advertisements selected based on personal data derived from a consumer’s activities across non-affiliated websites or applications.

In operational terms, this (likely to be) *is* where cookies, trackers, pixels, SDKs, and related adtech tools sit, particularly when used across sites/apps to infer interests and target ads.

2.2 “Sale” vs “share” constructs (California)

Some states treat targeted advertising separately from “sale.”

California uses a distinct construct: opt-out of “sale” or “sharing”, where sharing specifically refers to disclosures for cross-context behavioural advertising, typically implemented through cookie/pixel controls and a “Do Not Sell or Share My Personal Information” mechanism. California’s approach should be mapped carefully rather than forced into the VA/CO model. [CIT-CA-AG-CCPA]

2.3 Profiling and automated decision-making (significant effects threshold)

Across the mainstream “comprehensive law” cluster (Virginia, Colorado, and similar statutes), the consumer opt-out for profiling is not a general opt-out of automation.

It is a right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. Virginia sets out the standard statutory phrasing. [CIT-VA-VCDPA]

2.4 “Legal or similarly significant effects”

This threshold is designed to capture decisions that materially affect a person, such as eligibility for employment, housing, credit, insurance, education, or similarly significant life outcomes.

It is intended to separate low-impact personalisation from high-impact decisioning.

3 Exposure analysis: reject option presented after tracking loads

A website presents a cookie banner offering “Reject” but, upon initial page load, tracking cookies/pixels and third-party requests fire before the user has a meaningful opportunity to reject.

3.1 Why this creates elevated exposure

Even in an opt-out regime (rather than an EU-style prior consent regime), this design pattern creates several enforceable concerns:

1) **Effectiveness failure (opt-out is too late)**

If targeted advertising trackers are firing before the rejection can be applied, the mechanism is not controlling processing “at the relevant time.”

This undermines the practical effectiveness of the opt-out right, which is a core requirement across states.

2) **Disclosure and onward transfer before control**

Many adtech flows involve immediate transmission to third parties (analytics/ad networks).

If personal data is disclosed before rejection, the consumer right is frustrated because the disclosure has already occurred.

3) **Deceptive interface risk**

Presenting a “Reject” option that does not prevent initial tracking creates a strong argument that the interface is misleading.

This can evolve into a “deceptive practice” issue under state unfair or deceptive acts and practices regimes (UDAP), even where the privacy statute itself is framed around opt-out rights.

4) **Governance and accountability exposure**

Where tag managers or consent platforms are misconfigured, controllers may lack the ability to demonstrate compliance.

This becomes evidentially problematic: regulators increasingly focus on whether controls work in practice.

3.2 Why the EU comparator matters (Condé Nast example)

The Condé Nast cookie enforcement example is EU-based and not direct US authority, but it illustrates how regulators interpret “choice architecture.” The key lesson is not EU consent law. The key lesson is the enforcement logic around illusory choice and the harm created when tracking occurs before the user can exercise the presented control. There is also a related cross boarder claim, with the California regulator proceeding with a complaint under the CIPA.

3.3 Likely US regulatory characterisation routes

Targeted advertising opt-out not honoured effectively (functional failure).

Misrepresentation of privacy controls (banner says reject, tracking still fires).

Unfair practice because consumers are exposed to tracking they reasonably believed they had prevented.

Colorado is particularly relevant because its rules emphasise timing and effective mechanisms around profiling opt-out, and it is widely treated as operationally stringent. [CIT-CO-RULES] [CIT-CO-CPA]

4 Risk Assessment (Your own)

4.1 Scenario

Risk manager would like to understand their own site, or site, independently of vendors or consultants, own technical staff.

