iab.

April 7, 2025

The Honorable Brett Guthrie
Chairman, House Committee on
Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Joyce
Vice Chairman, House Committee on
Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

RE: Privacy Working Group Request for Information

The Interactive Advertising Bureau, Inc. ("IAB") welcomes this opportunity to provide comments in response to the House Privacy Working Group's ("Working Group") Request for Information. IAB, along with its member companies, shares the Working Group's commitment to a national data privacy standard that protects Americans' rights online and maintains our global leadership in digital technologies.

Founded in 1996 and headquartered in New York City, IAB (www.iab.com) represents over 700 leading media companies, brand marketers, agencies, and technology companies that are responsible for selling, delivering, and optimizing digital advertising and marketing campaigns. Together, our members account for 86 percent of online advertising expenditures in the United States.

We believe that consumers can have the benefits of digital advertising while also having robust consumer privacy protections. American consumers recognize the value the value of an ad-supported internet:

- 80% of consumers agree that the free and open, ad-supported internet is important to democracy and free speech.[1]
- 80% also agree that websites/apps are free because of advertising.[2]
- 91% would react negatively if they had to start paying for the websites/apps they currently use for free.[3]

Consumers benefit from personal data used to tailor ads to their interests, prevent fraud, and to conduct measurement and analytics for the delivery of digital ads. Personal data also enables limits on how often a consumer sees the same ad. It also is critical to measurement and attribution of digital ads, without which no advertiser would purchase ad inventory.

[1] Interactive Advertising Bureau, *The Free and Open Ad-Supported Internet: Consumers, Content, and Assessing the Data Value Exchange* (Jan. 2024), https://www.iab.com/wp-content/uploads/2024/01/IAB-Consumer-Privacy-Report-January-2024.pdf.
[2] *Id.*
[3] *Id.*

Reasonable uses of data supporting data-driven advertising also ensure that companies of all sizes can meaningfully engage in the digital ecosystem, thereby promoting competition throughout the economy. This includes small businesses that rely on personal data to reach their audiences, compete with larger companies, and grow their customer bases on limited budgets. Data-driven advertising has helped to create thousands of new small, medium, and self-employed businesses across multiple sectors of the economy, maintain tens of millions of jobs across the nation in every congressional district, and deliver trillions of dollars in consumer value.[4]

We look forward to collaborating with the Working Group as it evaluates how to protect consumer privacy, maintain a free and open internet, and enhance competition.

I. Roles and Responsibilities

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?

A comprehensive federal privacy law must define the distinct roles and responsibilities of controllers, processors, third parties, and consumers. Any federal law should look to the 19 states' generally-applicable privacy laws, which delineate these concepts in similar terms.

We recognize and support the states' commonly defined roles under the state privacy laws, including (1) "controllers," who alone or jointly with others, determine the purpose and means of processing personal data,[5] (2) "processors," who process personal data on behalf of a controller,[6] (3) "third parties," who are not consumers, controllers, or processors, (or their affiliates),[7] and (4) "consumers," who are U.S. residents of the United States and acting in a household capacity (and not include an individual acting in a commercial, or employment, or independent contractor context).[8]

B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

Controllers should be obligated to provide meaningful privacy disclosures, practice reasonable and appropriate data minimization, avoid undisclosed or unexpected secondary uses of personal data, maintain oversight of their service providers, maintain data inventories, effectuate consumer privacy rights, and enter into contracts with processors and third parties containing privacy protective provisions.

[4] John Deighton & Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, Interactive Advertising Bureau (Oct. 2021), https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf.
[5] *See, e.g.,* Va. Code Ann.§ 59.1-575; Conn. Gen. Stat. § 42-515(11).
[6] *See, e.g.,* Va. Code Ann.§ 59.1-575; Conn. Gen. Stat. § 42-515(29).
[7] *See, e.g.,* Va. Code Ann.§ 59.1-575; Conn. Gen. Stat. § 42-515(40).
[8] *See, e.g.,* Va. Code Ann.§ 59.1-575; Conn. Gen. Stat. § 42-515(7).

Processors should be required to process data in accordance with to the controller's instructions and not process personal data for their own commercial purposes; provided, however, they use such personal data for clearly articulated business purposes that appear in state privacy laws, such as market research,[9] and be obligated to assist controllers with their compliance obligations for information in the processor's control.

