NAI
PRIVACY, TRUST & ACCOUNTABILITY

The NAI's *Annual Report* 2025

PUBLICATION DATE
May 13, 2026

PRIVACY · TRUST · ACCOUNTABILITY

Table of Contents

I. Introduction

A new chapter in the NAI's story.

IN THIS SECTION

I. Introduction

A Message from the President & CEO

Welcome to a new chapter in the NAI's story. This year's annual report marks a deliberate departure from the format you may be accustomed to, reimagined from the ground up to be more accessible, more transparent, and more useful to the diverse audiences who engage with our work. The NAI celebrated 25 years of privacy self-regulation in 2025, and we wanted to write a report that reflects both the depth of the year behind us and the clarity our community deserves heading into the next 25 years of responsible, data-driven advertising.

This past year was, by every measure, pivotal for the NAI. Today, we find ourselves at the center of an industry that bears little resemblance to the one we set out to self-regulate in 2000, and yet the core challenge remains strikingly familiar: how do we enable innovation in digital advertising while ensuring meaningful, durable protections for consumers? Reaching this milestone gave us occasion to reflect on the principles that have anchored the NAI from the start, and to recommit to the standards-setting, member accountability, and policy engagement that have defined our work across 25 years of profound technological and regulatory change.

> ***Our work has never been more consequential.***

The privacy and data-protection landscape grew dramatically more complex in 2025, with new state comprehensive privacy laws taking effect, federal proposals advancing, enforcement priorities shifting, and international frameworks adding further layers of obligation for companies operating across borders. For NAI members, navigating this patchwork, and meeting the higher expectations that regulators, lawmakers, and the public now have for the digital advertising ecosystem, has become a defining business challenge. Our Self-Regulatory Framework, technical guidance, and strong standards evolved alongside this landscape to give members a credible path to demonstrable compliance.

This report is written for everyone with a stake in what comes next. Our members will find a record of the past year's accomplishments and a roadmap for the year ahead. Companies considering NAI membership will find a clear articulation of what we offer and why it matters. Lawmakers and policymakers will find evidence of how industry self-regulation, done thoughtfully, can complement and strengthen statutory regimes. And the broader ad-tech industry will find thought leadership through standards that define responsible privacy and data protection practices. Across all of these audiences, one conclusion comes through clearly: the NAI's value proposition—rigorous standards, accountable practices, and a credible voice in shaping privacy policy—is stronger than ever.

The pages that follow tell the story of a year in which the NAI and its members rose to meet a complex and consequential moment. I am proud of what we have accomplished together, and I am energized by what lies ahead.

Leigh Freund | *President & CEO*, The NAI

About the NAI

The voice of third-party advertising technology since 2000.

Founded in 2000, the NAI (Network Advertising Initiative) is the leading non-profit self-regulatory association dedicated to responsible data practices in digital advertising. 2025 marked the NAI's 25th year of continuous operation—making it the longest-running privacy self-regulatory program in the digital advertising industry. For its entire history, the NAI has worked at the intersection of privacy, technology, and policy to promote accountability across the advertising technology ecosystem.

The NAI serves as the voice of the third-party advertising technology industry. Our mission is built on three pillars:

Guidance

We provide specialized, practical resources designed to help advertising technology companies navigate a complex and rapidly evolving legal and compliance landscape. From our Self-Regulatory Framework to our working group outputs, our guidance translates broad legal requirements into operational practice.

Advocacy

We advocate for legislation and regulation that balances strong consumer privacy protections with the ability to sustain effective, data-driven advertising. We engage with federal and state policymakers, regulators, and enforcement agencies to ensure that the advertising technology perspective is represented in policy conversations.

Education

We work to build a culture of privacy within the advertising technology industry—helping companies understand that good privacy practices are not a cost center, but a foundation for long-term trust, competitiveness, and business success.

NAI membership requires participation in our Self-Regulatory Framework, including annual Privacy Reviews. This commitment to ongoing accountability distinguishes the NAI from trade associations and advocacy groups that focus exclusively on policy positions. Our members don't just talk about privacy—they undergo independent review.

The NAI's Model for Self-Regulation: A Virtuous Cycle

A new model for self-regulation.

The NAI's self-regulatory model creates a **feedback loop** where industry guidance, member collaboration, and regulator engagement reinforce each other to keep members ahead of the curve:

DEVELOP

Industry-leading Guidance

The NAI develops industry-leading guidance, best practices, and voluntary programs aligned with evolving privacy law—so members have a clear, actionable compliance roadmap without building one from scratch.

REVIEW

Annual Privacy Reviews

The NAI conducts annual privacy reviews and working groups with members, giving them direct access to best practices and regulator expectations, while surfacing where new guidance is needed most.

ENGAGE

Direct Policy Engagement

The NAI engages directly with regulators and policymakers at the federal and state level and brings back real-time insight into regulatory priorities and expectations that members can act on immediately.

Each phase strengthens the next: regulator conversations sharpen our guidance, guidance shapes member practices, and member experience informs how we engage regulators.

II. Organizational Update

A year of building, reviewing, and engaging.

IN THIS SECTION

— Membership
— Working Groups and Task Forces
— Self-Regulatory Framework
— Guidance, Standards & Best Practices
— Industry & Consumer Resources

II. Organizational Update

The NAI in Numbers

SINCE 2000	+4 NEW THIS CYCLE	2025 CYCLE COVERAGE	SINCE LAST REPORT
25 years of self-regulation	**74** member companies	**70+** privacy reviews completed	**7** documents & resources published

Membership

From early-stage startups to the largest ad-tech companies.

The NAI's **74 members** range from early-stage startups to large advertising technology companies, and collectively represent a significant share of the infrastructure that powers digital advertising in the United States. A quick glance at our extended membership directory shows the diversity and interconnectivity of our membership, which includes:

DSP
Demand-Side Platforms
that enable advertisers to reach audiences efficiently across digital channels.

SSP
Supply-Side Platforms
and exchanges that help publishers manage and monetize their advertising inventory.

DATA
Data Providers & Platforms
that enable audience segmentation, targeting, and measurement while managing consumer data responsibly.

ANALYTICS
Measurement & Attribution
companies that help advertisers understand campaign performance and allocate spend effectively.

IDENTITY
Identity & Infrastructure
providers that support the technical foundations of data-driven advertising, including privacy-preserving identity solutions.

AND MORE
From advertisers and publishers to measurement companies and identity providers, our membership reflects the full diversity of the digital advertising ecosystem.

Member Retention and Growth

Welcoming new members, retaining old ones.

The NAI welcomed **four new members** in the 2025 review cycle and **retained 92% of its existing members**, reflecting the continued value that companies find in NAI membership. Although the NAI did lose some members, these losses were largely the result of industry consolidation rather than voluntary departures.

Our members find tremendous value in all aspects of the NAI program, from privacy reviews to peer collaboration to policy thought leadership and advocacy. Here is what one of our members says about the NAI:

> *At AlikeAudience, we are committed to upholding the highest standards of data responsibility and transparency across the digital advertising ecosystem. Successfully completing the NAI review reinforces our dedication to privacy-first practices and industry compliance. We believe that responsible data usage is foundational to building long-term trust with our partners and clients, and we are proud to align with NAI's rigorous standards as we continue to deliver high-quality, privacy-compliant audience solutions globally.*
>
> — **Bosco Lam** | *CEO, AlikeAudience*

The NAI Working Groups

Structured collaboration: now more essential than ever.

As the advertising technology industry navigates an era of accelerating regulation and rapid technological change, structured collaboration around consumer privacy and trust has never been more important. The NAI's working groups provide a dedicated monthly forum for member companies, legal experts, and industry partners to engage with emerging privacy challenges and develop practical, consensus-driven solutions. In 2025, they produced several significant guidance documents, and shaped the NAI's policy positions on key regulatory developments.

Public PolicyWorking Group

This group focuses on federal and state legislative and regulatory developments that affect the advertising technology industry. In 2025, the group tracked and analyzed state privacy legislation and regulatory actions, provided strategic input on NAI comment letters and policy submissions, and helped develop the NAI's policy positions.

Legal & Regulatory Working Group

This group focuses on translating legal and compliance requirements into practical guidance for NAI members. In 2025, the group's work directly informed several major NAI publications, described below, and provided ongoing analysis of new and amended state privacy laws. The Legal and Regulatory Working Group is the primary vehicle for developing thoughtful, member-driven comments on proposed state regulations.

Specialized Task Forces

In addition to our two main working groups, the NAI operates focused task forces that allow participants to direct their engagement toward the issues most relevant to their organizations:

Consumer Choice Task Force

is developing best practices around Opt-Out Preference Signals and Universal Opt-Out Mechanisms to address one of the most operationally challenging areas of state privacy law compliance.

Sensitive / Health Data Task Force

drives the development of the Factor Analysis for HSPI and continues to monitor regulatory developments affecting health-related advertising.

Location Task Force

supports the administration of the Precise Location Information Voluntary Enhanced Standards and is currently contributing to the development of the forthcoming Location Data Best Practices.

Data Broker Task Force

monitors and supports compliance with state data broker laws, including the California Delete Act, and tracks emerging regulatory developments affecting data broker registration, consumer deletion rights, and related obligations.

The NAI is grateful to the member companies, law firms, and partners who dedicate time and expertise to these collaborative efforts. The working groups and task forces remain open to all NAI members, and we encourage broad participation in a landscape that promises continued regulatory evolution.

Self-Regulatory Framework & Resources

The NAI, together with key industry partners, spent the last several years rethinking its role, and launched a new model for self-regulation, including a new framework and a range of work products to shape the industry, set standards and guide members.

DECEMBER 2024

The NAI Self-Regulatory Framework

The NAI published the Network Advertising Initiative Principles and Self-Regulatory Framework, replacing the 2020 NAI Code of Conduct and ushering in a new era of self-regulation. Membership in the NAI requires participation in the Framework, which is designed to promote strong privacy practices for members engaged in Network Advertising. The Framework is comprised of three core components: (1) the NAI Principles for Privacy in Network Advertising, which establish baseline privacy standards that all members must adhere to; (2) standards of review for each Principle, serving as a guide for the NAI's annual privacy reviews with members; and (3) privacy guidance, tools, and best practices intended to help members uphold the Principles and develop processes for compliance with evolving U.S. privacy law requirements.

→ Read the Framework

OCTOBER 2024

Precise Location Information Solution Provider Voluntary Enhanced Standards

The NAI updated the Precise Location Information Solution Provider Voluntary Enhanced Standards (VES), which were initially released in June 2022. These Enhanced Standards prohibit the use, sale, and transfer of U.S. consumer precise location information related to sensitive points of interest. They also restrict participating companies from using, selling, or sharing any U.S. consumer precise location information for law enforcement or national security purposes, except when needed to comply with a legal requirement. The 2024 updates clarify how nationally recognized industry classification systems, such as the North American Industry Classification System (NAICS), can be used to identify sensitive POIs and comply with the Enhanced Standards, and improve administrability among signatories.

→ View Enhanced Standards

Guidance, Standards & Best Practices

MARCH 2026 — MEMBERS ONLY

The NAI Data Governance Checklist

The NAI published a Data Governance Checklist and Template to help member companies create or update written data governance programs aligned with the NAI Privacy Principles and regulatory expectations. The resource supports the NAI's Data Governance Principle and helps companies demonstrate accountability during annual NAI Privacy Reviews. To request access, contact membership@thenai.org.

FEBRUARY 2026

Factor Analysis for Health-Related Sensitive Personal Information

The NAI released a framework for evaluating whether personal information processed in advertising contexts qualifies as sensitive health data under U.S. privacy laws. The Factor Analysis for Health-Related Sensitive Personal Information (HSPI) ("Factor Analysis") helps companies navigate a fragmented regulatory landscape that can result in over-classification of benign data, under-classification of genuinely sensitive data, or companies withdrawing from jurisdictions altogether. The framework introduces five factors for assessing sensitivity: the source of the data, its contents, its intended use, whether consumers have a heightened expectation of privacy, and the risk of harm. Health-data sensitivity is contextual and fact-dependent; even neutral data can become sensitive depending on how it is collected and used. The Factor Analysis is a practical tool to help companies reason through close cases and arrive at sound data classifications that preserve the benefits of responsible health-related advertising.

