April 7, 2025

Via Electronic Mail

The Honorable Brett Guthrie, Chairman
The Honorable John Joyce, Vice Chairman
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515
PrivacyWorkingGroup@mail.house.gov

Re: Privacy Working Group Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce:

The Entertainment Software Association ("ESA") welcomes the opportunity to provide comments in response to the Privacy Working Group's ("Working Group") Request for Information ("RFI") issued by the U.S. House of Representatives Committee on Energy and Commerce. ESA is the U.S. trade association for the video game industry; our members are the innovators, creators, publishers, and business leaders reimagining entertainment and transforming how America plays video games on consoles, handheld devices, and personal computers.

The video game industry is a key economic sector that contributes over $100 billion to the U.S. economy. Three out of four U.S. households have at least one gamer in their home. Our industry creates jobs in every state with over 250,000 jobs across over 5,000 video game company locations in the U.S.[1]

In addition to being major contributors to the U.S. economy, ESA member companies are also leaders in protecting consumers' personal information, while continuing to innovate and transform online experiences. ESA and its members respectfully request that a carefully tailored federal privacy framework, which has the potential to protect consumers and support further growth and innovation in our industry, include the following features:

- Strong preemption of state laws to ensure businesses are not subject to a state patchwork of privacy regimes, which will enable companies to efficiently align their compliance strategies across the country;

- Enforcement by federal regulators rather than private plaintiffs, which would provide certainty and avoid piecemeal, potentially conflicting, litigation across plaintiffs and the courts;

- Explicit language allowing businesses to protect themselves and their users against fraud, cheating, and other malicious conduct;

- Flexible standards to assess risk and conduct cybersecurity audits to enable businesses to protect against the unauthorized disclosure of sensitive information and unduly burdensome paperwork;

[1] Entertainment Software Association, *Impact of the Video Game Industry*, https://www.theesa.com/state-impact-map/.

- Opportunities to offer consumer products through "free-to-use" business models that employ the transparent collection and processing of users' data;

- No inclusion of vague and potentially constitutionally problematic concepts that censor speech, like so-called "dark patterns" which attempt to restrict how businesses communicate with their users;

- Require consumers to submit data subject requests directly to the business with which a consumer has a direct relationship; and

- Narrowing obligations for "automated decision-making technology" ("ADMT") to only decisions that produce certain clearly defined legal or similarly significant effects to facilitate the growth of AI technologies in the US and respect intellectual property rights.

Each of these points are discussed further below.

* * *

I. ANY FEDERAL PRIVACY FRAMEWORK SHOULD BROADLY PREEMPT STATE PRIVACY LAWS.

A federal privacy framework should broadly preempt state laws that regulate personal data, including state laws regulating ADMT and AI. Unfortunately, today's patchwork of state privacy laws, many of which conflict with one another or present small but material variations on rights and duties, makes it difficult for consumers to understand which protections extend to their data. It is also burdensome for businesses that must continually identify and resolve conflicts across the different jurisdictions. Similarly, state ADMT and AI laws vary significantly state-by-state, chilling innovation and undermining American leadership in AI. Including state preemption in a federal privacy framework would alleviate this confusion by establishing a uniform set of consumer rights and business obligations nationwide.[2]

In addition, when establishing this national framework, Congress should also address other state laws that seek to regulate the privacy of personal data. In today's privacy landscape, conflicts between comprehensive privacy laws and other more specific state privacy laws are creating widespread confusion. For example, even though the California Consumer Privacy Act ("CCPA") provides California residents with mechanisms to opt out of certain types of online advertising and prohibits a private right of action, plaintiffs have been pursuing litigation against businesses that engage in CCPA-compliant advertising by weaponizing a state privacy statute enacted in 1967 to address wiretapping of telephone lines.[3] A broad nationwide privacy standard that eliminates these potential conflicts will promote privacy across the country and provide consistency so companies can deliver important privacy protections to all consumers.

A broad federal privacy framework will also provide much needed clarity with respect to children and teens personal data. With the proliferation of state minor protection laws, many of which have been challenged and enjoined by the courts, businesses lack certainty of the requirements when processing data from these consumers. A federal privacy framework should cover personal data from children and teens, with parents remaining in control over the processing of personal data from children under the age of 13.

---

[2] *See, e.g.*, 15 U.S.C. § 6821 *et seq.*; 15 USC § 1681 *et seq.* Notably, federal law already addresses wiretapping and eavesdropping. *See* 18 U.S.C. § 2511.