A federal law should avoid overly restrictive requirements relating to the controller processor relationship. One notable outlier among processor provisions is included in the *California Consumer Privacy Act*, is the prohibition against combining personal data in certain contexts and engaging in cross-context behavioral advertising.[10] This provision is absent from other state privacy laws, and should not be included in a federal privacy law because it would discourage parties to leverage processor relationships.[11]

Third parties, who can also become data controllers of personal data they receive, should be required to meet contractual privacy obligations, data security obligations, and reasonable data usage limitations.

All parties should be required to conduct risk-based privacy diligence of the partners from whom they receive personal data and to whom they disclose personal data, as well as privacy risk assessments.

C. Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?

Such a law should exempt from coverage small businesses with annual revenues under $25 million and not-for-profit organizations[12] because they uniquely benefit from targeted advertising as an efficient and cost-effective means of conducting product discovery. Without an exemption, they will face disproportionate harm to their organizations. In 2019, California's Department of Finance estimated that companies with fewer than 20 employees would have to spend roughly $50,000 in initial costs to become compliant with the *California Consumer Privacy Act*. Such costs should be borne by medium and large-sized companies rather than small businesses and

[9] Such purposes generally include auditing, security, and fraud prevention, deduplication, bot identification, short-term, transient internal use, performing services such as maintaining accounts, providing customer service, and fulfilling orders, debugging and error resolution, research and development, quality and safety maintenance, and to improve the relevant product or service. Cal. Civ. Code § 1798.105(d).

[10] California's privacy laws define "business" and "service provider" differently from the controller-processor framework used by other states, with stricter regulations on data processing activities by service providers. This distinction complicates compliance, as businesses can process data in ways their service providers cannot. Cal. Code Regs. tit. 11, § 7051.

[11] Processor relationships establish clear accountability to the controller's instructions through contractual obligations. Coupling this framework with opt-in requirements further enhances consumer protection, as it ensures consumers provide informed consent for data processing activity.

[12] Both the size threshold and exemption are consistent with a number of state privacy laws. *See, e.g.,* Cal. Civ. Code §§ 1798.100–1798.199, Va. Code Ann. §§ 59.1-571–59.1-581, Colo. Rev. Stat. § 6-1-1301, Utah Code Ann. § 13-61-101, Conn. Gen. Stat. § 42-471.

not-for-profit organizations for whom the cost of compliance is substantial (e.g., privacy technology vendors, engineering, and legal counsel).

II. Personal Data, Transparency, and Consumer Rights

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

Clearly defining "personal," "de-identified," "pseudonymized," and "sensitive" information in a federal privacy law will protect privacy, support a free and open internet, respect consumer preferences, and drive innovation.

State privacy laws provide a model for defining "personal data," which means collected or inferred information linked or reasonably linkable to an individual or device.[13] A federal privacy law should uniformly account for common carve-outs, such as "de-identified data,"[14] "publicly available information,"[15] and information protected by the First Amendment.[16]

Many state privacy laws generally recognize that "pseudonymized data" remains personal data,[17] although certain inconsistencies exist in a few states that exempt such data from various privacy obligations.[18] A federal privacy law should recognize that pseudonymized data ais personal data subject to consumer privacy choices—such as the right to opt-out of targeted advertising. Additionally, because pseudonymization is sometimes achieved through privacy-enhancing technologies, a federal privacy law should incentivize their adoption to support reasonable data minimization, security, reasonable purpose limitation, and accountability.

See Section II.D below for our discussion of "sensitive personal data."

B. What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?

Disclosure obligations should ensure consumers are provided with comprehensive notice at collection that is meaningful and accessible, and that accounts for the dynamic nature of the digital advertising industry, where third parties can change rapidly—sometimes within milliseconds—depending on which party wins a real-time ad placement bid (e.g., requiring

[13] *See, e.g.,* Va. Code Ann.§ 59.1-575; Conn. Gen. Stat. § 42-515(26).

[14] For instance, "de-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. *See, e.g.,* Va. Code Ann.§ 59.1-575.

[15] For instance, publicly available information means any of the following: (a). Information that is lawfully made available through federal, state, or local government records, and (b). Information that a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public through widely distributed media. Del. Code tit. 6 § 12D-102.

[16] *See, e.g.,* Cal. Civ. Code § 1798.145(l); Colo. Rev. Stat. § 6-1-1304(3)(d).

[17] *See, e.g.*, Conn. Gen. Stat. § 42-515(32); Del. Code tit. § 12D-102(27).

