April 7, 2025

The Honorable Brett Guthrie, Chairman
The Honorable John Joyce, Vice Chairman
House Committee on Energy & Commerce
2161 Rayburn House Office Building
Washington, DC 20515

RE: Privacy Working Group RFI

Dear Chairman Guthrie and Vice Chairman Joyce:

The Network Advertising Initiative (NAI) commends the House Privacy Working Group for undertaking a thorough review of existing privacy laws and seeking input on a prospective federal comprehensive data privacy and security framework ("National Privacy Framework"). The current patchwork of U.S. state consumer privacy laws provides inconsistent protection for American consumers and subjects U.S. businesses to regulatory fragmentation that stifles innovation, growth, and the provision of valuable services. Congress has the opportunity to replace this patchwork with a unified National Privacy Framework that benefits consumers, businesses, and the economy.

Founded in 2000, the NAI is the leading non-profit, self-regulatory trade association for advertising technology companies. For 25 years, the NAI has promoted strong consumer privacy protections, a free and open Internet, and enabled small businesses to thrive by promoting the highest voluntary industry standards for the responsible collection and use of consumer data.[1]

The NAI recommends that any National Privacy Framework should enshrine key areas of consensus that exist across current U.S. state privacy laws; and harmonize and simplify elements of those laws where they diverge. To that end, the NAI offers the following key recommendations, discussed in greater detail below:

- 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.
- 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 reasonable data minimization standard that enables beneficial data uses with meaningful guardrails.

[1] *See History of the NAI*, The Network Advertising Initiative, https://thenai.org/about-the-nai-2/history-of-the-nai/.

I. Roles and Responsibilities

Clear Data Responsibilities

The U.S. digital advertising industry is a vibrant segment of the U.S. economy, accounting for $225 billion in annual revenue in 2023.[2] Digital products and services are primarily ad-supported and contribute 12 percent to the U.S. GDP.[3]

Tailored advertising, which uses data to inform the selection and delivery of ads, is essential to ensure a robust, competitive digital media industry where small content creators and advertisers can compete more effectively with large digital platforms. The NAI compiled a comprehensive summary of empirical and survey research highlighting the key benefits of tailored advertising,[4] including the following findings:

- Consumers: 95% of consumers prefer consuming ad-supported content over paid subscriptions.[5]
- Advertisers: Tailored advertising optimizes ad spending, making small businesses 16 times more likely to see sales growth[6] and saving 37% on customer acquisition costs.[7] 69% of small and medium advertisers say they couldn't have launched or sustained their business without tailored ads.[8]
- Publishers: Tailored advertising fuels a free and diverse internet, driving 52% more revenue per user,[9] keeping content accessible, and helping small publishers compete in a market that favors the largest platforms.
- Society: Tailored digital ads save lives and strengthen public safety—boosting vaccination rates by up to 50% in underserved communities[10] and making gun owners 5x more likely to seek firearm safety information.[11]

---

[2] Interactive Advertising Bureau. "Internet Advertising Revenue Report." April 2024. https://www.iab.com/wp-content/uploads/2024/04/IAB_PwC_Internet_Ad_Revenue_Report_2024.pdf.

[3] Fed. Trade Comm'n, Comment Letter on the ANPR on Commercial Surveillance and Data Security at 2 (Nov. 10, 2022), https://internetforgrowth.com/wp-content/uploads/2022/11/I4G-sign-on-letter_FINAL_11.10.22.pdf.

[4] Network Advertising Initiative, Benefits of Tailored Advertising (Mar. 2025), https://thenai.org/wp-content/uploads/2025/03/NAI_Benefits-of-Tailored-Advertising_032025_final.pdf.

[5] IAB, The Free and Open Ad-Supported Internet 10 (2024), https://www.iab.com/wp-content/uploads/2024/01/IAB-Consumer-Privacy-Report-January-2024.pdf.

[6] Deloitte, Dynamic Markets: Unlocking small business innovation and growth through the rise of the personalized economy, at 2 (2021), https://internetforgrowth.com/wp-content/uploads/2022/11/Deloitte-Dynamic-Markets-Small-Business-Through-the-Rise-of-the-Personalized-Economy.pdf.