[3] *See, e.g.*, *Zarif v. Hwareh.com, Inc.*, No. 23-CV-0565-BAS-DEB, 2025 WL 486317, at *14 (S.D. Cal. Feb. 13, 2025).

Consistent with the comprehensive state privacy laws, businesses should obtain opt-in consent from teens when processing their personal data for certain purposes.

II. A FEDERAL PRIVACY FRAMEWORK SHOULD BE ENFORCED BY FEDERAL REGULATORS, NOT A PRIVATE RIGHT OF ACTION.

It is critical that a federal privacy framework is enforced by expert federal regulators that have a broad view of the issues affecting consumers, not through a private right of action. A private right of action would incentivize nuisance lawsuits that do not address consumer harms or result in any consumer benefit. For example, the Video Privacy Protection Act ("VPPA"), a 1988 statute enacted to protect the privacy of video tape rental history, has been used to file frivolous lawsuits against companies that use widespread Internet technologies, such as cookies and search technologies, to provide requested services to consumers. Indeed, an expansive interpretation of the VPPA is at issue in a pending petition for a writ of *certiorari* in *Salazar v. National Basketball Association*. *See Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533 (2d Cir. 2024). Accordingly, to protect American businesses and consumers from frivolous litigation and promote application of consistent regulatory standards, any federal privacy framework should prohibit an individual from enforcing the federal privacy framework or the VPPA. Businesses and consumers must be provided with clear guidance as to their rights and responsibilities under a federal privacy framework. This guidance should take the form of policy statements and explanations from expert regulators, who are well-positioned to develop coherent enforcement strategies and provide notice of their interpretations of privacy requirements to regulated parties. As the Federal Trade Commission ("FTC") has long done in the Children's Online Privacy Protection Act ("COPPA") context, publishing "FAQs," policy statements, and other materials to provide industry guidance will help businesses develop consistent and reliable compliance strategies that protect consumers.[4] By contrast, a private right of action would essentially put questions of interpretation in the hands of plaintiffs' lawyers, who frequently focus on allegations, not consumer harms, to pressure businesses into monetary settlements.

Allowing plaintiffs' law firms to shape regulations through widespread litigation often results in unexpected and extreme outcomes unintended by the legislature. For example, plaintiffs pushed for an aggressive interpretation under the Illinois Biometric Information Privacy Act ("BIPA") that statutory damages should accrue each time a person's biometric identifier or information is transmitted without prior informed consent, and not just once for when the identifier is collected. In ruling in favor of the plaintiffs, the Illinois Supreme Court recognized that this interpretation could result in the "financial destruction of a business." *Cothron v. White Castle*, 216 N.E.3d 918, 926 (Ill. 2023). This required the Illinois legislature to amend BIPA to override the *White Castle* decision and limit the circumstances in which damages could be imposed.

III. ANY FEDERAL PRIVACY FRAMEWORK SHOULD ENABLE BUSINESSES TO PROTECT THEMSELVES AND THEIR USERS FROM FRAUD AND SECURITY THREATS.

In the video game industry, preventing fraud and cheating is essential to ensure a fair and enjoyable experience for users. U.S. state privacy laws have consistently included security and fraud exceptions to transparency requirements, consumer rights, and other obligations.[5] Similarly, in developing a federal privacy framework, congressional lawmakers should consider how bad actors might abuse rights and duties intended to protect consumers' privacy. Such abuses should be avoided through

[4] FTC, Complying with COPPA: FAQ, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[5] *See, e.g.*, Tex. Bus. & Com. Code § 541.201(a)(6); Fla. Stat. § 501.716(1)(f); Va. Code 53 § 59.1-582(A)(7); Colo. Rev. Stat. § 6-1-1304(3)(a)(X).

exceptions that preserve businesses' ability to maintain the security and integrity of their products and services, ensure user safety, and safeguard intellectual property and trade secrets.

For example, a federal privacy framework should not require businesses to disclose information or honor rights requests that would jeopardize the privacy or security of the business or any person. This includes compliance with requirements that would preclude a company from efficiently preventing, detecting, and defending against harmful, illegal, and inappropriate conduct like cheating or toxic behavior. To illustrate, a video game company might need to withhold information, or refuse to honor a consumer's request to delete their data, in order to investigate and prevent financial fraud or grooming or to prevent bad actors from reverse-engineering systems. Similarly, businesses should be permitted to share personal data with third parties to investigate patterns of fraudulent conduct (*e.g.*, to identify that several account takeovers across online gaming platforms are originating from a single IP address).