[18] *See, e.g.,* Iowa Code § 715D.1(23); Neb. Rev. Stat. § 87-1102(27); Va. Code § 59.1-575.

disclosure of categories of third parties is more reasonable than naming specific entities as a way to meaningfully inform consumers).[19]

Consumers should receive clear and comprehensive disclosures regarding the collection, processing, and transfer of their personal data, especially sensitive data. Disclosures should specify the purpose and methods of collection, categories of data collected, and data processing activities accurately, plainly describe how data is processed, and provide the categories of third parties with whom the data is shared. Companies should also clearly disclose consumer privacy rights and how to exercise them. For sensitive personal data, disclosure restrictions should be more stringent. Notices must be clear, conspicuous, understandable, and prominently placed.

C. Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?

Balancing consumers' privacy expectations and interests in relevant ads is crucial when designing a federal privacy law. Companies should be obligated to provide a robust set of consumer rights and protections.

Further to the 19 state privacy laws, providing consumers with the right to opt-out of the "sale" of their personal data and targeted advertising across non-affiliated digital properties is fundamental, except where sensitive personal data is involved, in which case an opt-in should apply.[20] We also support the right of a consumer to access, delete, and correct personal data, subject to appropriate exemptions under existing state privacy laws.[21]

Companies also should have certain obligations to protect consumer privacy regardless of whether any consumer exercises a privacy right. Companies should undertake reasonable data minimization, which includes limiting the *collection* of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.[22] Likewise, controllers should only *process* the personal data where doing so is reasonably necessary to and compatible with the disclosed purposes for which such personal data is processed[23] and consistent with the consumer's reasonable expectations.[24] For example, when a digital publisher discloses to the consumer that it collects, processes, and discloses the consumer's personal data to enable targeted advertising (a core part of the value

[19] *See, e.g.*, Or. Rev. Stat. § 646A.578(4)(e); Minn. Stat. § 325M.16, subdiv. 1(5).

[20] It should be clear, however, that such opt-outs do not extend to essential, low-risk functions integral to supporting the ad-funded digital ecosystem, like contextual advertising (serving ads based on page content) or basic advertising measurement necessary for reporting, auditing, and fraud prevention

[21] *See, e.g.,* Va. Code Ann. §§ 59.1-576(C) (sectoral laws), Colo. Rev. Stat. § 6-1-1304(g) (de-identified data).

[22] *See, e.g.,* Colo. Rev. Stat. § 6-1-1308(3); Tenn. Code Ann § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1).

[23] *See, e.g.,* Colo. Rev. Stat. § 6-1-1308(4); Tenn. Code Ann § 47-18-3204(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1).

[24] *See* Cal. Code Regs. tit. 11, § 7002(b)

exchange for free or discounted content or as part of a brand loyalty program), such purpose should be *per se* reasonable.

Also fundamental to consumer privacy is controllers' obligation to conduct data protection assessments for processing activities that present a heightened risk of harm.[25] Likewise, to incentivize compliance, all parties should conduct risk-based privacy diligence of those from whom they receive personal data and to whom they disclose personal data,[26]and if so, have an exculpation from liability for partner wrongdoing relating to personal data disclosed.[27]

D. What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

Protecting "sensitive personal data" is critical, necessitating legal clarity and consistency for businesses to properly protect consumers. Currently, state privacy laws differ in what categories are deemed sensitive, they generally include an opt-in standard, and do not sufficiently account for context. For example, most state privacy laws include ethnicity as a sensitive data category. Of course, significant harm could result from using such data to make important eligibility decisions, but many consumer foods and packaged goods are directed to the preferences of specific ethnic populations. Imposing opt-in requirements to market to such groups makes it difficult for these companies to efficiently reach prospective customers (and for such customers to benefit from such information) and outweighs the minimal potential for harm.[28] Given these complexities, a blanket approach to sensitive data categories can have unintended consequences. For this reason, a federal privacy law should provide clearly-defined terms that carefully delineate when opt-in consent is required for certain categories and/or uses of sensitive data. Overly broad definitions of sensitive data could lead to consumer consent fatigue and hinder the ability for businesses to deliver relevant services, while also creating unnecessary barriers for legitimate processing activities.

[25] *See, e.g.,* Del. Code tit. § 12D-108(a); Interactive Advertising Bureau, *Data Protection Assessment Template* (Feb. 2025), https://www.iab.com/wp-content/uploads/2025/02/IAB_Data_Protection_Assessment_-February_2025.pdf.