[7] Nils Wernerfelt, et al., Estimating the Value of Offsite Data to Advertisers on Meta 24 (Becker Friedman Inst., Working Paper No. 2022-114), https://bfi.uchicago.edu/wp-content/uploads/2022/08/BFI_WP_2022-114.pdf.

[8] DataCatalyst, The Value of Digital Ads for Small Businesses: National Survey of SMB Leaders, at 12 (2023), https://datacatalyst.org/wp-content/uploads/2023/01/The-Value-of-Digital-Ads-For-Small-Businesses_-National-Survey-of-SMB-Leaders-13Jan2023.pdf.

[9] Garrett A. Johnson, et al., Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?, 39 Mktg. Sci. 1, 25 (2020); Garrett Johnson, Comment Letter on Trade Regulation Rule on Commercial Surveillance and Data Security (Oct. 24, 2022), https://www.regulations.gov/comment/FTC-2022-0053-0680.

[10] Joseph N. Luchman, et al., Association Between the United States Department of Health and Human Services' COVID-10 Public Education Campaign and Initial Adult COVID-10 Vaccination Uptake by Race and Ethnicity in the United States, 2020-2022, 25 Health Promotion Prac. 602, 606 (2024).

[11] Brady United, Annual Report Fiscal Year 2023 14 (2024), https://brady-2-stage.s3.amazonaws.com/Annual-Report-FY-23-Digital.pdf.

Nearly 80 percent of digital advertising revenue is currently concentrated across the ten largest online companies.[12] This imbalance exists because most websites and apps lack the scale and technical capabilities to compete with the large online platforms. Therefore, to maximize the value of their businesses, these companies regularly utilize advertising-technology (ad-tech) companies as partners in the provision of data-driven advertising, which includes tailored advertising (also referred to as targeted advertising), contextual advertising, and advertising analytics, measurement, and optimization services.

A National Privacy Framework should reduce privacy risks while promoting the continued growth of the ad-supported digital media industry. To that end, it should acknowledge and support the distinct and complementary roles that each party plays, create a responsible data stewardship framework that applies to all entities, and be mindful not to favor companies based on their position in the marketplace. The fact that a company collects information about consumers in a first-party instead of a third-party context does not make that company inherently better at protecting consumer privacy. For example, a third-party company providing advertising analytics and measurement is essential for effective digital advertising, and these services can be performed in a way that presents no greater risk than a first-party business that collects the same information directly from their users.

A national law that maps responsibilities to specific functions—controller, processor, or third party—is important to avoid confusion and provide consumers with consistent protections across different organizational structures. This approach also encourages businesses to clarify their data relationships in contractual agreements, thereby enhancing accountability. U.S. state laws are largely consistent in how they define and treat businesses within the digital media industry. These laws commonly categorize entities as "controller," "processor," or "third party." Controllers bear the primary responsibility for ensuring privacy rights compliance and can require processors and third parties to assist in fulfilling these rights.[13]

Most importantly, specific obligations and restrictions on third parties should be crafted with effects on competition in mind, particularly when third parties are already subject to all of the requirements of controllers. Such anticompetitive treatment benefits large first party data holders, and it disadvantages other businesses that are essential to the digital media industry – for example, the American Privacy Rights Act (APRA) would have favored first parties by requiring for opt-in consent for tailored advertising across websites, compared to an opt-out approach for first-party advertising.[14]

Affirmative Data Governance Obligations

A National Privacy Framework should establish three key data governance obligations that are foundational to consumer data protection: (1) mandatory data protection assessments (DPAs) for companies that process PI in a way that could pose risk to a consumer; (2) contractual requirements among entities that share PI; and (3) clear and practical diligence requirements. Data transparency and control, while foundational to all data privacy frameworks, is broadly recognized to have limitations in

[12] Id. at 1.

[13] *See, e.g.* Colo. Rev. Stat. § 6-1-1305 (requiring controllers and processors to meet their respective obligations and stating that processors "shall adhere to the instructions of the controller and assist the controller to meet its obligations"); Tex. Bus. & Com. Code § 541.104; Va. Code Ann. § 59.1-577(A).