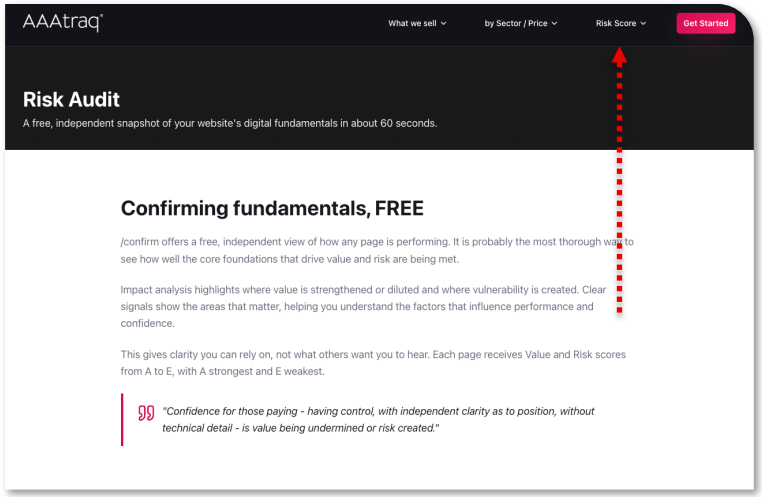
4.2 Self run

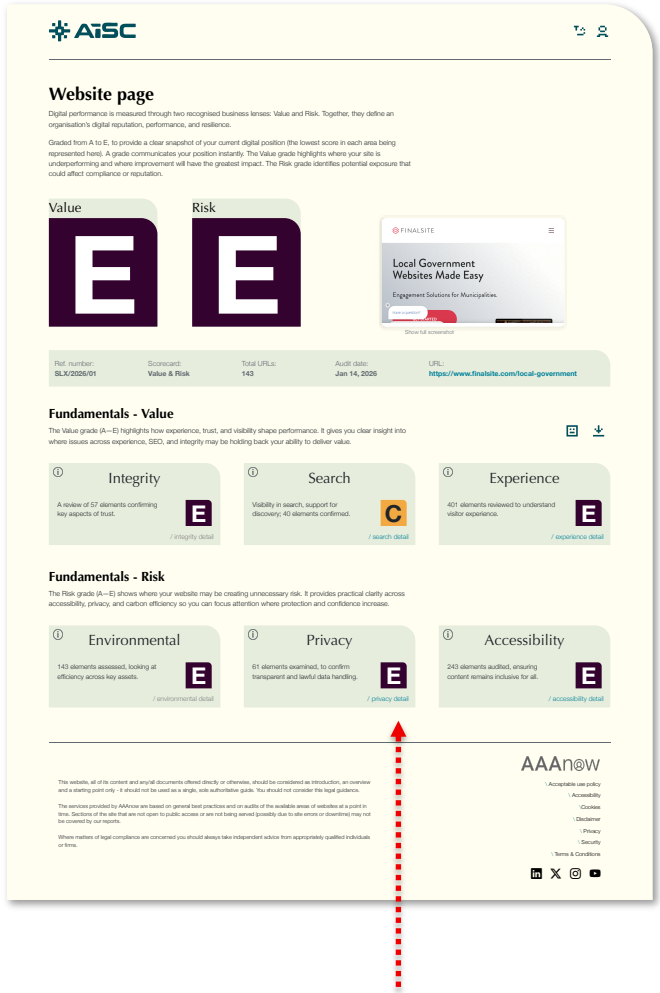
Using the free audit tool, offered by AAAtraq Risk manager can key in any address and carry out audit – results shown A – E (with E indicting highest level of exposure.

Visit https://web.aaatraq.com/risk-audit to do this, once run click on privacy for the detail (see arrow).

4.3 Full Audit / All websites

Via your broker (can also be requested at https://web.aaatraq.com/risk-audit) we offer an audit of all websites you own, operate or are responsible for, providing breakdown by website of exposure and overall summary.





5 Enforcement

A critical mistake is to think that data privacy authorities are turning a blind eye to failures to comply with key data privacy laws like the California Consumer Privacy Act. If anything, enforcement is accelerating. During 2025 there have been multiple lawsuits have resulted in fines, as well as potential damage to a company’s brand and reputation.