Additionally, any federal privacy framework should ensure that processing undertaken to implement online safety and security features is immunized from liability under state privacy laws and non-sectoral federal privacy laws. For example, when a business processes data to identify and stop credit card scammers per a federal law, it should not have to worry about liability under a state wiretapping statute.

IV. ANY RISK ASSESSMENT OR CYBERSECURITY AUDIT REQUIREMENTS UNDER A FEDERAL PRIVACY FRAMEWORK SHOULD BE REASONABLE, FLEXIBLE AND SATISFIED BY AN INTERNAL AUDIT.

A federal privacy framework should require businesses to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

This may require businesses to perform data security and cybersecurity audits to identify the appropriate data security measures that should apply to their collection, processing, and sharing of personal data. However, any audit requirement for these purposes should be satisfied by an internal audit rather than an external, third-party audit. Moreover, any audit requirement should be designed to avoid duplication of efforts, protect sensitive information, and avoid making confidential audit materials and results available in a manner that risks this information falling into the wrong hands. Specifically, an existing audit that is reasonably similar in scope and effect to the audit required by a federal privacy framework should satisfy the audit requirement. For example, a federal framework should recognize audits based on (i) the Information Security Management System ("ISMS") family of standards as published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC"), also known as the ISO/IEC 27000 series; (ii) the National Institute of Security Technology ("NIST") Cybersecurity Framework, or (iii) other sector-specific substantially equivalent standards. In addition, audits should be treated as confidential and proprietary information exempt from disclosure under the public records laws, and businesses should be permitted to exclude from audits information that could be misused by bad actors if made public or inadvertently released to unauthorized persons (*e.g.*, sensitive details about fraud detection systems).

Some state privacy laws require businesses to conduct "risk assessments" prior to engaging in certain processing. Similarly, a federal privacy framework should only require a risk assessment, where processing poses a significant risk to consumers' privacy and security, applicable only to activities in place after the effective date of the federal privacy framework.[6] Since, like cybersecurity audits, risk

[6] *See, e.g.*, Tex. Bus. & Comm. Code § 541.105(a); Ky. Rev. Stat. Ann. § 367.3621; Conn. Gen. Stat. § 42-522(a).

assessments are likely to contain highly sensitive and confidential information, businesses should not be required to disclose them publicly and they should be shielded from public records laws.[7] Additionally, businesses should be permitted to rely on existing risk assessments that are reasonably similar in scope and content to any assessment required under a federal privacy framework, and should only be required to update their assessments when there is a material change to the risks associated with a product or service.

Importantly, any cybersecurity audit or risk assessment requirements should not involve regular submission of materials to a regulator or any other party. Routine submission of such materials would be extremely burdensome on the government entities that must bear costs to review, maintain, and keep secure these documents. It also would likely raise significant legal concerns under the Paperwork Reduction Act.[8] Moreover, routine submission requirements would create novel commercial and national security risks by generating a repository of non-public security documentation covering a vast range of American businesses.

Finally, no cybersecurity audit or privacy assessment provision should be based on the business's size. Smaller organizations can present significant risks if, for example, they process sensitive personal data. Accordingly, risk thresholds for triggering these reviews should be based on the nature of the data and risks to consumers.

V. ANY FEDERAL PRIVACY FRAMEWORK SHOULD ENABLE FREE-TO-USE BUSINESS MODELS WITH APPROPRIATE DISCLOSURES.

ESA members recognize the value of data minimization. Our members strive to minimize data processing where doing so is compatible with the purpose of the service, particularly where sensitive personal data is at issue. However, too strict of a data minimization standard will inhibit companies' efforts to improve security, impede game development, and deprive consumers' choice for features and functionalities that they enjoy. Businesses should have flexibility to determine which data is required to provide a product or service, so long as they make their collection and use of personal data transparent to consumers.[9]

Notably, overly strict data minimization standards would limit opportunities for game development and improvement, particularly for new entrants to the market. For example, for some game developers that offer free or discounted versions of their games, it would not be feasible to offer these free and discounted versions without the collection of data for activities such as advertising. If the data minimization rules foreclose such offerings, developers might struggle to support their paid alternatives. This struggle might be particularly acute for new entrants to the market, who might find it difficult to convince consumers to pay to use their new products. Ultimately, this would result in consumers having diminished content. An overly strict data minimization standard might also deprive consumers of the choice to engage with personalized and dynamic experiences in video games – experiences that our members provide and that delight consumers.