→ Read the Factor Analysis

OCTOBER 2025

A Primer on Privacy-Enhancing Technologies

The NAI released a primer designed to help privacy professionals understand how Privacy-Enhancing Technologies (PETs) can protect consumer privacy and safeguard proprietary data while still enabling effective data-driven advertising. The paper examines four key PETs and their practical advertising applications. The primer also acknowledges that PETs involve trade-offs between accuracy and utility and are not a substitute for a robust privacy program, but can meaningfully complement existing data governance and compliance efforts across the industry.

→ Read the Primer

NOVEMBER 2023

Demographic Health Advertising Best Practices

The NAI released recommended best practices (known as Demographic Health Advertising Best Practices) outlining how companies can utilize demographic consumer data for health-related advertising. This guidance bolsters consumer privacy protections around sensitive consumer health information, while also providing for effective health advertising that benefits consumers and healthcare professionals.

→ View Best Practices

SEPTEMBER 2023

Legal & Regulatory Analysis: Sensitive Health Advertising

The NAI published the NAI Legal & Regulatory Analysis: Sensitive Health Advertising. This legal analysis explores state privacy laws, federal enforcement actions, and associated guidance and offers recommendations about how sensitive health data should be defined and treated.

→ Read Analysis

MARCH 2023

State Law Processing Addendum

The NAI launched the NAI State Law Processing Addendum, sample contracting language to help advertising and publisher partners address new contracting requirements in 2023. This addendum addresses key issues in the industry and provides a solid foundation for disclosures of advertising-related transactions within the United States.

→ View Addendum

APRIL 2022

Best Practices for User Choice and Transparency

The NAI published a set of Best Practices for User Choice and Transparency to help member companies better understand the practice of dark patterns and to implement the highlighted best practices to avoid them. This resource has a threefold purpose: to explain consumer choice and transparency obligations under the NAI Code; to examine the current legal environment at the state and federal levels; and to identify best practices and guide companies in maximizing effective and efficient notice and choice mechanisms with respect to collecting consumer data. Certain terms used in state and federal regulation may not line up precisely with terms used in the NAI Code; in those instances, we have noted the appropriate term in the NAI Code that would apply.

→ View Best Practices

Industry & Consumer Resources

MARCH 2026

Consumer Input & Feedback Form

The NAI published a Consumer Input & Feedback section on the NAI website in March 2026 to provide a way for consumers and the public to share information, concerns, and experiences related to advertising technology practices with NAI members. The information collected within the form will be used to inform NAI reviews of NAI member companies' practices, identify trends, and promote improved practices and accountability across the ad-tech industry.

MARCH 2026

The NAI Member Badge

In March 2026, the NAI launched a NAI member badge that NAI members can embed on their websites; the badge links out to a verification page. Displaying the badge signals to visitors, partners, and regulators that the company participates in the NAI's industry-led self-regulatory framework and is committed to responsible data practices in digital advertising. For more information send an email to membership@thenai.org.

JANUARY 2026

Benefits of Tailored Advertising White Paper

In January 2026, the NAI updated a comprehensive white paper highlighting research on the benefits of tailored advertising for small and medium-sized businesses, publishers, society, and consumers. This paper shows that tailored advertising is the most widely utilized type of digital advertising because it maximizes the relevance and effectiveness of campaigns by tailoring the ads consumers see based on websites they visit, products they search for, and apps they use.

→ Read White Paper

SEPTEMBER 2025

Consumer Privacy Resources

In September 2025, the NAI undertook a significant modernization of its consumer privacy resources, aligning its tools and guidance with its new Self-Regulatory Framework and evolving U.S. state and federal privacy requirements:

- **GPC Browser Extension:** The NAI created a user-friendly Global Privacy Control (GPC) browser extension, designed to deploy Opt-Out Preference Signals in compliance with privacy laws across more than a dozen states. The extension prioritizes usability while ensuring legal consistency across multiple state frameworks.
- **Advertising Privacy Settings:** The NAI also expanded its consumer guidance by publishing step-by-step instructions for exercising privacy choices directly with NAI member companies, as well as across major technology platforms—including web browsers, mobile devices, connected TVs, and streaming devices.
- **Launch of Consumer Choice Task Force:** To support ongoing industry compliance, the NAI established a Consumer Choice Task Force charged with developing best practices around Opt-out Preference Signals and Universal Opt-out Mechanisms. The task force is designed to engage a broad coalition of stakeholders, including policymakers, researchers, consumer advocates, and user design experts.
- **Opt-Out Tools Sunset:** In parallel, the NAI retired its legacy cookie-based and email-based opt-out tools, which were tied to its now-deprecated Code of Conduct. To ensure continued opt-out access under industry self-regulatory standards, the NAI has integrated the Digital Advertising Alliance's AdChoices tools into its consumer opt-out page.

→ View on Our Website

III. Privacy Review Findings

The first review cycle under the new Framework.

IN THIS SECTION

— Findings on Transparency
— Findings on Consumer Choice and Control
— Findings on Sensitive Personal Data
— Findings on Data Governance
— Looking ahead to 2026

III. 2025 Privacy Review Program Findings

The Privacy Review Program is designed to support member companies in upholding high privacy standards, deepening their understanding of applicable legal requirements, and implementing processes and privacy practices that advance a robust compliance posture—helping members honor consumers' rights, meet regulator expectations, and demonstrate robust data governance practices to partners. Through the Privacy Review Program, the NAI receives valuable feedback from members about how advertising technology is evolving and the real obstacles that arise when operationalizing processes to support strong privacy programs.

The NAI actively incorporates the feedback and insights generated from its members' annual privacy reviews in its work, particularly those regarding emerging concerns and compliance challenges. This feedback plays a critical role in shaping the NAI's self-regulatory and policymaker engagement efforts, the development of practical tools and guidance, such as best practices, and the creation of resources for the broader membership to improve regulatory readiness and competitive positioning.

In this first review cycle under the Framework, the NAI staff conducted over 70 reviews[1], inclusive of annual reviews of established members, as well as new members joining the NAI (as part of their application process). The reviews included requests for information about each member company's use of technologies, privacy disclosures, data processing practices, and offerings for consumer choice and processing of rights requests. Members submitted written responses and provided excerpts and additional documentation when appropriate, such as terms of use, advertisements, policies, and FAQs. After receiving the responses, the NAI Privacy Review Team reviewed the information provided, alongside publicly available information, consumer choice mechanisms, and disclosures to assess adherence with the NAI Framework.

High-Level Takeaways:

Written Data Governance Is Now a Baseline Expectation

Federal and state regulators increasingly require documented governance programs—not just good practices—and the NAI's new Data Governance Checklist and Template (members-only) equips members to meet that expectation.

Sensitive Data Classification Is Top Priority, But Also an Ongoing Challenge

The NAI staff found meaningful variation in how members classify sensitive data, and hopes the NAI's new Factor Analysis is a tool that will help members make consistent, defensible classifications.

[1] As of publication, the NAI staff is finalizing privacy reviews with three member companies.

Conditional Rights Language Should Be Avoided

State regulators have explicitly rejected conditional phrasing like "you may have certain rights depending on where you live" as evidence of noncompliance, so members are encouraged to state rights clearly and universally or maintain a current, state-specific list.

GPC Now Presents Both Technical and Disclosure Obligations

Honoring opt-out signals like GPC is no longer enough, as regulators now expect businesses to accurately explain in their privacy notices how those signals are processed, and a new 2026 CCPA requirement mandates on-site display for how signals are processed.

Fulfillment of Data Rights Requests Is Getting More Complex, Requires Thoughtful Processing

Regulators now expect deletion and access requests to cover derived, inferred, and back-end data across data environments, making DSAR fulfillment one of the most operationally demanding compliance challenges members face.

Following the review of responses and other materials, the NAI staff met with representatives from reviewed member companies to discuss the company's practices, including any follow-up questions, and shared observations related to choice mechanisms and consumer rights request portals. These meetings provided the NAI staff with additional in-depth insight into each company's services and greatly increased the NAI staff's ability to flag potential privacy issues for members. Staff reviewed changes in law and technology that were relevant to each member, explored best practices reflected in NAI guidance and regulator enforcement efforts, and highlighted enforcement priorities that may be useful to the member company in evaluating its compliance posture. Staff made best practice suggestions and discussed various compliance challenges, including feedback on the member's practices organized under the NAI Framework principles of transparency, choice and consumer control, data governance, sensitive personal data, and accountability.

During these privacy review meetings, the NAI staff also routinely walked through the company's consumer-facing workflows and tools, offering observations and insights about how websites appear from the consumer perspective. This feedback often covered how the sites render for the consumer in different environments (e.g., web and mobile, or variations based on IP address), potential points of confusion or friction for the consumer, and potential inconsistencies that may raise regulator concern. These reviews allowed companies to glean more nuanced insights about the consumer experience and to maximize the effectiveness of privacy tools.

Following each meeting with a member company and its representative(s), the NAI staff drafted a detailed privacy report with feedback tailored for each member company. Feedback primarily consisted of best practice considerations and recommendations for updates to choice mechanisms, consumer-facing portals, privacy disclosures, data governance documentation and practices, and policies regarding the collection and processing of sensitive data, with citations to relevant laws and regulations, enforcement reports, regulator guidance, and NAI tools and resources. In particular, the NAI staff sought to highlight regulatory priorities with members in the Privacy Review reports. To that end, the NAI staff delved into enforcement reports, public filings, best practice documents and guidance regulators publish to promote greater compliance and help companies evaluate how well their practices align with the NAI's understanding of regulator expectations. In addition to the best practice considerations in the member's Privacy Review Program report, some members also had required action items for the members to take to be in adherence with the NAI Principles and accountability requirements.

a. 2025 Privacy Review Cycle — Findings on Transparency

How members communicate privacy practices to consumers.

Under the Framework, each member company must provide transparency into its processing of personal data. In reviewing these practices, the NAI staff inquired about each member's notice that describes the processing of personal data it controls, reviewed the content of the notice and public-facing disclosures, and provided recommendations and considerations regarding applicable best practices for transparency.

The NAI staff found the vast majority of member companies disclosing the processing of the personal data in detail, and providing notices outlining the personal data the member collects, the categories collected, the sources of collection, and the purpose of the processing. While the NAI staff did provide recommendations to some members about how they could improve the clarity of the purposes for processing or sharing or describe the partners to whom the company discloses information in more detail, largely the notices adhered to the NAI Framework. The NAI staff noted required action items in some cases where references to deprecated NAI tools were outdated, and also suggested members provide more comprehensive notices in one place for all consumers (as opposed to, for example, in a state level notice).

i. Timely Updates

The principle of transparency is important under law and under the NAI Principles, and timely updates to consumer-facing disclosures with relevant changes are an important part of adhering to the principle of transparency. Given that the NAI sunset its legacy consumer choice tools in 2025 and replaced them with a GPC browser extension and other resources, the NAI staff focused on reviewing members' websites to ensure members update disclosures so consumers will be able to locate appropriate choice mechanisms. Similarly, the NAI staff reviewed disclosures and flagged links to outdated policies. Staff advised members to refresh those links, add "last updated" dates as part of the disclosures and verify all links function as intended so consumers receive accurate information.