5.1 California:

- In March **2025** the American Honda Motor Co **were fined USD $632,500 for breaches of the CCPA**, including “using an online privacy management tool that failed to offer Californians their privacy choices in a symmetrical or equal way”. Essentially, they used a tool that allowed opt-in via one click, but required multiple steps to decline it.
- In May **2025** Todd Snyder was **fined $345,178 for breaches of the CCPA, caused** by the failure to configure and then monitor properly a cookie consent platform properly that meant it wasn’t working for 40 days and users could not opt out.
- In July **2025** Healthline Media **settled for a payment of USD $1.55 million** for breaching the California Privacy Protection Act (CCPA) in a number of ways, including failing “to opt consumers out of the sharing of their personal information for targeted advertising.” Additionally, Healthline Media was found to have “deceived” consumers through a consent banner that actually failed to disable tracking cookies.
- In October **2025** the Tractor Supply Company **received a $1.35 million fine** for various CCPA breaches. This included a failure to recognize opt-out preferences on its website, and a form that enabled people to indicate they didn’t want their personal information sold, but then failed to enact this via third-party tracking technologies.
- Global publisher Condé Nast is also currently **facing a class-action privacy lawsuit** in California alleging that trackers were installed on websites including *The New Yorker* and *Wired* without valid user consent, in violation of the California Invasion of Privacy Act (CIPA). A judge has allowed the case to proceed, with a trial date still to be set.

State of California Department of Justice

ROB BONTA
Attorney General

Search

Translate Website | Traducir Sitio Web

HOME ABOUT MEDIA CAREERS REGULATIONS RESOURCES PROGRAMS APPOINTMENTS CONTACT

Attorney General Bonta Announces Largest CCPA Settlement to Date, Secures $1.55 Million from Healthline.com

Press Release / *Attorney General Bonta Announces Largest CCPA Settlement to ...*

Tuesday, July 1, 2025

Contact: (916) 210-6000, agpressoffice@doj.ca.gov

Action represents fourth settlement, continued enforcement priority under the California Consumer Privacy Act

OAKLAND — California Attorney General Rob Bonta today announced a settlement with website publisher Healthline Media LLC (Healthline), resolving allegations that its use of online tracking technology on its health information website, Healthline.com, violated the California Consumer Privacy Act (CCPA). An investigation by the California Department of Justice (DOJ) found that Healthline failed to allow consumers to opt out of targeted advertising and shared data with third parties without CCPA-mandated privacy protections — including data suggesting that a person may have a serious health condition. The settlement includes $1.55 million in civil penalties and strong injunctive terms, including a novel term that prohibits Healthline from sharing article titles that reveal that a consumer may have already been diagnosed with a medical condition — banning the company from engaging in these types of data transmissions.

5.2 The situation in other US states

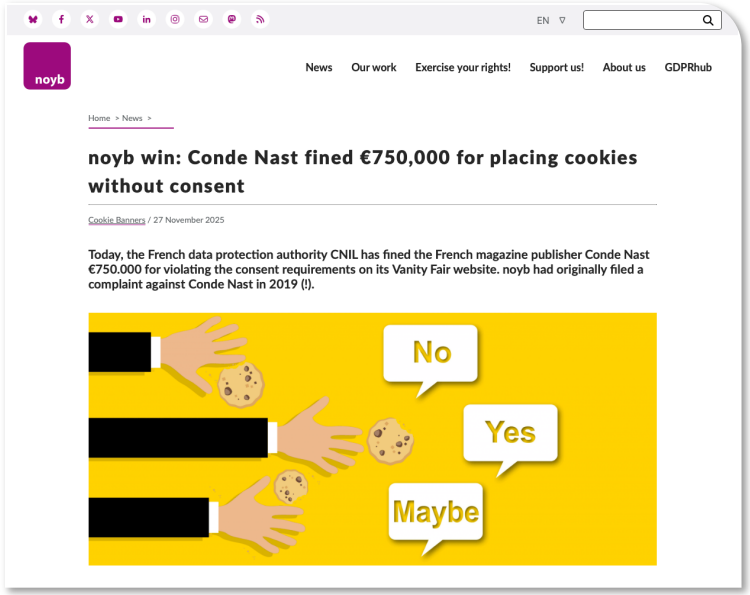
While the most notable activity might be focused on California, other states are playing catch-up. In April 2025, the Michigan Attorney General filed a lawsuit against Roku for collecting and sharing sensitive data relating to children, including via tracking pixels and cookies. The Texas Attorney General has also taken action on large companies including General Motors and Google for sharing information without consent.