[14] As APRA defined "Online Activity Profile" as sensitive covered data scoped to online activity *across third-party websites*, it effectively created a framework requiring opt-in consent for tailored advertising products, giving first-party advertising providers a competitive advantage. *See* American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 101(41).

achieving privacy and data protection. Over-reliance on this approach unfairly shifts the burden of data collection from businesses to consumers.[15]

Companies that utilize consumer data should be good stewards of that data, regardless of how a consumer chooses to exercise their privacy rights through notice and choice mechanisms, and irrespective of what role they play in the digital ecosystem. Good data governance, including thorough risk assessments, business partnership requirements, and proper due diligence, is vital to protect against different and unanticipated risks associated with modern data processing, and helps to protect all consumer data, even data not subject to consumer control.

Data protection assessments for specific types of data are required by many state laws, help companies understand the potential risks and benefits of data processing, and create a roadmap for data stewardship throughout the data life cycle.[16] Contractual requirements can help business partners clarify use cases and restrictions for shared data, and due diligence to ensure that both data protection assessments and contractual requirements are honored is essential to data stewardship.

II. Personal Information, Transparency & Consumer Rights

Effective privacy protections rely on clear definitions of key terms, such as "personal information (PI)" and "sensitive personal information (SPI)," to ensure that companies provide the requisite notice and choice to consumers, encourage data minimization, and create incentives for businesses to provide additional protections from downstream misuse and harms. The myriad state laws are nearly unanimous in their treatment of PI and SPI, creating an opt-out standard associated with certain processing and sharing of PI, and requiring businesses to obtain opt-in consent from consumers before a business may process SPI.[17]

Personal Information (PI)

PI should be defined as "any information that is linked or reasonably linkable to an identified or identifiable individual." The definition should not seek to encompass "households" as California has sought to do,[18] as this risks creating consumer choice conflicts within a household. It should also define and exclude aggregated, de-identified, and publicly available data.

Pseudonymous Data

Pseudonymous data is an important subset of PI that offers enhanced privacy protections for consumers. When appropriate administrative and technical controls are in place, this data cannot be attributed to a specific individual without being combined with additional PI. Pseudonymous data has been a central facet of protective processing in digital advertising for decades. Many states correctly exclude pseudonymous data from the scope of access, correction, deletion, and portability rights, as these functions require a company to link additional PI to the pseudonymous data to fulfill these

---

[15] *See* Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, J. High Tech. L. (2013); *See also* Jen King et al., *Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interact*, World Economic Forum, 1, 26 (July 2020).

[16] Va. Code Ann § 59.1-576; Tenn. Code Ann. § 47-18-3307; Tex. Bus. & Com. Code § 541.105.

[17] With the exception of California, all enacted state consumer privacy laws that define "sensitive personal information" or "sensitive data" require affirmative opt-in consent before a controller may process such data. See, e.g. that a controller shall "not process sensitive data concerning a consumer without obtaining the consumer's consent."

[18] *See* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(v).

requests.[19] A federal law should take the same approach: incentivize businesses to utilize pseudonymization as a privacy enhancing step.

Sensitive Personal Information (SPI)

As a critical element in promoting privacy for consumers, SPI should be reasonably defined and take a risk-based approach that focuses on preventing uses of data that present special risks of harm, while preserving valuable uses of data that benefit both consumers and businesses.[20] For example, the majority of state privacy statutes include core sensitive data elements, such as genetic or biometric data that is processed for the purpose of uniquely identifying an individual; personal data collected from a known child; and precise geolocation data. However, the treatment of information related to consumer health is more complex and is not addressed consistently across state laws.

An overly broad definition of SPI that encompasses virtually all data related to health or the human body should be avoided. Adopted by some states, broad definitions of SPI may include information that does not pose special risks or sensitivities to consumers.[21] For example, including information about any health-related "treatment"[22] as a form of sensitive personal information could sweep in harmless information, such as whether a consumer has purchased band-aids (to "treat" a cut or scrape) after seeing an ad for band-aids, or purchased ibuprofen (to "treat" a minor ache or pain) after seeing an ad for a particular brand of over-the counter pain reliever. Applying a heightened standard for SPI to this type of benign data needlessly increases friction for businesses processing it for legitimate purposes and generally undermines the concept of particularly sensitive data that deserves special protections.