[26] The obligation to conduct diligence under state privacy laws is frequently embedded in contractual requirements. *See, e.g.,* Del. Code tit. 6 § 12D-107(b)(5) (requires controllers to mandate their Service Provider to allow for reasonable assessments); Cal. Code Regs. tit. 11, § 7002(a)(4).

[27] *See, e.g.,* Cal. Code Regs. tit. 11, § 7002(b).

[28] For example, privacy enhancing technologies, which uses pseudonymized personal information, enables advertisers and regulators to confirm that data handling aligns with privacy standards, thus fostering a competitive and trustworthy digital advertising environment.

III. Existing Privacy Frameworks & Protections

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

Subject to our comments in Section B below, federal privacy law should be informed by the prevailing state models that focus on pragmatic, principled, and risk-based requirements, which benefits both consumers and the digital advertising industry, fostering consumer trust and industry innovation. Examples include: (1) role-based obligations that align with entities' roles as controllers, processors, or third parties; (2) preserving first-party advertising, marketing, and content personalization that allow businesses to enhance their direct relationships with consumers; (3) opt-out regime for sale and targeted advertising across non-affiliated digital properties that prioritizes consumer choice without unnecessary barriers; (4) legally-mandated contractual provisions that provide clear accountability between parties; (5) reasonable data minimization that allows legitimate business uses while respecting reasonable consumer expectations; (6) risk-based differentiating obligations based on data sensitivity, with clear definitions for sensitive personal data; and (7) preserving reasonable uses of third-party data for digital advertising purposes. Consumers and industry can further benefit from choice options that are clear, understandable, and simple to use as consumers may not fully understand the full scope of "sale" or what "targeted advertising" means.

It is also crucial that any comprehensive privacy law incorporate exemptions to enable critical business and operational functions such as preventing and responding to security incidents, protecting against fraud or other illegal activity, and complying with legal obligations.

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

State privacy laws are generally consistent regarding the right to opt out of the sale of personal data and targeted advertising and to access, delete, and correct personal data. The obligations of controllers, processors, and third parties are also generally the same. Most of the digital advertising industry successfully addresses the different state privacy law nuances by applying a highest standard approach to requirements.[29] More than 1,300 companies achieve this through the IAB Multi-State Privacy Agreement, which creates a standard set of privacy terms by finding the highest common denominator across the state privacy laws and applies to digital advertising transactions amongst the signatories.[30]

[29] Interactive Advertising Bureau, *IAB State Privacy Law Survey Results* 16 (Aug. 2023), https://www.iab.com/wp-content/uploads/2023/08/IAB-State-Privacy-Law-Survey-August-2023_FINAL.pdf.

[30] *See* www.iabprivacy.com

However, state laws vary, for example, regarding data minimization. Many states limit collection to what is "adequate, relevant, and reasonably necessary" related to a disclosed or specified purpose.[31] Most states follow this data minimization standard, striking a thoughtful balance between consumer privacy and business needs. By contrast, Maryland prohibits the collection of personal information to "what is necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains."[32] Maryland also prohibits sensitive data collection unless it is "strictly necessary" to provide or maintain a specific product or service, thereby prohibiting the consumer from even providing consent for other uses and limiting personal information processing when the entity "should have known" that the user is a minor (an unclear, difficult-to-meet standard).[33] This Maryland approach is suboptimal due to its overly restrictive constraints and, as such, should not be incorporated into a federal privacy law.

Additionally, businesses face significant burdens deciphering the differences in the categories and lack of precision in the state privacy laws around when personal data is sensitive, including, for example, determining which data elements constitute health data, including when creating audience segments. Reviewing thousands of data elements without regulatory clarity is inefficient and regulatory confusion does not advance privacy.

Separate from state privacy and breach notification laws, more than half of U.S. states have laws requiring security for personal information.[34] These laws vary in terms of applicability, required security measures, enforcement mechanisms, and other key elements. Variations in state data security laws create unnecessary and costly compliance burdens that benefit neither businesses nor consumers. A preemptive federal privacy law should provide a uniform framework for data security that streamlines compliance and provides consumers with consistent protections.

C. Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?

To provide U.S. consumers with equal privacy protection, and to ensure legal consistency and business certainty, a comprehensive federal privacy law should fully preempt all state privacy laws related to data privacy and security.