Furthermore, the Attorney Generals of Colorado, Connecticut and California announced a joint investigation into whether businesses are properly honouring requests to opt out of having their data sold and receiving targeted advertising indicated through Global Privacy Control (GPC).

5.3 Regulation in Europe

In parallel, the picture in Europe is also one of tightening regulation:

- In September 2025 CNIL, the French data protection authority, fined retailer SHEIN 150 million euros for privacy breaches relating to cookies including failing to obtain consent, displaying incomplete cookie banners, a lack of information about the identity of third parties and the fact that new cookies were placed even if a user refused all cookies.
- Condé Nast was also fined 750,000 Euros by CNIL in November 2025, the French, for failing to obtain user consent before placing cookies on one of its French sites, although there are long-standing complaints about two others.
- Separately, in the UK, the Information Commissioner’s Office (ICO) has started more actively monitoring of the UK’s 1,000 websites while also dramatically increasing the potential fines for non-compliance.



6 Practical compliance controls (checklist)

6.1 Web/adtech controls

Tag manager configured to prevent pre-rejection marketing tag firing.

Pixel governance: no third-party calls before opt-out state is applied.

Cookie classification maintained and updated.

SDK review for mobile equivalents.

6.2 Opt-out implementation controls

Clear opt-out method for targeted advertising.

Ensure opt-out applies across devices where technically feasible.

Confirm opt-out applies to downstream adtech partners where contractually required.

Where applicable, implement and test universal opt-out signals.

6.3 Vendor / processor controls

Contracts include opt-out honouring obligations.

Third-party adtech disclosures and restrictions documented.

Ensure processors support suppression lists / opt-out propagation where applicable.

6.4 Evidence controls

Automated scans demonstrating tag order.

Records showing opt-out preference signal detection and application.

Audit logs of consumer opt-out processing.

6.5 Practical mitigation measures (technical and governance)

<u>Technical controls</u>

1. Implement true pre-fire governance in tag manager: no third-party marketing tags before opt-out state resolved.
2. Separate essential vs advertising/analytics tags, with strict defaults.
3. Confirm that pixels do not load until opt-out status permits.
4. Audit network calls on first page load (browser dev tools, automated scanning).

<u>Governance controls</u>

1. Maintain a tag inventory and vendor list with mapped purposes.
2. Implement change control for tag additions (ticketing and approvals).
3. Evidence pack: logs showing opt-out honoured, tag firing sequence, and preference persistence

7 APPENDIX sources and citations (by state)

7.1 Core statutory and regulator anchors

Virginia

Virginia Consumer Data Protection Act (statutory text; opt-out includes targeted advertising, sale, and profiling significant effects). [CIT-VA-VCDPA]

Colorado

Colorado Revised Statutes, § 6-1-1306 opt-out includes targeted advertising, sale, profiling significant effects. [CIT-CO-CPA]

Colorado profiling opt-out rules (4 CCR 904-3-9.04). [CIT-CO-RULES]

Practical resource note on universal opt-outs for targeted ads/sales (secondary but useful for presentation). [CIT-CO-UOOM]

Connecticut

Connecticut 2025 amendments analysis confirming profiling right expanded beyond “solely automated”. [CIT-CT-AMEND]

California

California Attorney General CCPA page explaining “sharing” refers specifically to cross-context behavioural advertising. [CIT-CA-AG-CCPA]

Industry legal analysis on cross-context behavioural advertising mechanics (useful as secondary clarification, not authority). [CIT-CA-SECONDARY]

Reference sources (recommended for final publication hardening)

For each state in the master grid, the final publication version should add:

Official statute link (state legislature or official code repository)

Attorney General guidance where available

Reputable legal analysis for definitions and effective dates

Note: In this draft, citations are anchored to the most widely used statutory and regulator exemplars to ensure legal correctness of the targeted advertising and profiling significant effects framing.