This distinction is particularly important in the context of data-driven advertising and marketing, where tailored ads provide significant benefits to consumers based on non-sensitive health conditions, such as the illustrative examples above and other run-of-the-mill issues that – while related to health and the human body – are by no stretch of the imagination sensitive. The definition of SPI should therefore focus on uses of PI that pose specific, heightened risks of harm, and avoid sweeping in additional data types

[19] Several state privacy laws – including those in Colorado, Connecticut, Delaware, Indiana, Kentucky, Minnesota, Montana, Nebraska, New Hampshire, Tennessee, Texas, and Virginia – explicitly exempt pseudonymous data from certain consumer rights, so long as the controller "can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information." CRS 6-1-1307(3). These laws illustrate how existing frameworks balance privacy protection with operational feasibility.

[20] The Texas Data Privacy and Security Act is a good, albeit imperfect, example as its definition of SPI appropriately includes data that is used to derive sensitive data types, which contrasts with various other state statutes that define SPI to include a much wider range of information that *could* be used to make a sensitive data inference. *See* Tex. Bus. & Com. Code § 541.001(29) ("Sensitive data means a category of personal data. The term includes: (A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status; (B) genetic or biometric data that is processed for the purpose of uniquely identifying an individual; (C) personal data collected from a known child; or (D) precise geolocation data.") (quotations removed).

[21] For example, Washington's My Health My Data statute defines "consumer health data" broadly to include a consumer's "past, present, or future physical or mental health status" and any information derived or extrapolated from non-health information that could be seen as making a health-related inference about the consumer. *See* Wash. Rev. Code § 19.373.010(8); *see also* New York Health Information Privacy Act, S 929, 2025 Leg. (NY 2025) (defining "regulated health information" to include inferences drawn or derived about an individual's physical or mental health without limitation).

[22] Washington's My Health My Data's definition of "consumer health data" also includes "[i]ndividual health conditions, treatment, diseases, or diagnosis[.]" Wash. Rev. Code § 19.373.010(8)(v)(i) (emphasis added).

without carefully balancing the potential benefits with potential risks. This may be accomplished by creating a framework where companies are required to make risk determinations based on processing, whether the processing results in a sensitive inference or reveals SPI that may create a heightened risk of harm to consumers.

Definitions such as those used across most of the state laws make this important distinction, only characterizing PI as sensitive when it is actually used to identify a specific health condition or diagnosis.[23] Contrasting with the above examples, even though ibuprofen is technically a "treatment" that can be used to alleviate minor aches and pains, businesses do not need to – and generally do not – use information about the purchase of ibuprofen over-the-counter to identify a specific health condition or diagnosis. The definition of sensitive health information should allow for this distinction as it permits a valuable level of flexibility. For example, if a business *were* to use combinations of otherwise benign PI – like the purchase of ordinary consumer goods – *for the purpose* of inferring or identifying a consumer's specific health condition, then in that case the inference about the consumer's health condition would itself qualify as sensitive information.[24] The outcome of processing is a key element under this approach, which should be buttressed by the affirmative requirements discussed below to ensure consumer data is properly characterized, protected, and aligned with the appropriate requirements for transparency and control. Conversely, crafting an overly broad definition causes an over-reliance on consent, which in turn leads to consent fatigue for consumers.[25]

Consumer Data Rights, Transparency, and Control

All state privacy laws provide consumers with individual rights, which may include the rights of access, correction, deletion, and opting out of the "sale" of PI, "targeted advertising," and profiling with a legal or similarly significant effect.[26] All consumer rights should be subject to reasonable verification requirements and certain exceptions, including exceptions for pseudonymous data in certain circumstances as noted above, such as routine and essential practices like provision of contextual advertising and the provision of security, essential analytics and measurement, and fraud prevention – consistent with the approach taken in the Children's Online Privacy Protection Act Rule.[27]

A National Privacy Framework should build on the broadly aligned transparency provisions in existing state laws by establishing a uniform standard for privacy notices and consumer choice. Across these laws, there is a strong consistency in requiring disclosures about the categories of personal data processed, the purposes for which the data is collected and used, and the categories of third parties with whom personal data is shared.[28]

---

[23] For example, Connecticut considers personal data to be "Consumer Health Data" only when the personal data is "use[d] to identify a consumer's physical or mental health condition or diagnosis[.]" Conn. Gen. Stat. § 42-515(9).