State regulators in Connecticut, Minnesota, and Delaware have made clear that they will treat outdated timestamps as an indicator that a company is not maintaining its notices in alignment with modern practices and requirements, and have cited stale notices in enforcement contexts. The California Consumer Privacy Act (CCPA) requires businesses to update their privacy policies at least every twelve months, which is a cadence that the NAI staff was able to remind several members of as they considered their next planned updates. The risk associated with longer spans without updated notices is compounded for ad-tech companies where innovation can drive more frequent changes in business activities. The NAI staff recommends that members treat the "last updated" date as a compliance consideration in its own right. Even where substantive changes to data practices are minimal, periodic review and refresh of consumer-facing disclosures demonstrates an ongoing attention to transparency that regulators now expect to see.

ii. Declarative Rights

Under the transparency principle, the NAI staff also discussed with members the importance of clarity regarding consumer rights. Members typically had privacy policies that included both notice to consumers about their privacy rights, as well as sections that outline how to exercise those rights. Some members would include conditional phrasing in their privacy notices, such as

"you may have certain data rights under state privacy laws," "depending on where you live," and "residents of certain U.S. states." Notices that took this approach would typically include a list of states that had specific privacy laws, but sometimes would inadvertently omit states with recently enacted comprehensive privacy laws. With twenty states now having operative privacy statutes, and more on the way, failing to timely update disclosures may result in residents of some states not being properly informed of their rights, a common issue which regulators are taking note of. State regulators have actively and specifically rejected the approach where companies include conditional phrasing such as "you may have certain data rights under state privacy laws."[2] During reviews, the NAI staff surfaced a clear and converging enforcement signal from multiple state regulators: conditional phrasing is not just a stylistic weakness—it is being considered by regulators as evidence of legal noncompliance.[3]

Given the regulators' statements, the NAI staff amplified that message during privacy reviews to businesses who could improve on clarity for consumers. The NAI staff consistently pointed members toward two possible compliance paths: either (1) plainly stating that all U.S. consumers may exercise the enumerated rights (where accurate), or (2) providing an explicit, maintained list of covered states that is updated as new laws come into force. The NAI staff observed that many members were moving in the direction of broadly applying rights and already stating that all U.S. consumers may exercise the certain rights (particularly opt outs), and the review process facilitated direct conversations about practical approaches to evolving privacy notices and aligning consumer choice tools and rights request portals. In these conversations, it was apparent that members are carefully balancing the considerations for a single consolidated notice compared with state-specific listings and the burden of maintaining updated state law references and rights portals and tools that track various states' requirements.

iii. Variation of Certain Rights Among the States

While states have largely coalesced around providing consumers certain privacy rights (e.g., the right to request access, deletion, correction), other provisions related to consumer rights have a broader range of divergence among the states. For example, the scope of an authorized agent's

---

[2] *See, e.g.*, Delaware Dep't of Justice Att'y Gen. Kathy Jennings, *Frequently Asked Questions*, https://attorneygeneral.delaware.gov/fraud/personal-data-privacy-portal/frequently-asked-questions/ ("Under the DPDPA, businesses are required to clearly and meaningfully inform Delawareans of their consumer rights and how to exercise them. The DPDPA's consumer rights are similar to many other states who have enacted comprehensive data privacy laws. Thus, many businesses may be able to inform residents of multiple states of these consumer rights in a single section.
While the DPDPA does not require a Delaware specific section, the description of consumer rights must unambiguously indicate those rights are available to Delaware residents. Statements such as "you may have rights" or "if your state has a data privacy law" are not sufficiently clear to inform Delaware residents of their rights and, therefore, do not comply with the DPDPA. Businesses must state the described consumer rights may be exercised by either (i) all users or all United States users or (ii) clearly describe the subset of users, including explicitly identifying Delaware residents, among residents of other states.").

[3] For example, Delaware's Attorney General has issued unambiguous guidance stating that phrases like "you may have rights" or "if your state has a data privacy law" do not satisfy the Delaware Personal Data Privacy Act's requirements. Delaware has taken the position that a notice must either confirm that all U.S. consumers may exercise the listed rights, or it must explicitly identify Delaware residents as consumers who have the listed rights. Oregon's and Connecticut's enforcement reports have similarly characterized portals and notices as deficient where consumers in those states cannot readily determine whether the rights described apply to them.

ability to exercise rights on behalf of consumers, a consumer's right to appeal a controller's response to a rights request, and a controller's obligation to provide information about third-party disclosures of personal information vary between different comprehensive state privacy laws and present additional complexity for companies working to operationalize compliance.

The NAI staff developed member-only resource materials to assist companies in their compliance efforts for authorized agent rights and requests, as well as appeal rights. The NAI staff highlighted regulator guidance on these points, such as Indiana's Data Consumer Bill of Rights document, which emphasized the need to include the entire appeals process in the privacy policy, as well as the need to provide resources for where a consumer can report a complaint to the Office of the Indiana Attorney General.[4]

Deciding how to effectively provide transparency into third-party sharing of personal data is one of the most nuanced notice issues members face, as specific expectations appear to vary meaningfully depending on which state's law applies, and in what context. The NAI staff flagged this divergence in state approaches across numerous member reviews. The core tension in the approaches is that states address this obligation in two structurally different ways: (1) through what must appear in the *privacy policy*, and (2) through what must be provided in response to a *consumer access request*. These two tracks carry different requirements, which can present challenges for companies seeking to apply a consistent approach.

A number of states[5] permit (or require) privacy policies to list *categories* of third parties rather than specific company names. This approach offers meaningful operational flexibility, as a member can disclose categories like "analytics companies," "data brokers," "third-party advertisers," and "payment processors" without naming every individual partner[6] (which can, in some circumstances, implicate trade secrets). Colorado's regulations add important nuance, however: they specify that category-level disclosure must be at a "sufficiently granular level of detail" that gives consumers a meaningful understanding of the type of, business model of, or processing conducted by the third party.[7] Oregon's consumer privacy law similarly requires that privacy notices describe all categories of third parties "at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data[.]"[8]

One of the more operationally difficult parts of the third-party disclosure landscape involves states that require disclosure of *specific third-party names*. Minnesota's Consumer Data Privacy Act gives consumers the right to obtain a list of the specific third parties to which the controller

[4] S.B. 5, 123d Gen. Assemb., Reg. Sess. (Ind. 2023 Indiana's Consumer Data Protection Act).
[5] Colorado, Connecticut, and Texas. California, Delaware, and Maryland apply a similar categories-based approach when responding to consumer access requests.
[6] Colorado (4 CCR 904-3, Rule 6.03(A)(1)(e)(i)) and Oregon (646A.578(4)(e)) describe all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data.
[7] Colorado 4 CCR 904-3, Rule 6.03(A)(1)(e)(i).
[8] Or. Rev. Stat. § 646A.578(4)(e) (providing for a consumer to obtain from a controller, at "the controller's option, a list of specific third parties, other than natural persons, to which the controller has disclosed: (i) The consumer's personal data; or (ii) Any personal data…").

has disclosed their personal data.[9] Oregon takes a similar approach to access requests, requiring disclosure of *specific* third parties when requested by the consumer, as opposed to the more common approach of providing *categories* of third parties in access requests.[10]

Further complicating the landscape, Rhode Island's data privacy law, which came into force on January 1, 2026, requires controllers to disclose the names of specific third parties to whom "personally identifiable information" has been *sold* directly in the privacy policy. This requirement is particularly challenging for ad-tech members because Rhode Island has not defined "personally identifiable information" in the statute, even though it is a distinct term from "personal data," and that creates interpretive uncertainty.[11] Equally notable, unlike the CCPA and other states' express trade-secret protection, Rhode Island does not appear to include a comparably explicit trade-secret carve-out—creating doubt as to whether companies can omit the names of some or all partners on proprietary grounds.[12]

In discussions with member companies, the NAI staff discussed practical approaches to entity-level transparency in this fragmented landscape and how it can pose a significant challenge: members with large, dynamic publisher and exchange partner ecosystems must now consider whether maintaining a continuously updated, publicly posted list of named third-party recipients is operationally feasible, legally required, and competitively defensible. Furthermore, as states revise their statutes, as Connecticut has (with a new right to third party disclosure of specific entities coming into force this summer),[13] businesses must continue to monitor and revise their compliance posture on this important point.

iv. Transparency of Opt Outs and the Global Privacy Control

Transparency of the scope of opt outs and consumer controls was a major priority for privacy reviews. Given regulator focus on companies not only honoring consumer choice but also providing transparency into the scope of the control, the NAI staff spoke with member companies at length about disclosure language concerning choice mechanisms, such as Opt-Out Preference Signal detection, processing and scope. With regulators actively enforcing on this point—and in particular CalPrivacy's enforcement action against Tractor Supply, which penalized the company not only for failing to honor Opt-Out Preference Signals, such as the Global Privacy Control (GPC), but for failing to explain in its privacy policy how those signals would be honored—the NAI

[9] Minnesota § 6, 325O.05, 1(a)-(e), (g), (h) (providing that a "consumer has a right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data," or if the controller does not maintain this information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead.).
[10] Or. Rev. Stat. § 646A.574(B).
https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled.
[11] Rhode Island, R.I. Gen. Laws § 6-48.1-3(a)(2).
[12] *Id.*
[13] *See* An Act Concerning Broadband Internet, Gaming, Social Media, Online Services and Consumer Contracts, Pub. Act No. 25-113 (Conn. 2025) at 34 ("(7) obtain from the controller a list of the third parties to which such controller has sold the consumer's personal data or, if such controller does not maintain a list of the third parties to which such controller has sold the consumer's personal data, a list of all third parties to which such controller has sold personal data, provided the controller shall not be required to reveal any trade secret.").

staff reinforced that regulators not only expect tools to effectively provide for consumer choice, but also that businesses accurately describe these choices to consumers in privacy notices.[14]

With this in mind, the NAI staff analyzed privacy policies for disclosures and prompted members to reflect on their posture as to GPC, the ability to detect GPC, how it was described in the notice, and whether there was a display indicating to the consumer whether and how GPC was processed. The NAI staff and members discussed how to distinguish the GPC scoping from any older "Do Not Track" notices, and informed members about regulations that govern expected scoping of opt outs.[15] For example, the NAI staff closely analyzed disclosures for descriptions of whether the GPC as an opt-out signal would cover the device, the browser, associated consumer profiles, and/or pseudonymous profiles. California's enforcement action against Disney noted that consumers who opted out through GPC "were opted out from Disney's data sharing with ad-tech partners, but only for the specific service and device the consumer was using when they requested to opt-out, even if they were logged in to their Disney account" and underscores both the need to implement the opt-out and also that it is an enforcement priority. The importance of this issue was also highlighted by the fact that Connecticut regulators announced a collaboration with California and Colorado in a joint investigative sweep focused on GPC compliance; an effort that spotlights the scrutiny disclosures face and the trend of state regulators working together to elevate messaging.[16]

The NAI staff also closely examined the opt-out mechanisms members provided directly on members' websites and the language used to describe and scope those mechanisms. Regulators expect opt-out mechanisms to describe the consumer's right to opt out and provide instructions for how consumers may submit a request.[17] With this in mind, the NAI staff encouraged members to provide clear instructions and use statutorily defined terms, such as "targeted advertising," "sale/sharing," and "profiling," when describing the scope of an opt-out mechanism. Similar to evaluations of opt-out preference signal-related disclosures, the NAI staff also closely examined whether members' opt-out mechanisms sufficiently described its application to a consumer's device, browser, associated consumer profiles, and/or pseudonymous profiles.

[14] *See In re Tractor Supply*, No. ENF24-M-TR-04 9/26/2025 Board Decision at ¶ 43, https://cppa.ca.gov/pdf/20250930_tractor_supply_bd_sfo.pdf.
[15] *E.g.*, Cal. Code Regs. tit. 11 § 7025(c)(1) ("The business shall treat the Opt-Out Preference Signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the Opt-Out Preference Signal as a valid request to opt-out of sale/sharing for the consumer.").
[16] *See California Privacy Protection Agency Announces Joint Investigative Privacy Sweep: CA, CO, and CT Investigate Businesses Refusing to Honor Consumers' Right to Opt-Out of the Sale of Their Personal Information*, California Privacy Protection Agency (Sept. 9, 2025), https://cppa.ca.gov/announcements/2025/20250909.html.
[17] *See, e.g.*, Cal. Code Regs. tit. 11 § 7013(f).

b. 2025 Privacy Review Cycle — Findings on Consumer Choice and Control

Where consumer-facing tools meet back-end data reality.