Links (references used)

Virginia VCDPA (overview / statute reference): https://law.lis.virginia.gov/vacode/title59.1/chapter53/
Colorado CPA statute (opt-out section): https://law.justia.com/codes/colorado/title-6/article-1/part-13/section-6-1-1306/
Colorado CPA Rules (profiling opt-out, 4 CCR 904-3): https://coag.gov/resources/colorado-privacy-act/
California AG CCPA (sharing and CCBA): https://oag.ca.gov/privacy/ccpa
Connecticut amendments commentary: https://iapp.org/news/a/connecticuts-privacy-law-amendments-broaden-consumer-rights-expand-data-types-covered/
Cross-context behavioural advertising explanation (secondary): https://www.ropesgray.com/en/insights/alerts/2023/01/california-privacy-rights-act-regulations-what-your-business-should-know
EU comparator (Condé Nast cookie enforcement): https://noyb.eu/en/noyb-win-conde-nast-fined-eu750000-placing-cookies-without-consent
https://iapp.org/resources/article/us-state-privacy-legislation-tracker
https://www.ropesgray.com/en/sites/state-privacy-law-tracker
https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/
https://www.mayerbrown.com/en/insights/resource-centers/cybersecurity-and-data-privacy-resource-center/state-privacy-law-tracker

State	Law name (acronym)	Effective date	Targeted advertising opt-out	Cross-context behavioural advertising captured (cookies/pixels/trackers)	Profiling opt-out (legal or similarly significant effects)	Required opt-out mechanisms (link, preference centre, UOOM, etc.)	Universal opt-out signal required?	Enforcement authority	Notes (one-line, practical)
Alabama	None								
Alaska	None								
Arizona	None								
Arkansas	None								
California	CCPA/CPRA (CCPA) *California Invasion of Privacy Act (CIPA).*	Jan 1, 2020	Yes	Yes (share = CCBA)	No (not the VA/CO “significant effects” profiling opt-out model)	“Do Not Sell or Share” style link and rights request methods	Yes	CA AG and CPPA (split enforcement)	CCBA is treated under “share”; cookies and trackers are central in practice. (California Attorney General)
California	*California Invasion of Privacy Act (CIPA).*	Under CIPA, plaintiffs commonly argue that deploying third-party tracking code that captures and transmits user interaction data to a third party without valid consent can constitute unlawful “interception” or “eavesdropping” under California Penal Code § 631(a). Separately, some web-tracking claims allege that certain tracker configurations operate like a “pen register” / “trap and trace” device and therefore violate California Penal Code § 638.51(a) when implemented without the legally required authorization (often framed as lack of consent and/or the statute’s order requirement). Note: the Condé Nast tracker complaint explicitly pleads **CIPA § 638.51(a)** in connection with installing and using trackers without prior consent / authorization.							
Colorado	Colorado Privacy Act (CPA)	Jul 1, 2023	Yes	Yes (targeted ads scope)	Yes	Controller method plus UOOM where applicable	Yes	AG and District Attorneys	Enforcement is AG or DAs only. (leg.colorado.gov)
Connecticut	Connecticut Data Privacy Act (CTDPA)	Jul 1, 2023	Yes	Yes	Yes	Controller method plus opt-out preference signal where applicable	Yes	Attorney General	CT AG publishes enforcement reporting and guidance. (CT.gov)
Delaware	Delaware Personal Data Privacy Act (DPDPA)	Jan 1, 2025	Yes	Yes	Yes	Controller method plus UOOM where applicable	Yes	Attorney General	Listed as enacted comprehensive law by CIPL; UOOM requirement reflected in UOOM summaries.
Florida	Florida Digital Bill of Rights (FDBR)	Jul 1, 2024	Yes	Yes (definition is atypical vs other states)	Yes	Controller method (not a 2026 UOOM	No (not shown as	Attorney General	FL Senate summary lists opt-outs including targeted