[24] In this example, Target's use of benign purchase data to infer a consumer was pregnant would qualify as sensitive information. *See* Target Hill, Kashmir, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, Forbes.com (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

[25] Luis Alberto Montezum & Tara Tauman-Bassirian, *How to Avoid Consent Fatigue*, IAPP (Jan. 29, 2019), https://iapp.org/news/a/how-to-avoid-consent-fatigue/.

[26] See, e.g., Colo. Rev. Stat. § 6-1-1306; Va. Code Ann. § 59.1-577; Conn. Gen. Stat. § 42-518; Tex. Bus. & Com. Code § 541.051.

[27] See definition of "Support for the internal operations of the Web site or online service," Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013).

[28] See, e.g., Colo. Rev. Stat. § 6-1-1308(1); Va. Code Ann. § 59.1-578(C); Tex. Bus. & Com. Code § 541.052.

Transparency and choice surrounding the processing of SPI should meet a higher standard threshold; be provided in a clear and conspicuous manner; explain what data will be collected and processed; and provide the categories of entities that this data may be shared with, and for what purposes data will be processed and shared. Over the years, the NAI has played a leading role in promoting robust notice and choice architecture for the collection and use of PI for advertising and marketing,[29] and in some cases for non-marketing use cases.[30]

Opt Out Preference Signals

A National Privacy Framework should provide consumer opt-out rights through user-enabled opt out preference signals (OOPS). The law should establish a clear, uniform set of criteria for the implementation of OOPS to ensure that they reflect authentic consumer choices, are easy to use, and are deployed in a manner that does not unfairly advantage the platforms sending the signals; nor unfairly disadvantage businesses that receive the signal. The law should also establish a process, led by the Department of Commerce (DOC) through which OOPS can be evaluated and approved, including their specific implementation in browsers or across other connected devices.

Twelve state privacy laws currently require companies to honor OOPS[31] deployed across browsers as an opt out of targeted advertising and sales of personal information,[32] with some laws extending it to profiling.[33] These laws broadly include common, well-considered safeguards to ensure their adherence to key requirements and functionality. While the specific statutory language varies, these laws are largely aligned on key principles that should guide a federal approach:

- A valid OOPS must not rely on default settings but must reflect an affirmative, freely given, and unambiguous choice by the consumer;[34]
- The signal must be consumer-friendly and easy to use by the average consumer;[35]
- An OOPS must not unfairly disadvantage another controller.[36]

---

[29] NETWORK ADVERTISING INITIATIVE, Best Practices for User Choice and Transparency (2022), https://thenai.org/wp-content/uploads/2022/05/NAI-Dark-Patterns-Final-5.12.22.pdf; *See also* Ryan Smith, *Takeaways for Digital Advertising Businesses from the FTC Staff Report on Dark Patterns*, Network Advertising Initiative (Oct. 20, 2022), https://thenai.org/takeaways-for-digital-advertising-businesses-from-the-ftc-staff-report-on-dark-patterns/.

[30] NETWORK ADVERTISING INITIATIVE, Best Practices: Using Information Collected for Tailored Advertising or Ad Delivery and Reporting for Non-Marketing Purposes, https://thenai.org/wp-content/uploads/2021/07/nai_nonmarketing-bestpractices-0620_final-1.pdf (2020).

[31] The twelve states with privacy laws that recognize OOPS are California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, and Texas.

[32] "Selling" personal information is broadly defined as the selling, releasing, or disclosing of a consumer's personal information to a third party for monetary or other valuable consideration. *E.g.* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(ad); Tex. Bus. & Com. Code § 541.001(28).

[33] "Profiling" is widely defined as any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. E.g. Cal. Civ. Code § 1798.140(z); Tex. Bus. & Com. Code § 541.001(24). Although most states do not require businesses to honor OOPS signals for profiling, California and New Jersey have suggested they might require this functionality in the future. *See* N.J. Stat. Ann. § C.56:8-166.11.