Under the Framework, each member company must offer consumers method(s) to signal a choice about how the company processes their personal data, for those activities which require choice under applicable laws. The NAI staff reviewed each member company's process in place describing how the member provides and honors methods for consumers to signal choice about processing of personal data. The NAI staff also reviewed those activities which require choice under applicable laws and provided recommendations and considerations regarding applicable best practices for consumer choice and control.

i. Reviewing Consumer-Facing Tools

In this initial privacy review cycle under the Framework, the NAI staff focused on consumer choice and usability of consumer-facing tools. The NAI staff aligned its priorities with those identified by state regulators, noting that a top priority across the states was to ensure companies are receiving and responding to consumer requests, with a particular focus on company websites and consumer-facing portals.[18] To accomplish this, the NAI incorporated website testing and utilized inbox submissions to assist members in understanding how their consumer-facing tools are working in practice. The NAI staff amplified warnings from state regulators where they made known that they are sending test emails to companies' privacy inboxes to monitor response times. As part of the review, the NAI staff submitted test requests to opt-out mechanisms and Data Subject Access Request (DSAR) portals, emailed messages to inboxes and monitored for responses, reviewed cookie banners and settings, and evaluated how member company webpages behaved when a GPC signal was present, among other measures.

On the whole, the NAI staff found a strong record of timely and substantive responses from member companies, reflecting the meaningful investments member companies have made in privacy compliance and operations. For example, members typically provide thoughtfully designed choice mechanisms that are clearly presented to consumers and effectuate choice immediately upon submission. In addition, many members have tools designed to surface information requested by consumers in a timely response, and with thoughtful and proportionate verification measures. Nevertheless, the reviews surfaced a range of technical and usability issues and identified opportunities for members to improve their practices. Among the most common technical issues observed were outdated or broken links within privacy disclosures and opt-out sections, missing confirmation emails that left NAI testers without any indication that their requests were received, "endless scroll" barriers that could obscure access to choice mechanisms, and broken CAPTCHAs. The NAI staff also observed instances where privacy preference center pages failed to load properly when common browser privacy tools or extensions were enabled, raising the concern that the very consumers most actively seeking to exercise their rights may find it more challenging to do so.

[18] *See, e.g.*, Connecticut's 2026 Enforcement Report (highlights the Attorney General's focus on ensuring businesses honor Opt-Out Preference Signals, noting that it previously announced an investigative sweep with California and Colorado flagging potential noncompliance with Opt-Out Preference Signal-related provisions).

The NAI staff also reviewed cookie banners closely, and accompanying disclosures. The majority of companies had cookie banners and prominent, accessible statements about the use of cookies. Some companies also provided more granular disclosures concerning different categories of cookies, such as those that are "necessary," as compared to others that might relate to marketing and advertising. The NAI staff urged some member companies to review their cookie policy disclosures and the categorizations reflected in their cookie preference tools to ensure accuracy and consistency. In several instances, the NAI staff observed potential discrepancies between how cookies were described in policies and how they were categorized within cookie tools, which could create confusion for consumers. At times, it appeared that the names of cookies or classifications of certain cookies as "necessary" could be revised to better align with consumer expectations. For example, some cookies categorized as "necessary" appeared to support analytics or advertising related functions, rather than being strictly required for the site to operate.

In addition, the NAI suggested some member companies using third-party vendors to provide cookie management tools consider whether the names and public-facing descriptions of the cookies are sufficiently clear and accurate and do not mislead consumers. In some cases, vendor-provided cookie names or descriptions are highly technical or abbreviated, making it difficult for consumers to meaningfully understand the function of the cookie without additional context. Companies should consider whether these descriptions can be clarified to improve transparency. In addition, the NAI suggested that if partners with cookies were previously listed in a privacy policy, it may make sense to revise that approach and refer the consumer to the cookie tool for such information, rather than trying to keep a dynamic list updated in a policy. The NAI staff noted that given the evolving nature of vendor relationships and tracking technologies, ensuring that disclosures are consistent across the policy and consent tool and reflect current practices will reduce the likelihood of consumer confusion.

ii. Symmetry in Choice & Design

In 2025, the NAI staff observed continued heightened regulatory scrutiny over user experience (UX) best practices, particularly the need to design user-friendly cookie banners and preference centers and consumer controls that avoid dark patterns. While this has been an ongoing priority, CalPrivacy's enforcement action against Honda provided helpful guidance for offering symmetry in choice, noting that the path for a consumer to exercise a more privacy-protective option cannot be longer, more difficult, or more time-consuming than the path to exercise a less privacy-protective option, effectively stating that opt-out workflows cannot be harder than opt-in workflows. This led to the NAI staff having conversations with several members to clarify that regulators may expect that cookie tools that feature a clear "Accept All" button, for example, should also then present a clear "Reject All" button. In practice, many NAI member companies had thoughtfully designed pathways to enable consumers to utilize mechanisms. The NAI staff raised with some members the importance of clearly labeling all opt-out mechanisms, including any toggles, with an understanding that interfaces should not assume user knowledge about what is the default or that a given toggle would effectuate an *opt-out* of sale and sharing and not an *opt-in*.

The NAI staff also identified and flagged a range of design issues that are at risk of falling short of emerging best practices. Several members' opt-out and DSAR flows included points of unnecessary friction for consumers, such as requiring consumers to provide more personal information than necessary to implement an opt-out request. Furthermore, the NAI staff

discussed what regulators have classified as verifiable rights compared to non-verifiable "Opt-Out of Sale/Share" requests from consumers. As CalPrivacy's Honda decision drew a sharp line between *verifiable* consumer requests (such as requests to know, correct, and delete) and *non-verifiable* consumer requests (such as requests to opt-out of sale/sharing and requests to limit the use of sensitive personal information), there are emerging best practices on ensuring the use of identity verification (such as an email confirmation, a signed affidavit, or providing a government ID) is limited only to those requests that allow for it, such as requests to delete, requests to correct, and requests to know.[19] The NAI staff also noted that CalPrivacy's enforcement action against Ford also found that requiring consumers to confirm their email address before processing an opt-out request effectively imposed a verification requirement that created unnecessary friction and prevented the company from processing some opt-out requests unless consumers completed that additional step. Where member companies may have appeared to require personal information to implement an opt out, staff discussed what information may be strictly necessary to process the opt-out and where eliminating verification measures from opt-out workflows would be a more favorable posture. The NAI staff also reflected to members that they should ensure the information provided is clear and readily accessible to consumers; and website or tool designs cannot require a user to scroll down through a lengthy privacy policy, or click "read more" to locate relevant information for a choice or links for submitting a request.[20]

Though California Attorney General's matter against Disney was announced further into the Privacy Review Program review cycle, it serves to highlight how confusing partially effectuated opt-outs can be for consumers, and how partial opt-outs could be viewed as deceptive practices by regulators.[21] When managing opt-outs across different services and devices, or through various opt-out mechanisms, members were reminded to be clear on the effective scope of the tool and encouraged to rigorously evaluate their methods and confidence for implementing choice and communicate any limitations clearly to consumers (such as articulating any limit to how an opt out can be implemented or how long an opt out can persist) to avoid subverting consumer choice.

iii. Data Rights Requests & The Back-End Data Reality

Data subject access and deletion requests are increasingly interpreted by state regulators as broad requests that extend beyond simply providing a user with their visible account information. Insights from the Oregon Department of Justice's One-Year OCPA Enforcement Report[22] explicitly address this issue, warning companies that relying solely on "self-help" or

[19] *See* Cal. Code Regs. tit. 11 § 7060.

[20] *E.g.*, *see* Cal. Code Regs. tit. 11 § 7004(a)(5)(A) ("Upon clicking the "Do Not Sell or Share My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.").

[21] In the Disney enforcement action, California Attorney General scrutinized Disney's use of opt-outs, as they "only partially effectuated opt-out requests" by only opting the consumer out of Disney's data sharing with ad-tech partners on that specific device without effectuating the opt out request "across all of Disney's systems, brands and devices." The complaint makes clear that "[w]hen a business creates a form, toggle, or other tool, and chooses to label it as an opt-out, even though it does not fully opt-out the consumers who use it, the business is engaged in deception."

[22] Or. Dep't of Justice, *Enforcement Report: The Oregon Consumer Privacy Act, The First Year (Aug. 2025)*, https://www.doj.state.or.us/wp-content/uploads/2025/08/OCPA-One-Year-Enforcement-Report-2025.pdf.

account-centric tools to satisfy consumer rights requests may not comprehensively cover the scope of the rights. The report emphasizes that when consumers request a copy of their data or ask for its deletion, controllers have a strict obligation to provide all data, which includes derived and "back-end" data. For many companies, providing back-end data, which may encompass modeled marketing profiles, audience segments, and inferred shopping patterns, can be time- and resource-intensive, as they may need to pull down and format each consumer request. Moreover, certain companies that may have particularly sensitive data have to continually evaluate the sensitivity of the data against the verification measures they are able to use to validate whether an access request should be granted.[23]

During discussion of the challenges accompanying access and deletion requests, several members articulated that satisfying a single access request can be further complicated by the reality of data silos across the digital advertising ecosystem. Because a consumer's information rarely lives in a single, centralized database, businesses often face the significant operational challenge of querying highly distributed data environments to retrieve or delete the necessary records. This task could include tracking down personal data that may have been securely hashed and pushed into data clean rooms, shared with offline onboarding partners, or fragmented across various internal analytics and measurement platforms. As the NAI staff reminded member companies, the Oregon enforcement report makes clear that a business cannot satisfy its legal obligations by leaving out data from distributed environments; instead, it must ensure its DSAR fulfillment processes are robust and provide both raw and derived data from across services, even if needing to draw on disparate silos of data.

iv. Deletion Requests

Beyond the initial retrieval of data, businesses must also grapple with the complexities of cascading both access and deletion requests to ensure a consumer's request is comprehensively effectuated. When a consumer submits a deletion request, the controller must ensure that this is effectively passed downstream to processors, vendors, and partners who have received the data. Methods for notifying others about deletion requests vary widely, from manual email updates with file attachments, to shared files in the cloud, to fully automated technical integrations.

Those member companies that registered as data brokers in California, in particular, experienced a large spike in deletion requests relative to their size. Some smaller companies that previously received very few or no requests before registration then saw a growth in requests from dozens to hundreds or so of requests per month once registered. Other companies experienced a more severe spike in deletion requests, with several companies attributing the large increase in requests to authorized agents. These companies otherwise noted seeing a moderate increase in individual consumer requests. Where there is an uptick in authorized agent requests, many members continue to struggle with an "actionability gap" as they are provided data from incoming deletion requests that does not allow the member to match the request with data the member company has (e.g., a MAID is not provided), or the necessary verification step is not completed by the consumer (or their agent).

Member companies must also currently navigate state privacy laws that are split on the scope of the deletion right. Where a minority of states (California, Iowa, and Utah) limit deletion rights only to data the *consumer provided directly*, the vast majority of state privacy laws now give

[23] For example, processing certain forms of sensitive data warrants a more stringent verification process. *See* Cal. Code Regs. tit. 11 § 7060(c)(3).

consumers a broader right to delete *all personal data a controller has concerning them*, which would include data obtained from third parties.[24] The NAI consistently highlighted the importance of maintaining comprehensive and thoughtful data maps across all internal systems to best understand where personal data about any given consumer is coming from.