State	Law name (acronym)	Effective date	Targeted advertising opt-out	Cross-context behavioural advertising captured (cookies/pixels/trackers)	Profiling opt-out (legal or similarly significant effects)	Required opt-out mechanisms (link, preference centre, UOOM, etc.)	Universal opt-out signal required?	Enforcement authority	Notes (one-line, practical)
						state in the cited UOOM list)	required by 2026)		ads and significant-effects profiling. (Florida Senate)
Georgia	SB 111 Georgia Consumer Privacy Protection Act								
Hawaii	SB 1037								
Idaho	None								
Illinois	HB 3041 Illinois Data Privacy and Protection Act								
Indiana	Indiana Consumer Data Protection Act (ICDPA)	Jan 1, 2026	Yes	Yes	Yes	Controller method (link or preference centre style)	No (not shown as required by 2026)	Attorney General	Enacted comprehensive law effective 2026.
Iowa	Iowa Consumer Data Protection Act (ICDPA)	Jan 1, 2025	Yes (operationally present; rights framing differs across summaries)	Yes	No	Controller method (and disclosures); no UOOM requirement	No	Attorney General	Multiple analyses note no profiling opt-out; no UOOM requirement. (OneTrust)
Kansas	None								
Kentucky	Kentucky Consumer Data Protection Act (KCDPA)	Jan 1, 2026	Yes	Yes	Yes	Controller method (link or preference centre style)	No (not shown as required by 2026)	Attorney General	Enacted comprehensive law effective 2026.
Louisiana	None								
Maine	None								
Maryland	Maryland Online Data Privacy Act (MODPA)	Oct 1, 2025	Yes	Yes	Yes	Link plus opt-out preference signal requirement (per compliance summaries)	Yes	Attorney General	Maryland is cited as requiring opt-out preference signals by 2025–2026 in compliance guidance. (Data Matters Privacy Blog)
Massachusetts	S 2619 Massachusetts Data Privacy Act H 4746 Massachusetts Consumer Data Privacy Act								
Michigan	SB 359 Personal Data Privacy Act								

State	Law name (acronym)	Effective date	Targeted advertising opt-out	Cross-context behavioural advertising captured (cookies/pixels/trackers)	Profiling opt-out (legal or similarly significant effects)	Required opt-out mechanisms (link, preference centre, UOOM, etc.)	Universal opt-out signal required?	Enforcement authority	Notes (one-line, practical)
Minnesota	Minnesota Consumer Data Privacy Act (MCDPA)	Jul 31, 2025	Yes	Yes	Yes	Controller method plus UOOM where applicable	Yes	Attorney General	Listed as enacted comprehensive law and included in 2026 UOOM states list. (Data Matters Privacy Blog)
Mississippi	SB 2015 Mississippi Consumer Data Privacy Act								
Missouri	None								
Montana	Montana Consumer Data Privacy Act (MCDPA)	Oct 1, 2024	Yes	Yes	Yes	Controller method plus UOOM where applicable	Yes	Attorney General	Montana is included in the 2026 UOOM list. (Data Matters Privacy Blog)
Nebraska	Nebraska Data Privacy Act (NDPA)	Jan 1, 2025	Yes	Yes	Yes	Controller method plus UOOM where applicable	Yes	Attorney General	Nebraska is included in the 2026 UOOM list. (Data Matters Privacy Blog)
Nevada	None								
New Hampshire	New Hampshire Data Privacy Act (SB 255)	Jan 1, 2025	Yes	Yes	Yes	Controller method plus UOOM where applicable	Yes	Attorney General	New Hampshire is included in the 2026 UOOM list. (Data Matters Privacy Blog)
New Jersey	New Jersey Data Protection Act (NJDPA)	Jan 15, 2025	Yes	Yes	Yes	Controller method plus UOOM where applicable	Yes	Attorney General	New Jersey is included in the 2026 UOOM list. (Data Matters Privacy Blog)
New Mexico	None								
New York	A 5827 American Data Privacy and Protection Act A 4947 New York Privacy Act A 3044 New York Privacy Act (C) A 8158 New York Privacy Act (C) A 974 New York Data Protection Act (C) S 8524 New York Data Protection Act (C)								
North Carolina	H 462 North Carolina Personal Data Privacy Act S 757 North Carolina Consumer Data Privacy Act								