[34] Nine of the twelve states have language stating that OOPS may not make use of a default setting but must reflect an affirmative, freely given and unambiguous consumer choice to opt out; CA, CO, and NJ are the only outliers.

[35] All twelve of the relevant states include language to this effect regarding OOPS being consumer friendly and easy to use by the average customer.

[36] All twelve of the relevant states include language to this effect regarding OOPS not unfairly disadvantageing another controller.

The current state patchwork does not provide for a consistent or centralized process to evaluate signaling mechanisms or their specific implementation across browsers, or to validate the deployment and administration of OOPS. State regulators also lack the resources to provide for fair and consistent use of OOPS.

Therefore, one of the biggest opportunities for a National Privacy Framework is to establish key criteria for the use of OOPS, and to authorize the Department of Commerce to establish a transparent and accountable process for evaluating OOPS implementation across browsers, platforms, and devices. This process would address the current regulatory gap across the states and ensure that OOPS are deployed effectively for users, but without creating market advantages for platform providers.

Data Minimization

Data minimization is a critical component of an effective National Privacy Framework, providing a core set of protections around consumer data. A well-scoped approach to data minimization should provide flexibility for processing personal data, maximize transparency for consumers, and avoid overly restrictive limits on processing like those adopted under the Maryland Online Data Privacy Act (MODPA).

Data processing restrictions should include the following:[37]

- Require the business to identify and disclose the data being collected and the purposes for which the data is processed;
- Allow for data processing in accordance with notice to consumers and consumers' expression of preferences;
- Provide rights to consumers to opt out of processing of their personal data for legally or similarly significant purposes; and
- Provide requirements for businesses to create policies to retain and process data for only as long as reasonably necessary to fulfill the purpose for which it was collected.

Processing restrictions should *not* include the following, as these are overly restrictive and lack sufficient data protection benefits to offset limits on beneficial uses:[38]

- Limit collection and processing of personal data to that required for providing a specific product or service requested by the consumer;[39]
- Enumerate a list of permitted purposes for processing;[40] or
- Overly restrict the use of sensitive personal data for revenue generating purposes like tailored advertising.[41]

Many of the state privacy laws incorporate this balance of data minimization principles. The Texas Data Privacy and Security Act, for example, requires that collection of personal data be "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to

[37] Many states incorporate the following requirements including Delaware (Del. Code Ann. tit. 6, § 12D-106(a)(1), (2)(2023)) and Virginia (§ 59.1-574(A)(1), (2)(2023)).

[38] The following restrictions were included in the draft American Privacy Rights Act and/or the current Maryland Online Data Privacy Act.

[39] Md. Code Ann., Com. Law § 14-4707(a)(8), (b)(1)(i); APRA page 41-42.

[40] Am. Priv. Rts. Act, H.R. 8818, 118th Cong. § 102(d).

[41] *Id.* § 102(b); *see also* Md. Code, Com. Law § 14-4707(a)(1)-(2) (limiting the collection or processing of SPI to what is strictly necessary to provide or maintain a specific product or service requested by the consumer AND prohibiting a controller from selling or sharing sensitive personal information regardless of consumer preference).

the consumer."[42] The Oregon Consumer Privacy Law also adopts this standard, requiring that companies disclose the purposes for processing personal data and limiting permissible collection to what is "[a]dequate, relevant and reasonably necessary to serve th[ose] purposes. . ."[43]

These state privacy laws supplement a balanced approach to data minimization with appropriate consumer controls over specific data processing activities – such as requiring consent for the processing of sensitive data[44] and allowing consumers to opt out of certain uses of their data.[45] This approach prevents blanket restrictions on how businesses can process data for important and beneficial purposes like improving their product or service or generating revenue from advertising, so long as the processing is proportionate to those purposes and consumers are given appropriate transparency and control over the processing.[46]

This approach contrasts the APRA approach to identify only a limited set of pre-ordained "permitted" purposes for which data processing is allowed and instead provides for strong consumer data protection without limiting valuable data processing, including future processing purposes that have not yet been enumerated through a cumbersome legislative process.[47] Both the APRA and MODPA create an ambiguous and potentially unreasonable standard by limiting processing to what is "reasonably necessary and proportionate" to "provide or maintain a specific product or service requested by the consumer to whom the data pertains," regardless of whether a consumer consents.[48] This approach may not allow for the provision of data-driven advertising functions such as tailored advertising or ad measurement and optimization, both of which are critical for monetizing digital media.