[31] *See, e.g.,* Colo. Rev. Stat. § 6-1-1308(3); Conn. Gen. Stat. § 42-520(a)(2).

[32] Md. Code Ann. Comm. Law § 14-4606(B)(1).

[33] *Id.* at § 1404607(A)(1).

[34] *See* National Conference of State Legislatures, Data Security Laws, https://www.ncsl.org/technology-and-communication/data-security-laws-private-sector.

D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?

A comprehensive federal privacy law should minimize duplication overall. Certain federal sectoral laws should be preserved to avoid redundancy and ensure consistent consumer protection. If a company collects personal data not already regulated by HIPAA, FCRA, GLBA, and COPPA, the company would need to comply with the new federal privacy law. With respect to state sectoral laws, the federal law should also fully preempt those laws. Without preemption, a sue and settle environment that already exists is likely to expand, forcing small businesses to spend resources defending claims rather than focusing on creating quality content and improving products and services for consumers.

IV. Data Security

A. How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?

A comprehensive privacy law should require companies to implement a risk-based security program to protect personal information. Because organizations' risk profiles and network deployments may vary, the comprehensive privacy law should outline broad categories of security processes but not be prescriptive. The comprehensive privacy law should require risk assessments, access controls, regular testing and evaluation, employee training, and incident response and notification. The law should also encourage adopting data protection technologies such as encryption by creating safe harbors regarding notification and reporting. Within these broad categories, the specific security controls should be designed to manage the risks identified in the risk assessment, including financial loss, identity theft and significant harm (e.g., social security numbers or credit card data) and aligned with generally-accepted cybersecurity risk management frameworks like the National Institute of Standards and Technology's Cybersecurity Framework.

V. Artificial Intelligence

A. How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?

AI is critical to U.S. innovation and competitiveness. A federal privacy law should facilitate responsible AI development, ensuring regulations support advancements within digital advertising and beyond. A balanced approach is needed, applying privacy safeguards proportional to risks while also considering the benefits of AI innovation.

A comprehensive federal privacy law should account for the use of algorithms, machine learning, artificial intelligence, predictive analytics, or other automated methods by requiring companies to evaluate relevant risks. Requirements on automated processing and decision-making should focus on activities that produce legal or similarly significant effects for consumers, aligned with state laws. These provisions should be tech-neutral and facilitate data processing, including with artificial intelligence, require ongoing monitoring, evaluation of evolving algorithmic systems, and assess the cumulative impact of artificial intelligence systems. Additionally, a federal privacy law should fully preempt state automated decision making technology laws and provisions to establish a consistent, unified regulatory framework, ensuring clarity and uniformity in the U.S.

VI. Accountability & Enforcement

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

The Federal Trade Commission and state Attorneys General should have sole enforcement authority of a federal comprehensive privacy law. These state and federal entities possess specialized knowledge, expertise, and deep understanding of data practices to protect consumers effectively. Their authority would allow for consistent and uniform application of the law across industries and jurisdictions, reducing conflicting interpretations and streamlining business compliance.

In addition, the law should specifically note that nothing in the law should be construed to allow for a private right of action, because including one is likely to lead to a flood of frivolous lawsuits, which would disproportionately burden businesses and potentially undermine the goal of protecting consumer privacy. The law also should offer businesses a reasonable cure period so they can make a bona fide effort to rectify compliance issues before facing enforcement actions, promoting fairness and encouraging proactive compliance.

B. What expertise, legal authorities, and resources are available—or should be made available—to the Federal Trade Commission and state Attorneys General for enforcing such a law?

With rapid changes in technology and business practices, the Federal Trade Commission should be provided with robust resources for attorneys and technologists with a strong understanding of complicated digital advertising architectures.

C. How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?

Companies that conduct adequate privacy diligence of their partners should be exculpated from liability for partner wrongdoing relating to the personal data they disclose or receive. A federal privacy law also should recognize businesses’ use of existing data security standards and frameworks to meet the new requirements through the inclusion of an affirmative defense.

* * *

IAB thanks the House Privacy Working Group for considering these recommendations and looks forward to working closely with the Working Group and the House Committee on Energy and Commerce on federal comprehensive privacy legislation.

Respectfully Submitted,

/s/ Michael Hahn

Michael Hahn
Executive Vice President & General Counsel
Interactive Advertising Bureau, Inc.
116 E. 27th Street, 7th Floor
New York, New York 10016
michael.hahn@iab.com
(212) 380-4700