State	Law name (acronym)	Effective date	Targeted advertising opt-out	Cross-context behavioural advertising captured (cookies/pixels/trackers)	Profiling opt-out (legal or similarly significant effects)	Required opt-out mechanisms (link, preference centre, UOOM, etc.)	Universal opt-out signal required?	Enforcement authority	Notes (one-line, practical)
North Dakota	None								
Ohio	None								
Oklahoma	None								
Oregon	Oregon Consumer Privacy Act (OCPA)	Jul 1, 2024 (for-profit); Jul 1, 2025 (nonprofit); UOOM Jan 1, 2026	Yes	Yes	Yes	Controller method plus universal opt-out signals from Jan 1, 2026	Yes	Attorney General	Oregon has staged applicability and a 2026 UOOM requirement. (TrustArc)
Pennsylvania	HB 78 Consumer Data Privacy Act SB 112 Consumer Data Privacy Ac								
Rhode Island	Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)	Jan 1, 2026	Yes	Yes	Yes	Controller method (no UOOM requirement)	No	Attorney General	Rhode Island explicitly does not require UOOM recognition. (dwt.com)
South Carolina	SB 112								
South Dakota	None								
Tennessee	Tennessee Information Protection Act (TIPA)	Jul 1, 2025	Yes	Yes	Yes	Controller method (link or preference centre style)	No (not shown as required by 2026)	Attorney General	Enacted comprehensive law effective 2025. (Data Matters Privacy Blog)
Texas	Texas Data Privacy and Security Act (TDPSA)	Jul 1, 2024; UOOM Jan 1, 2025	Yes	Yes	Yes	Controller method plus UOOM from Jan 1, 2025	Yes	Attorney General	UOOM is delayed to Jan 1, 2025 under common compliance guidance. (Didomi)
Utah	Utah Consumer Privacy Act (UCPA)	Dec 31, 2023	Yes	Yes	No	Controller method (no UOOM requirement)	No	Attorney General	Utah does not include significant-effects profiling opt-out; no UOOM requirement. (OneTrust)
Vermont	Vermont has a later privacy bill, S.71 (consumer data privacy and online surveillance), which includes draft text referring to a “Vermont Data Privacy Act,” but it is in bill process, not enacted law.								

State	Law name (acronym)	Effective date	Targeted advertising opt-out	Cross-context behavioural advertising captured (cookies/pixels/trackers)	Profiling opt-out (legal or similarly significant effects)	Required opt-out mechanisms (link, preference centre, UOOM, etc.)	Universal opt-out signal required?	Enforcement authority	Notes (one-line, practical)
Virginia	Virginia Consumer Data Protection Act (VCDPA)	Jan 1, 2023	Yes	Yes	Yes	Controller method (link or preference centre style)	No (not shown as required by 2026)	Attorney General	Standard “VA model” includes significant-effects profiling opt-out.
Washington	None (comprehensive consumer privacy)		No	N/A	No	N/A	N/A	N/A	Not enacted as a comprehensive consumer privacy law in the cited enacted set (separate health-data law exists).
West Virginia	HB 2953 Consumer Data Protection Act HB 2987 Relating to the Consumer Data Protection Act								
Wisconsin	SB 166 AB 172								
Wyoming	None								