III. Existing Privacy Frameworks & Protections

A National Privacy Framework should apply in the following ways to existing privacy frameworks:

- preempt existing state privacy laws to provide a uniform standard that gives consumers across all states a clear and consistent set of protections, and provides business with a coherent legal environment that fuels innovation and U.S. economic growth;
- retain existing federal sectoral privacy laws that have for many years provided a framework for protecting Americans' sensitive information, including financial, health, eligibility, and children's data;
- exempt data processed by companies that are subject to regulation under these sectoral privacy laws.

[42] Tex. Bus. & Com. Code §§ 543.101(a)(1), 541.204(a)(2).
[43] Or. Rev. Stat. § 646A.578(1)(a)-(b).
[44] Tex. Bus. & Com. Code § 543.101(b)(1).
[45] *Id.* § 543.051(b)(5).
[46] Restrictions in the APRA raised concerns about businesses' inability to perform these tasks with personal data. *See* Centre for Information Policy Leadership, *Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploration of Potential Effects* 7-10 (Aug. 2024), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_data_minimization_us_privacy_landscape_aug24.pdf.
[47] *See generally* American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 102.
[48] Md. Code, Com. Law § 14-4707(b)(1)(i).

V. Artificial Intelligence

There is significant overlap between certain AI regulations and data privacy law, in that both maintain a core objective to protect consumers from harms resulting from the processing of their PI/SPI. However, recent approaches to regulate AI have been expansive and over-restricting, forcing regulators to explore paring back requirements.[49] As such, a federal consumer privacy law should refrain from including AI/Automating Decision Making Technologies (ADMT) requirements to avoid unnecessarily restricting businesses without any corresponding privacy protection. Optimally, requirements for transparency and control around AI should be crafted to align effectively with data privacy notices.

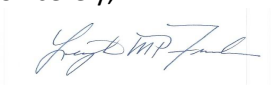
VI. Accountability & Enforcement

A National Privacy Framework should provide for joint and exclusive enforcement by the FTC and state attorneys general, and establish a safe harbor mechanism that provides a formal role for self-regulatory organizations to work cooperatively with federal and state regulators, with strong oversight and accountability mechanisms through the FTC. Effective self-regulation incentivizes and aids compliance and it minimizes the enforcement burden on regulators. A National Privacy Framework should therefore provide for FTC approved self-regulatory programs, under which companies in good standing should have a presumption of legal compliance.[50] This approach would be consistent with the framework established under COPPA, which has proven effective for more than two decades, providing for nearly 40 enforcement actions and widespread compliance administered by multiple recognized safe harbor providers.[51]

Conclusion

Again, thank you for the opportunity to provide input into this important process. If we can provide any additional information, or otherwise assist you during this process, please do not hesitate to contact me at leigh@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

Sincerely,



Leigh Freund
President & CEO
Network Advertising Initiative (NAI)

---

[49] California's proposed automated decision-making technology (ADMT) regulations present an example of overlapping transparency and control requirements that would result in businesses conducting tailored advertising to serve redundant and duplicative notices to consumers. *See generally* California Privacy Protection Agency Proposed Text, Cal. Code Regs. tit. 11 (proposed Nov. 22, 2024). In response to industry concerns and comments, the California Privacy Protection Agency (CPPA) moved to pare back controversial portions of its proposed ADMT regulations, including removing tailored advertising from its scope, during its board meeting held on April 4, 2025. *See* Yuan, Xu, *California Privacy Regulator to Remove Behavioral Advertising from AI Rules*, MLex (Apr. 4, 2025), https://www.mlex.com/mlex/data-privacy-security/articles/2321590/california-privacy-regulator-to-remove-behavioral-advertising-from-ai-rules.

[50] See SAFE Data Act, Sec. 403 regarding approved certification programs

[51] Federal Trade Commission, *Kids' Privacy (COPPA)*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa (last visited Apr. 4, 2025)