The NAI staff also spoke with some member companies about the importance of ensuring that personal data is purged and putting in place measures to ensure that the data *remains* deleted over time. This represents another obligation that requires strict additional controls and sophisticated data governance. In response, some member companies noted they anticipate some friction when implementing consumer deletion requests, as data may reemerge through data sources and repopulate a deleted profile, such as may occur when a consumer changes their phone number or gets a new email address.

v. GPC Implementation of Opt Outs

Beyond analyzing user interfaces, the NAI staff replicated the testing methodology employed by some regulators on business websites, such as A/B testing a webpage with GPC enabled and GPC disabled to observe which third-party tracking tags fire and which cookies are dropped in each state. In some cases, it was unclear whether a member's website limited tracking when a GPC signal was active, and in some instances staff did not observe one or more valid GPC specifications being detected by certain tools used in testing. During reviews, there was also some discussion about how there are technical limitations where GPC signals received through websites may not be broadly implemented across the member's services due to an inability to match the browser signal to other services. The NAI staff emphasized the importance of closely evaluating the technical reach of an opt out, especially for those members who maintain device graphs, as regulators in California made clear through enforcement that a business limiting the opt-out request received via GPC to the specific device the consumer was using, even when the consumer was logged into their account across several other devices, would be treated as a deceptive practice.[25] However, rightsizing the scope for an opt out may be challenging for businesses, particularly where device graphs are probabilistic and not deterministic. Among probabilistic device graphs there may be a risk of either over-matching and opting out the wrong person or device, or under-matching and failing to fully opt out the right person or device. Moreover, as confidence in a device's association with other devices or browsers or individuals may evolve over time (as is the nature of probabilistic device graphs), so too may the ability to track and honor the opt out.

In addition, the scope of the opt-out preference signal and whether it would be respected for consumers in states without specific legal requirements to honor such a signal was also a

[24] *Compare* Cal. Civ. Code § 1798.105(a) (scoping the Right to Delete to personal information "which the business has collected *from the consumer*") *with* Conn. Gen. Stat. § 42-518(a)(3) (scoping the Right to Delete to personal information "*provided by, or obtained about, the consumer*"), illustrating the trend to increase the scope of a deletion request to all personal data collected about a consumer. See also, the bill the California legislature is considering that will expand the deletion right to all personal information the business has collected "*from or about* the consumer." *See* CA SB 923, https://legiscan.com/CA/text/SB923/id/3340074.

[25] Compl. *California v. Disney*, Case No. 26STCV04425 at ¶ 15, (Feb. 11, 2026), ("When a business creates a form, toggle, or other tool, and chooses to label it as an opt-out, even though it does not fully opt-out the consumers who use it, the business is engaged in deception. The same is true when a business tells consumers that it honors the Global Privacy Control or other opt out preference signals, when it actually doesn't.").

question for some members. Providing consumers with adequate information to understand what a signal would actually accomplish is important to ensure consumer expectations are met and not frustrated. The NAI staff also flagged for members a new and visible CCPA regulatory requirement that took effect January 1, 2026: businesses are now required to display on their website whether a consumer's opt-out preference signal has been processed as a valid request to opt out of sale or sharing.[26]

Because regulators increasingly treat a company's public-facing website and privacy notice as visible indicators of its potential overall compliance posture, the NAI staff highlighted that regulators would expect websites to detect and process GPC signals regardless of whether a company primarily operates in a business-to-business (B2B) context. Even if a B2B company processes very limited personal information through its website and has a website only for business clients, regulatory bodies are actively testing these sites to see if businesses are correctly detecting and processing GPC signals. The NAI staff reinforced that the absence of GPC-related disclosures or functioning opt-out capabilities on a publicly accessible B2B website could draw regulators' attention and broader scrutiny of privacy practices.

c. 2025 Privacy Review Cycle — Findings on Sensitive Personal Data

The hardest classification problem in privacy.

Under the Framework, each member company must limit its processing of sensitive personal data to disclosed purposes (and purposes consented to by the consumer as required by applicable laws) and provide additional safeguards when processing such data. During reviews, the NAI staff asked questions about the internal policies members have in place for assessing when personal information may be sensitive. This included closely examining the various types of health-adjacent data members may collect and process, as well as any information that is derived or inferred from nonhealth information. If it is determined that a member does process sensitive personal data, the NAI staff would review relevant safeguards, disclosures, as well as how and when the member obtains the relevant consent or ensures such consent is obtained on its behalf.

i. The Challenge of Classifying "Sensitive Data"

Members have overwhelmingly developed internal policies for classifying sensitive personal data. However, given the evolving and somewhat varied frameworks for determining when personal information meets a higher threshold of sensitivity that requires heightened protections, the NAI staff observed a lack of uniformity for classifying sensitive data amongst members. Concerning health data specifically, the NAI staff observed a wide variety of approaches taken at the state level to define health-related sensitive personal data, and the challenges these different approaches present to members. For example, some states define health-related sensitive personal data narrowly, limiting the classification only to data *revealing* a mental or physical health diagnosis, whereas other states take a broader approach that envelops all data identifying a consumer's past, present, or future physical or mental health status.[27]

---

[26] As of January 1, 2026, CCPA Regulation § 7025(c)(6) requires a display for whether an Opt-Out Preference Signal has been processed as a valid opt-out of sale/share.

[27] *Compare* Tex. Bus. & Com. Code § 541.001(29) (Texas definition of "Sensitive Data") *with* My Health My Data Act, RCW 19.373.010(8)(b)(xiii) (Washington definition of "Consumer Health Data").

Beyond statutory definitions, the NAI staff also paid close attention to enforcement actions that provide additional context on when personal data should be classified as sensitive and often during Privacy Reviews raised matters for members' consideration. For example, in the settlement between the California Attorney General and HealthLine Media, there was strong emphasis placed on the CCPA's provisions that limit the use of personal information for only those purposes that are consistent with the *reasonable expectations of the consumer*.[28] Known as the "purpose limitation principle," its application in the Healthline matter suggests that there may be varying degrees of data sensitivity, and that the sharing of personal data "of a more intimate nature" with third parties may be unlawful when consumers would not expect that to happen.

In the face of this complexity, there are a range of compliance approaches that the NAI staff observed during Privacy Reviews: (1) members attempting to force simplicity by over-classifying any information related to health as sensitive and therefore subjecting the data processing to heightened requirements; (2) members under-classifying what constitutes sensitive personal data, or failing to recognize in certain cases where a broader category of data could meet various legal definitions, creating a compliance gap; or (3) members choosing to withdraw altogether from jurisdictions where they perceive risk that almost any data processing could trigger broad definitions of what is sensitive.

To support consistent, well-reasoned sensitivity classifications for health data, the NAI staff developed a *Factor Analysis for Health-Related Sensitive Personal Information* as a tool to assist members with the growing challenge of classifying health-related sensitive data.[29] The tool acknowledges that health data sensitivity often emerges from a confluence of factors: how data is collected, what it contains; how it is used; and what risks it creates. For those members struggling with the complexity of reasoning through sensitivity classifications, the NAI recommended the adoption of this tool, and encouraged members to pay close attention to the concerns of regulators regarding the types of data that should be classified as sensitive under state and federal law.

ii. Disclosure, Consent, and the "Limit the Use" Choice Mechanism

Those members that process sensitive personal data for Network Advertising, must adhere to a stricter—and in some ways more fragmented—regulatory framework. However, despite the disjointed approach to regulating sensitive personal data at the state level, there is a universal understanding that the processing of sensitive personal data carries a heightened risk of harm to consumers that warrants increased transparency and choice. For example, some states have explicit requirements to disclose the categories of sensitive personal data collected and the specific purposes for the processing.[30] As part of the privacy review, the NAI staff evaluated

[28] *See California v. HealthLine Media*, Case No. CGC-25-626794, July 1, 2025 Complaint at ¶ 22; Cal. Code Regs. tit. 11 § 7060(c)(3).

[29] *See* Network Advertising Initiative, *Factor Analysis for Health-Related Sensitive Personal Information*, (Feb. 24, 2026), https://thenai.org/wp-content/uploads/2026/02/NAI_Factor-Analysis-for-Sensitive-Health-Information_02242026.pdf.

[30] *See, e.g.*, Cal. Civ. Code § 1798.100(a)(2) (requiring businesses to disclose at or before the point of collection the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared); *see also* Tex. Bus. & Com. Code § 541.102 (requiring controllers engaged in the sale of sensitive data to include a notice that says "NOTICE: We may sell your sensitive personal data.").

privacy notices and other disclosures to understand how members currently approach these heightened disclosure requirements. Overall, members that are knowingly processing sensitive personal data have sufficiently disclosed the categories of sensitive personal data they collect and the purposes for the processing.[31]

As the vast majority of state comprehensive privacy laws require opt-in consent to process sensitive personal data,[32] members that are knowingly processing sensitive personal data have taken varying approaches for either obtaining consent, or verifying that proper consent has been obtained when the data was initially collected. Indeed, consent obligations are generally tied to the *processing* of sensitive personal data, not merely its *collection*.[33] This means that a controller receiving sensitive personal data from a partner to use for advertising likely needs valid consent for its own processing and cannot simply rely on the fact that the partner obtained consent for its separate use of the data. As such, consent language needs to be transparent and encompass all intended uses of the data—including downstream uses for advertising.

For these reasons, the NAI encouraged members that are processing sensitive personal data to go beyond contractual provisions concerning consent to conduct due diligence and review the consent language presented to consumers. For members that partner with a small number of publishers, this task is relatively easy and manageable, and can be done by reviewing each individual publisher or asking each publisher to provide screenshots of the relevant consent prompt. However, the NAI encouraged members that partner with a large number of publishers providing sensitive data to conduct necessary due diligence, recognizing it may be approached in a more scalable manner.

California is unique in that its comprehensive privacy law requires providing a conspicuous link titled "Limit the Use of My Sensitive Personal Information" when a business is processing sensitive personal data for purposes outside of what is strictly necessary.[34] Known as a *Limit the Use* mechanism, it must be offered alongside California's other distinct "Do Not Sell or Share My Personal Information" mechanism. With few exceptions, NAI members are well attuned to these requirements, and often bundle these mechanisms under a single "Your Privacy Choices" alternative opt-out link.[35]

iii. Precise Geolocation Data

During the 2025 Privacy Review cycle, the NAI staff again emphasized to member companies that precise geolocation data remains one of the most sensitive and heavily scrutinized categories of data in the digital advertising ecosystem. Recent state laws in Maryland and Oregon introduced strict limitations on the sale of precise geolocation data, representing a meaningful

[31] The NAI staff also observed that members were more likely to overstate the categories of sensitive personal data they process, as opposed to understating.
[32] *See, e.g.*, Conn. Gen. Stat. § 42-520(a)(4); Tex. Bus. & Com. Code § 541.101(b)(4); *but see* Cal. Civ. Code § 1798.100(a)(2) (relying on notice and the reasonable expectations of the consumer in lieu of consent); Utah Code § 13-61-302(3) (relying on notice and choice mechanisms in lieu of consent); Iowa Code § 715D.4(2) (relying on notice and choice mechanisms in lieu of consent).
[33] *See, e.g.*, Conn. Gen. Stat. § 42-520(a)(4) ("A controller shall… not **process** sensitive data concerning a consumer without obtaining the consumer's consent[.]") (emphasis added).
[34] *See* Cal. Civ. Code § 1798.121.
[35] *See* Cal. Code Regs. tit. 11 § 7015 (providing the option for an alternative opt-out link allowing for the bundling of the *right to opt-out of sale/sharing* and *right to limit* mechanisms).

shift from prior state law frameworks that primarily relied on notice and choice. Rather than conditioning processing on consumer consent alone, these laws impose categorical restrictions that directly constrain how location data may be used and monetized.

These restrictions have had significant and, in some cases, immediate operational implications for companies engaged in location-based advertising. In practice, some companies scaled back or discontinued certain location-based activities, while others reassessed whether to operate in particular state markets at all. These responses reflect the extent to which the new legal requirements are reshaping core business practices, rather than simply requiring incremental compliance adjustments.

In response to these two state laws, NAI members and their partners have made significant adjustments to their standard business models. Some companies have chosen to withdraw certain location-based services from these jurisdictions altogether, rather than attempt to redesign those offerings within the new constraints. As a result, certain products and use cases that depend on precise geolocation (such as in-store visitation measurement or attribution of advertising to real-world outcomes) may no longer be available in those states. Other companies have continued operating in these jurisdictions, but with more limited functionality. In practice, this has generally involved restricting or eliminating the use of precise geolocation data in those contexts and limiting services to those that can be supported without relying on that data. While these approaches allow for continued operation, they can materially reduce the effectiveness and precision of advertising and analytics capabilities, highlighting the tradeoffs companies are making to navigate evolving legal requirements.

1. Compliance through Technical Measures

As there has been greater scrutiny of the use of precise geolocation information, many companies are exploring and adopting technical measures to reduce the sensitivity of location data while preserving utility. One method observed in the reviews is the truncation of IP-derived location data, such as limiting precision to two decimal places. While these approaches may reduce granularity, they also raise important questions about whether such transformations meaningfully mitigate sensitivity under emerging legal standards, particularly where re-identification risks may remain, or where the data can still be used (alone or in combination with other data) to approximate a user's precise location or visits to sensitive points of interest. Regulators are increasingly focused not just on how data is labeled, but on whether it can still reveal precise or sensitive insights about individuals in practice.[36]

In speaking with members that process precise geolocation data, the need for robust filtering of sensitive points of interest remained a key compliance challenge for some. Across reviews, companies demonstrated varying levels of maturity in identifying and excluding locations that may reveal sensitive characteristics, such as healthcare facilities, places of worship, or other locations tied to intimate aspects of individuals' lives. This issue has taken on heightened importance in light of recent legal developments, including state laws that specifically call out health-related location data as requiring enhanced protections. Notably, New York's geofencing

[36] The FTC's April 2024 action against InMarket Media reflects this kind of functional scrutiny. The FTC defined regulated "Location Data" to exclude coarse location only where the underlying precise signal was "used solely for the purpose of generating such coarse location and then deleted within 48 hours of collection," meaning data is not treated as exempt simply because the output looks imprecise, but based on whether precise data was retained or capable of use at any point in the process.

law prohibits the establishment of a geofence of 1,850 feet or less around a healthcare facility for the purpose of delivering digital advertisements, building consumer profiles, or inferring an individual's health status or treatment. Since the development of the NAI's Voluntary Enhanced Standards for Location Information Solution Providers in 2022, the NAI has been encouraging members to identify sensitive locations and take steps not to process or share precise geolocation data related to these locations. In the NAI privacy reviews with members, the NAI staff highlighted the consistent focus of regulators on data related to sensitive locations and promoted the NAI's Voluntary Enhanced Standards.

New state regulations and increased scrutiny of the use of geolocation information, particularly data that can approximate visits to sensitive points of interest such as health facilities, places of worship, reinforce that compliance in this space must be an ongoing function requiring continuous refinement and validation.

2. Meaningful & Informed Consent

Regulators and enforcement actions continue to emphasize that the collection and use of precise geolocation data must be grounded in meaningful, informed consent. This expectation extends beyond the initial point of collection to the broader data supply chain, meaning that companies that receive or rely on location data are increasingly expected to conduct due diligence and implement contractual safeguards to ensure that upstream partners, such as app publishers and SDK providers, are obtaining valid consent.[37] As a result, accountability for consent is no longer limited to the first-party interface; instead, it is distributed across all participants in the ecosystem.

Recent enforcement actions further illustrate this regulatory focus. State and federal regulators have demonstrated a willingness to bring cases where location data practices are perceived to reveal sensitive information or where consumer expectations are not met.[38] Regulators are increasingly evaluating these practices holistically, examining not only technical compliance, but also considering the sensitivity of the data and whether the overall use of the data aligns with consumer disclosures and expectations.

[37] The FTC's January 2025 action against Gravy Analytics and Venntel illustrates this expectation. The order required Gravy to implement a formal "Supplier Assessment Program," including annual assessments of upstream data suppliers designed to "confirm that consumers provide Affirmative Express Consent" for the collection and use of their location data, and to "cease from using, selling, licensing, transferring, or otherwise sharing or disclosing" location data from any supplier that could not demonstrate valid consent. The order further required Gravy to impose contractual obligations on recipients of its location data requiring those recipients to pass equivalent prohibitions to any third parties to whom they resell or transfer the data.

[38] The FTC's 2022 complaint against Kochava alleged that the data broker sold precise geolocation data linked to mobile advertising IDs in a format that allowed customers to track consumers to sensitive locations without any technical controls to prevent such use (and the parties recently reached an undisclosed settlement). The Commission's actions against Gravy Analytics and Mobilewalla (finalized in early 2025) addressed similar concerns that data brokers sold precise, non-anonymized location data without verifying that consumers had meaningfully consented to its collection or sale. In his statement in those matters, then-Commissioner Ferguson articulated the consent-centered standard that has emerged from these cases: "The sale of non-anonymized, precise location data without first obtaining the meaningfully informed consent of the consumer is therefore an unfair act or practice in violation of Section 5." These actions highlight concerns around the collection of granular location signals, the sharing of such data with third parties, and the adequacy of disclosures and consent mechanisms.

iv. Precise Location Information Solution Provider Voluntary Enhanced Standards

The NAI's Precise Location Information Solution Provider Voluntary Enhanced Standards ("VES") represent the NAI's accountability mechanism for the subset of member companies (known as "signatories") that collect precise location data and use it to provide location-based audience segments or analytical services. Signatories voluntarily sign on to the VES, which prohibit the use, sale, and transfer of U.S. consumer precise location information related to Sensitive Points of Interest (SPOIs), and separately prohibit the use, sale, or sharing of any U.S. consumer precise location information for law enforcement or national security purposes, except where needed to comply with a valid legal requirement. In 2024, the NAI updated the VES to clarify how nationally recognized industry classification systems, such as the North American Industry Classification System (NAICS), can be used to identify sensitive locations and operationalize a process that aligns with the standards, a practical update aimed at improving consistency and administrability across signatories.

The annual accountability reviews of VES signatories surfaced important lessons about how companies are implementing the standards in practice and where the most persistent operational challenges lie. One of the most significant findings concerns the methods signatories use to comprehensively identify SPOIs. Across signatories, the NAI staff observed a range of approaches, including licensing third-party point-of-interest databases, conducting manual location audits, and applying keyword-based search methodologies to classify location data. No single approach has emerged as definitive. Signatories expressed a shared desire for more resources on this front to strengthen the collective reliability of sensitive location filtering. At the same time, they are acutely aware of the inherent limitations of any SPOI dataset, as it represents a best effort at a moment in time; its coverage is constrained by the availability of sources to quality-check against and its durability over time cannot be fully guaranteed. The NAI staff is actively considering what additional resources and coordination mechanisms could support signatories in this work.

Temporary sensitive locations were consistently a challenge identified in VES privacy reviews, given the nature of these geographic locations that are sensitive only during specific events or timeframes, such as a convention center hosting a health-related conference or a park used for a religious gathering. Identifying these dynamically sensitive locations is significantly more resource-intensive than maintaining a static SPOI directory, and current methodologies are limited in the ability to capture this category. The NAI is continually evaluating what practices or tools could help address these challenges, and encourage members to include contractual limitations and the innovation of techniques to more comprehensively capture SPOIs.

Two additional findings from the VES reviews merit recognition. First, the NAI staff observed that several signatories have developed SPOI categories that go beyond what the VES expressly requires to classify additional location types as sensitive. Examples include the classification of parts of Native American reservations and firearms-related locations—such as gun stores and shooting ranges—as SPOIs. This kind of voluntary expansion of protections reflects a mature privacy culture and a proactive posture toward consumer protection that aligns with the spirit of the NAI Framework. Second, in discussions about business practices, signatories reported that they routinely decline business opportunities they assess as carrying unacceptable privacy risk, which the NAI sees as an indication that the values embedded in the VES are integrated into commercial decision-making, and rather than treated as a separate compliance exercise.

Finally, the NAI staff asked signatories about the volume of law enforcement requests they have received for consumer location data—a topic that has drawn significant public and regulatory scrutiny. The responses indicated that the volume of such requests has not been overwhelming. Importantly, signatories reported that they evaluate each such request carefully, asking whether it is properly propounded and narrowly tailored before any response is provided. These processes reflect the kind of principled gatekeeping that the VES were designed to encourage, and they offer a model for how industry can maintain meaningful accountability over government access to sensitive data.

v. Children's Privacy

During Privacy Reviews, the NAI staff discussed the topic of children's data with member companies, focusing on strong compliance and increased activity by both regulators and legislators. The NAI staff provided member companies with updates on developments in the space among enforcement agencies, and often provided links to resources about new and unfolding efforts among industry, as well as state and federal regulators, to ensure members are forward-thinking in compliance efforts related to children's data.[39] The enforcement of these laws is somewhat in flux, as there have been several constitutional challenges that are being actively litigated.[40]

Amidst the evolving landscape of privacy laws in force, the NAI staff highlighted the importance of members continuing to evaluate their entire data ecosystem, particularly regarding app-level data sources. Specifically, members should consider whether and how contracts with partners and data source vendors address app-level data sources. It is essential for members to continue assessing the presence of children and app-sourced data within their ecosystems. Members whose business model does not include processing children's data should confirm that other parties are both doing their due diligence with regard to any appropriate age verification APIs and then follow through and do not share children's information with members.[41]

---

[39] For example, certain states passed laws aimed to require app stores to include age verification and transmit related signals include Utah's App Store Accountability Act (SB 142) (enacted March 26, 2025 and now amended as HB 498), Texas' App Store Accountability Act (SB 2420) (enacted May 27, 2025, enjoined in December 2025), Louisiana's Act 481 (enacted June 30, 2025), and most recently, Alabama's App Store Accountability Act (HB 161) (enacted February 17, 2026). Apple announced a Declared Age Range API, allowing apps to ping an API to obtain information that a parent or guardian can input for their child's declared age range, and similarly, Google has a Play Age Signals API in beta.

[40] In December 2025, a federal court in Texas enjoined the Texas App Accountability Act from enforcement, which was due to begin in January 2026. In Utah, in February 2026, a First Amendment challenge to Utah's law was filed with the goal of enjoining the law. Utah then amended the app store accountability law to narrow obligations and included a private right of action, in an effort to combat current and future First Amendment challenges.

[41] A company can acquire "actual knowledge" of children's data through various means. For instance, the platform from an API could inform the company the age range of the child, or they could have "actual knowledge" from other information available to them. Such as the case where OpenX had actual knowledge from human review of apps that were child-directed. There, OpenX's policies and procedures included a traffic quality team that conducted a human review of each Web site or App that sent ad requests, to ensure compliance with OpenX's supply policies and to accurately classify the subject matter of all Web sites and Apps for the benefit of its demand-side partners. Hundreds of child-directed Apps that OpenX reviewed were not flagged as child-directed and have participated in the OpenX Ad Exchange. The FTC alleged that OpenX had actual knowledge that these Apps were child-directed based on its human review

During Privacy Review meetings, the NAI staff also encouraged members to consider reviewing and updating their privacy policies to clarify the company's approach to minors' data in light of the evolving state privacy laws. There is a growing trend among states placing restrictions on the collection and processing of personal data of consumers under the age of 18—rather than 16, the threshold used in earlier laws. This can be seen with the Maryland Online Data Privacy Act (MODPA), which went into effect on October 1, 2025, and prohibits controllers from processing the personal data of a consumer for targeted advertising or selling the personal data of a consumer if the controller knew or should have known that the consumer is under the age of 18. Additionally, Colorado's Children's Privacy Amendment, which also went into effect on October 1, 2025, prohibits controllers from knowingly processing the personal data of minors (under age 18) for the purposes of targeted advertising, sale, and profiling without consent. The NAI staff encouraged members to consider reviewing their privacy disclosures and consider raising the age threshold to 18, if they have not done so already.

d. 2025 Privacy Review Cycle — Findings on Data Governance

Building durable accountability.

Under the NAI's Framework, each member company must take steps to ensure that its processing of personal data comports with its commitments and legal obligations. The NAI staff reviewed member companies for whether each had implemented a written data governance program that addresses personal data processing across its organization. In particular, the NAI staff inquired about whether there was written data governance about how the member honors consumer opt-out requests it receives; processes the member has in place to respond to consumer requests in a timely fashion; steps the member takes to update disclosures to reflect new data processing; and steps the member takes as part of its partner and vendor due diligence. The NAI staff provided recommendations and considerations regarding applicable best practices for data governance.

i. Data Governance Programs

In our reviews, many members had satisfactory written data governance documentation in place. As this principle did not have a predecessor element in the NAI's previous codes, it was adopted as a signal to members about the importance of developing and documenting responsible data stewardship. It is understood that state law often requires policies, and regulators frequently ask to see more written evidence for how practices are memorialized, how expectations are communicated to employees, and how companies demonstrate consistency in following the processes. Data governance is also growing in importance as it helps members ensure that data is well managed (with proper consents and known provenance, for example) to then be prepared for potential uses of data for AI and govern the risk and compliance for those areas. The NAI staff highlighted the need to have written records of how companies would recognize and respond to consumer opt-outs and exercising of rights, and required members to take steps to develop such written data governance where needed, to be in adherence with the Framework's Principle on Data Governance.

---

of the Apps. Therefore, the distinction between "intentional" and "knowingly" is critical for companies to comply with.

The emphasis on written data governance reflects a broader regulatory environment in which federal and state privacy regulators are increasingly expecting companies to evidence their processes through documented policies and procedures—not just verbal assurances or ad hoc practices that are documented only when requested. For example, CCPA regulations require businesses that receive, sell, or share the personal information of 10 million or more consumers annually to establish, document, and comply with a training policy for staff handling consumer requests.[42] The DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data (DOJ Bulk Data Rule) similarly requires covered entities to maintain a written Data Compliance Program, including annual certification of written policies and procedures. Regulators are increasingly focused not only on whether data governance processes are written down, but also on whether those policies are communicated to staff through regular training and manuals, and employee training on adherence to data governance programs should not be glossed over by businesses. This focus on employee training underscores that written documentation is becoming a baseline expectation for demonstrating accountability to both self-regulatory bodies and government enforcers.

To support members in meeting these expectations, the NAI produced a new Data Governance Checklist and Template, designed to assist members in formalizing and memorializing their processes in line with both the NAI Principles and federal and state regulators' expectations. The tool walks members through key considerations for developing an effective written data governance program and provides a template policy as a starting point. It also highlighted certain laws that impose specific obligations around sensitive data, including the Protecting Americans' Data from Foreign Adversaries Act (PADFAA), the DOJ Rule, and state-specific geolocation and health data laws, such as Oregon's geolocation restrictions, Maryland's consumer health data provisions, New York's geofencing law applicable to healthcare facilities, and Washington's My Health My Data Act. By providing this resource, the NAI aims to help members both meet evolving privacy standards and build the kind of documented compliance infrastructure that positions them well as regulatory scrutiny continues to intensify.

ii. Cross-Border Data Protection

The federal government's increased efforts to limit national-security risks posed by the sale of Americans' sensitive data to foreign adversaries have created new obligations for member companies that rely on the collection and use of data for advertising. The DOJ Bulk Data Rule and PADFAA incorporate new diligence measures and require additional assessments of partners and their data practices.

In reviewing member responses to the 2025 Privacy Review Questionnaire, the NAI observed a wide range of steps taken with respect to the DOJ Bulk Data Rule and PADFAA. A number of member companies reported sophisticated, multi-step frameworks to address obligations that included data flow mapping, transfer impact assessments, third-party screening systems, and transaction evaluation checklists. The most common compliance action reported by members was an update to contracts and data processing agreements to include representations and warranties that counterparties are not "covered persons" or otherwise connected to countries of concern. Some companies' compliance programs reflected a broader approach where they would identify restricted and prohibited transactions, conduct robust due diligence before onboarding new partners, embed required clauses in contracts, and establish ongoing audit and oversight

[42] Cal. Code Regs. tit. 11 § 7100.

processes. Members that have taken these more comprehensive steps were positioned to identify and address potential gaps before they became operational risks, as enforcement appears to ramp up.

The NAI staff observed that a number of members are seeking greater clarity on the relationship between the DOJ Rule and PADFAA, and in particular, on where compliance strategies for the two frameworks should diverge. Several members noted that they had taken measures to address obligations for both laws, and acknowledged uncertainty about whether meaningful distinctions warranted differentiated approaches.

During Privacy Review meetings, the NAI staff encouraged members to carefully evaluate the full scope of these laws, including the laws' definitions of data and identifiers that are broadly classified as sensitive, and review how the companies are performing due diligence on customers, partners, and vendors, particularly for any foreign-controlled entities, and to consult with counsel where applicability is uncertain.

e. Looking Ahead to the 2026 NAI Privacy Review Cycle

What's next for the Privacy Review Program.

As the NAI plans for the 2026 Privacy Reviews, staff is focused on how best to assist members as they confront new privacy challenges. Members demonstrated a strong investment of time and resources in complying with privacy laws and adhering to the NAI Privacy Framework during the 2025 review cycle. Staff will build on this meaningful engagement to evolve the Privacy Review questionnaire and topics to be covered in the next review cycle.

ONGOING FOCUS

Continued Testing of Opt-Outs, Data Broker Registration & the DROP

The NAI staff plans to continue to test opt-out mechanisms and will also study the trend of user experiences varying across jurisdictions (e.g., California IP address compared with a Massachusetts IP address) and how that impacts consumer experience, choice, and gating of access to tools. The NAI staff will continue to follow whether and how members register as data brokers, align disclosures with practices, and integrate with the Delete Request and Opt-out Platform ("the DROP").

The NAI staff will also continue to discuss the importance of considering all data practices and whether there is a need for each member company to register as a data broker, particularly in California, where fines for failing to register (and thereby failing to honor deletion requests when the DROP comes online) are expected to grow and be a significant potential liability. As demonstrated by the 2025 cycle, the Privacy Review Program serves as a valuable check on gaps that can develop over time as data processes, laws, and staff change.

NEW DILIGENCE

Accountability Related to Cross Border Data Flows

In addition to reviewing websites, consumer-facing tools, and integrations, the NAI will be doing diligence on broader topics in the coming cycle. As the NAI has updated its membership agreement to include a commitment from members that the members are not "Covered Persons" as defined by the DOJ Rule, the NAI will be taking steps in the next cycle to check accountability on those representations of members.

The NAI has a proposal pending for a similar member commitment where members will make representations that they are not "Covered By A Foreign Entity" as defined by PADFAA as part of the 2027 NAI membership agreement, and related due diligence questions will follow as part of the NAI Privacy Review Program. The NAI will develop guidance to help members navigate these requirements and the laws more broadly.

TOOLS & FEEDBACK

Building Practical Tools & Integrating Consumer Insights

Finally, the NAI staff will continue to develop tools that will aid members in adherence with the Framework and overall posture for compliance in the marketplace. The NAI created a consumer inquiry form for feedback related to member company's privacy practices and will be integrating any feedback about specific member companies into the next Privacy Review cycle to elevate any consumer concerns and inquiries.

The NAI staff will use member feedback about what is helpful for members to inform and create practical tools, to include a record to show that members have responded to the NAI's Privacy Review Program questionnaire and had their NAI review.

IV. Public Policy Advocacy

Engaging with policymakers.

IN THIS SECTION

— Federal engagement
— State legislative tracking
— Regulatory rulemaking and enforcement
— Industry collaboration

IV. Public Policy Advocacy

Regulator Dialogue

Engaged in discussions with state and federal regulatory agencies to better understand regulatory enforcement trends and priorities, and to translate these into practical member guidance to enable member companies to align their digital advertising models with evolving legal standards.

State & Federal Legislation

Closely monitored legislative developments at both state and congressional levels to advise member companies about emerging legal trends, and to advocate for consensus approaches that balance the need for stronger consumer privacy and data protection with the need to preserve the viability of data-driven advertising across digital media.

Regulatory Filings

Filed over a dozen sets of comments with state and federal regulatory agencies, seeking to inform and promote consistent and practical regulations and enforcement approaches across sometimes disparate jurisdictions.

In conjunction with the NAI's industry-leading self-regulation, the NAI leverages insights from its Privacy Review Program to inform our recommendations to policymakers. Over the past year, the NAI submitted over a dozen U.S. state and federal regulatory and legislative filings, while also engaging directly with policymakers at the state and federal level. The NAI's priorities included the following issues.

PROMOTE

Industry Self-Regulation and Data Governance Processes that Align with the Current U.S. Privacy Regulatory Environment

The NAI's Privacy Framework is built on the core premise of collaboration between industry and U.S. regulatory officials, whereby the NAI educates industry about key legal requirements and regulator expectations that are relevant to digital advertising, with a focus on ad-tech businesses. Conversely, the NAI also educates policymakers and regulators about key issues affecting our members and the industry at large, informed by our hands-on privacy reviews with each member company.

The NAI champions a self-regulatory approach that combines robust industry education and coordination around consensus practices to help businesses operationalize strong state and federal regulation. Through engagement with policymakers and our industry thought leadership, the NAI seeks to balance strong consumer data protection with technological realities to promote compliance with key priorities expressed by U.S. regulators.

PROMOTE

a Uniform National Privacy Legal Framework

The establishment of a durable, national privacy framework remains the NAI's primary federal objective, as replacing the current fragmented state landscape would offer meaningful consistency for companies and consumers alike. Throughout the past year, we have actively engaged with bipartisan leadership across both chambers of Congress to advocate for a comprehensive legislative model anchored by several fundamental pillars:

- Adopt a robust data governance framework that combines practical definitions, a set of strong and consistent consumer rights, and affirmative responsibilities for businesses.
- Adopt a data minimization standard that enables beneficial data uses with meaningful guardrails.
- Establish a clear definition and criteria for "de-identified data" to reduce privacy risks and treat data that has been de-identified as no longer meeting the definition of personal information.
- Level the playing field for all entities across the digital media industry rather than favoring companies based on their market position as either a first or third-party.
- Promote robust enforcement by federal and state regulators.

PROMOTE

Interoperability and Consistency Across U.S. State and Federal Privacy Frameworks Through Rulemaking or Interpretive Guidance

Where state statutes permit, the NAI has encouraged agencies to develop regulations that align core implementation elements across jurisdictions so companies can build privacy compliance once and deploy it consistently.

The NAI works to educate about the need for scalable, operationalizable rules and cross-state consistency, particularly in states actively engaged in rulemaking in 2025, such as California, Colorado, and New Jersey, and through interpretive guidance and opinion letters in those states that do not have rulemaking authority. Combined, these tools improve compliance more effectively than enforcement alone, and they are essential inputs for self-regulatory organizations like the NAI to promote effective compliance. The NAI also promoted the use of flexible safe harbors or compliance pathways based on standard disclosures and forms, rather than one-size-fits-all mandates.

PROMOTE

Effective Consumer Choice Mechanisms & Opt-Out Preference Signals

The NAI has been a leading proponent of policies that support the development and adoption of robust, user-friendly privacy controls, including the Global Privacy Control (GPC). In conjunction with the NAI's release of new consumer resources in 2025 to promote user choice in accordance with new legal requirements, including the launch of a user-friendly GPC browser extension, detailed instructions to exercise choices via

platform-level controls, and sunsetting its legacy opt-out tools, the NAI prioritized engagement on this issue at both the state and federal level.

The NAI has specifically emphasized the consistent set of state legal requirements for provision of Opt-Out Preference Signals, such as the need to represent affirmative consumer intent, be free of default activation, and not be implemented in a way that unfairly disadvantages other businesses. The NAI continues to highlight the potential threat to consumers and a competitive marketplace if browser or platform providers implement these signals that preference their own business models.

PROMOTE

Protections for Sensitive Data That Are Strong, Consistent, and Risk-Based

The NAI has consistently promoted policies that provide strong protections for sensitive personal information, while avoiding overly broad definitions and scope that could result in unnecessary restrictions on responsible uses of this data that are authorized by and beneficial to users. Specifically, the NAI promotes the following objectives across this important data set:

- **Children's data** — State policies should align with the Children's Online Privacy Protection Act (COPPA) to the greatest extent possible, avoid requirements for age verification, apply a multi-factor test to determine the direction of websites and apps, and assign primary responsibility to first parties to determine the intended audience, rather than third-party companies that are not in a position to make these determinations.
- **Precise location data** — Define a category of "sensitive locations" where consumers expect and deserve heightened protections beyond opt-in consent already required, using the NAI's Voluntary Enhanced Standards for Precise Location Information as a model to limit processing, selling, and sharing of data associated with sensitive locations. Policies should distinguish between precise location (accuracy within a radius of about 1,750 feet, often relying on a mobile device's GPS) vs. coarse location (less precise, often using Wi-Fi and mobile data signals rather than GPS) and encourage businesses to de-identify, rely on aggregate data, or generally render precise location data non-sensitive where possible.
- **Sensitive health data** — Adopt a targeted, risk-based approach to health data—rejecting overly broad definitions and rigid consent regimes that would sweep in routine digital advertising data. This approach is reflected in the *NAI's Factor Analysis for Health-Related Sensitive Personal Information*,[43] and avoids sweeping in low-risk data and creating unnecessary limitations on collection or processing in the absence of a significant risk of harm. The NAI also recommends a distinction be retained between

[43] *See* Network Advertising Initiative, *Factor Analysis for Health-Related Sensitive Personal Information*, (Feb. 24, 2026), https://thenai.org/wp-content/uploads/2026/02/NAI_Factor-Analysis-for-Sensitive-Health-Information_02242026.pdf.

HIPAA-regulated data (e.g., health records, medical bills) and sensitive health data that is outside the scope of regulation by the Department of Health and Human Services (HHS), but is still related to health in such a way that may warrant additional protections (e.g., data from period tracker apps and wearable technologies). The NAI encourages the adoption of enhanced consent requirements that are effective yet practical to deploy.

PROMOTE

Effective Transparency and Control Requirements for Data Brokers

The NAI supports the goal of increasing consumer transparency about data collected and stored by data brokers, and empowering consumers to exercise deletion and opt-out rights, including through centralized mechanisms such as California's Deletion Request and Opt-out Platform (DROP). Across multiple engagements with regulators in California and other states, the NAI has advocated for workable, risk-based obligations that align with how data broker systems actually operate, and that ensure data broker registries are designed with data minimization and technical feasibility in mind. Specifically, data brokers should only be required to process requests for data tied to identifiers they can reasonably match, and they should not be obligated to collect or process additional personal information or retrieve or maintain deletion lists that cannot be operationalized. In our public policy engagement in 2025, the NAI also prioritized the following objectives:

- Harmonize data broker requirements with existing privacy frameworks and avoid duplicative or conflicting obligations, ensuring that consumer protections are strengthened without creating unnecessary operational burdens or unintended privacy risks.
- Adopt clear definitions, such as what constitutes a data broker, and data associated with a matched identifier to ensure consistent and predictable compliance.
- Build infrastructure and practices that ensure safeguarding system integrity, including protections against unauthorized or fraudulent use of centralized request mechanisms that could inadvertently increase risk for consumers.

AVOID

Seeking to Accomplish Consumer Data Protection Objectives Through the Adoption of Novel AI Policies

There is significant overlap between U.S. data privacy laws and newer laws and regulations pertaining to AI. While both policy frameworks maintain a central objective to protect consumers from harms resulting from the processing of their PI/SPI, the NAI encouraged policymakers to prioritize data privacy frameworks to achieve this objective. The NAI has also encouraged policymakers to avoid unnecessarily restricting businesses' utilization of AI without significant corresponding privacy protection. Optimally, requirements for transparency and control around AI should be crafted to align effectively with data privacy

notices. Specifically, the NAI has made several key recommendations related to AI laws and regulations:

- Avoid novel opt-in requirements for AI uses, such as training, unless the statute clearly requires them.
- Align transparency and choice requirements so they fit existing data privacy notice-at-collection requirements, rather than creating redundant, overlapping notice and choice architectures.
- Ensure that transparency requirements protect trade secrets when operationalizing data access rights.
- Apply existing legal requirements to AI training, such as transparency, data minimization, purpose limitation, and consumer rights.

PROMOTE

Policies That Ensure Consumer Authorized Agents Act Responsibly on Behalf of Consumers

Consumers in the U.S. deserve privacy rights such as the ability to opt out of targeted advertising and request access to or deletion of their personal information. The NAI recognizes consumer authorized agents as a potentially useful tool. However, these are inconsistently defined across current state laws and operate in a fragmented environment, where more attention is needed to ensure they achieve desired objectives. The NAI has promoted two steps for policymakers to achieve these objectives.

First, the NAI recommends that regulators enforce against agents selling tools that amount to deceptive marketing, misrepresenting their services, and violating subscription cancellation rules. Regulators can also enforce reasonable security measures for agents to prevent indiscriminate sharing of their customers' personal data. Further, the NAI recommended that legislators and regulators promote standards in the authorized agent market, such as standardized request forms and technical specifications. This would help ensure businesses have the information they need to act on a request and may help minimize the amount of information agents include in requests.

V. Conclusion & Outlook

Looking forward.

IN THIS SECTION

— The Regulatory Road Ahead
— Technology Trends Shaping the Industry
— The NAI's Future Priorities
— A Call to Engage

V. Conclusion & Outlook

The Regulatory Road Ahead

The privacy compliance landscape that NAI members will navigate in 2026 and beyond is defined by one overriding trend: the center of regulatory gravity in the United States has shifted decisively to the states.

> ***With 21 comprehensive state privacy laws now on the books and enforcement activity reaching unprecedented levels, the era of treating privacy as a static, one-time compliance exercise is over.***

Several developments will demand particular attention in the year ahead. In California, the launch of the Delete Request and Opt-Out Platform (DROP) system introduces a centralized mechanism for consumer deletion requests with significant per-violation penalties for noncompliance. New operational requirements around automated decision-making technology, risk assessments, and cybersecurity audits are also now in effect. The California Privacy Protection Agency has indicated it is pursuing hundreds of open investigations, and a reformed funding model—in which enforcement revenue directly replenishes the agency's budget—will only expand its capacity over time.

Beyond California, Texas has established itself as an aggressive enforcement jurisdiction, with settlements related to alleged privacy violations exceeding $1 billion in 2025. Multi-state coordinated enforcement—particularly around Global Privacy Control compliance—emerged as a defining trend, with bipartisan coalitions of state attorneys general conducting joint sweeps and investigations. Sensitive data categories, including health information, precise geolocation, biometrics, and children's data, remain at the center of regulatory attention across jurisdictions.

Until consensus can be achieved in Congress on a uniform national privacy law, state-driven laws and regulations will continue to be a major driver of the industry compliance landscape.

> ***The NAI's focus will be to continue to help advertising technology companies navigate a complex and evolving patchwork which is what our self-regulatory program is substantially geared toward.***

Technology Trends Shaping the Industry

The advertising technology industry continues to undergo significant structural change. Several technology trends will shape the privacy landscape in 2026 and intersect directly with the NAI's work:

Artificial Intelligence (AI)

AI-driven tools are transforming how advertising is created, targeted, measured, and optimized. Members have long been on the cutting edge of using AI and machine learning (ML) for various functions, but agentic AI is now promising to further power and streamline the entire programmatic workflow, boosting efficiency and allowing teams to dedicate more time to strategic planning. As policymakers across the country continue to grapple with regulating AI systems, the NAI is actively exploring this space and plans to develop resources that help members address AI governance within their existing privacy programs.

Privacy-Enhancing Technologies

PETs—including trusted execution environments, multiparty computation, differential privacy, and zero-knowledge proofs—are moving from theoretical interest to practical deployment. Our 2025 PETs Primer provided a foundation for understanding these tools, and the NAI expects to build on this work as adoption accelerates and regulators begin to evaluate how PETs interact with consent and data minimization requirements.

Identity and Signal Evolution

The decreasing availability of third-party cookies and the growth of alternative identity solutions—along with the rise of Universal Opt-Out Mechanisms/Opt-Out Preference Signals such as GPC—are reshaping how the industry manages consumer preferences and data flows. The NAI created a Consumer Choice Task Force in 2025, and we will continue working with members, policymakers, and other stakeholders to develop guidance and best practices to assist and promote industry compliance with current state legal requirements.

Emerging Media Channels

Connected TV, retail media networks, and in-game advertising are a few examples of data collection contexts where industry is actively working to align practices with existing privacy frameworks. In some cases, frameworks were not created with these contexts in mind. Therefore, the NAI is actively working with members and other stakeholders to apply consistent practices across these platforms that align with legal requirements. Recent enforcement activity around smart TV data practices underscores the need for companies to prioritize compliance across these contexts in 2026.

The NAI's Future Priorities

As we look to the year ahead, the NAI's agenda is shaped by the regulatory realities and industry developments described above. Our priorities for 2026 include:

Continuously Improving the Privacy Review Program

by refining our review standards as we gain experience under the new Framework and by developing enhanced guidance to help members address common compliance challenges identified during the 2025 review cycle.

Developing AI and Advertising Governance Resources

building on our working group discussions to provide practical frameworks for responsible AI use in advertising technology.

Better Informing Public Policy and Enforcement

by leveraging the insights that we gained from our 2025 privacy review cycle, and working even more closely with policymakers and enforcement officials as they continue to develop and enforce policies to strengthen consumer data protections.

We've heard loud and clear the call for more direct engagement, and we will heed that call.

Advancing the Consumer Choice Task Force's Work

with the goal of publishing best practices around Opt-Out Preference Signals and universal opt-out mechanisms that help members comply with the growing number of states requiring GPC recognition.

A Call to Engage

> ***The NAI's strength has always come from the engagement and commitment of its community.***

To our current members: thank you. Your participation in the Privacy Review Program, your contributions to our working groups and task forces, and your desire to establish your businesses as leaders in responsible data governance and heightened privacy standards are what make our self-regulatory model work. We encourage you to deepen your engagement—there is more to do, and your expertise and perspective are essential.

To companies considering NAI membership: the value proposition has never been stronger. In an era of accelerating state enforcement and rising compliance complexity, the NAI offers specialized guidance, peer collaboration, an independent accountability framework, and a voice in the policy conversations that shape your operating environment. We invite you to learn more at thenai.org or by contacting membership@thenai.org.

To policymakers and regulators: the NAI remains committed to constructive engagement. Self-regulation works best when it operates in dialogue with policymakers and enforcement officials. The NAI therefore welcomes continued opportunities to share our expertise, our data, and our perspective on how to achieve strong consumer privacy protections while preserving the competitive, innovative digital advertising ecosystem that benefits consumers, businesses, and publishers alike.

> ***Twenty-five years later, the NAI's mission is more important than it has ever been. The challenges are real, the stakes are high, and the work continues.***
>
> ***The NAI looks forward to what we will accomplish together with our members and partners to advance our mission of promoting Privacy, Trust & Accountability across the digital advertising industry.***

25 Years of *Privacy Self-Regulation*

NAI

PRIVACY, TRUST & ACCOUNTABILITY

thenai.org

The NAI

@NAI