By the same token, many U.S. state privacy laws permit a business to require users to provide certain data as a condition of providing the product or service, including where a consumer opts out of the collection or processing of that data.[10] A federal privacy framework should clarify that businesses may

[7] *See, e.g.*, Tex. Bus. & Comm. Code § 541.105(d); Ky. Rev. Stat. Ann. § 367.3621; Conn. Gen. Stat. § 42-522(c).
[8] 44 U.S.C. §§ 3501-3521.
[9] Tex. Bus. & Com. Code § 541.101(b)(1); Fla. Stat. § 501.71(1)(a); Ky. Rev. Stat. Ann. § 367.3621.
[10] Tex. Bus. & Com. Code § 541.201(a)(6); Fla. Stat. § 501.716(1)(f); Ky. Rev. Stat. Ann. § 367.3617.

elect to not make certain products or services available to consumers where they do not have access to necessary data.

VI. ANY FEDERAL PRIVACY FRAMEWORK SHOULD AVOID CENSORSHIP OF FREE SPEECH.

ESA and its members are committed to ensuring that consumers can make informed decisions regarding the privacy of their personal information, and business conduct that rises to the level of being deceptive or unfair will continue to be unlawful under current law.[11] Under the Biden Administration, however, the FTC and a few states pursued an aggressive agenda against vaguely defined "dark patterns."[12] Such dark pattern prohibitions cause confusing overlap with existing fraud law, are arbitrary, and substitute reasonable business judgement with paternalistic government overreach.

For example, an FTC report published in 2022 included as potential examples of "dark patterns" interface designs that are commonplace across industries, including video games, and that have countervailing consumer benefits. This report suggested that "requiring consumers to buy things with virtual currency" or "making the free version of a game so cumbersome and labor-intensive that the player is induced to unlock new features with in-app purchases" could constitute dark patterns.[13] However, consumers appreciate these features and the flexibility to play their games and make purchases in different ways online. A paternalistic ban on these innovative game features therefore would have the counterintuitive effect of making game play less enjoyable and convenient for players.

To avoid arbitrary application of the vague "dark pattern" definition, businesses may be discouraged from building interactive interfaces or avoid communicating with their users in ways that are informed by and tailored to those users' interests and preferences.[14] Thus, restrictions on dark patterns may force businesses to self-censor and use only that language and formatting that is the most unobjectionable or that is statutorily prescribed. Suppressing businesses' speech in this manner is unconstitutionally vague and cannot survive First Amendment scrutiny.

VII. A FEDERAL PRIVACY FRAMEWORK SHOULD IMPOSE REQUIREMENTS BASED ON THE DIFFERENT ROLES PLAYED BY BUSINESSES.

Like every U.S. state privacy law, a federal privacy framework should allocate certain duties to "controllers" who determine the means and purposes of processing, and others to "processors" who carry out processing on behalf of and under the instructions of a controller.[15] A federal privacy framework should clearly set out the responsibilities that apply to each type of entity, and confirm that each entity is responsible for its own compliance. For example, controllers should not be responsible for regulating the processors with whom they engage in transactions. This approach provides businesses clear standards by which to operationalize their compliance.

---

[11] *See* 15 U.S.C. § 45.

[12] Cal. Civ. Code §1798.140(l).

[13] FTC, Bringing Dark Patterns to Light at 23-25 (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

[14] *Reno v. Am. C.L. Union*, 521 U.S. 844, 872 (1997) ("The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech.").

[15] *See, e.g.*, Tex. Bus. & Comm. Code § 541.001(8); Ky. Rev. Stat. Ann. § 367.3611(8); Fla. Stat. § 501.702(9)(a).

In particular, any consumer rights requests included in a federal privacy framework should be handled by the controller. This approach makes sense because the controller is the the entity with whom the consumer has a direct relationship. Given that different controllers may have different sources of information available to them, each controller should be responsible for verifying the accuracy of any correction rights request, and a controller should not be required to pass along such requests.

VIII. ANY REQUIREMENTS FOR AUTOMATED DECISION-MAKING TECHNOLOGY SHOULD APPLY ONLY TO DECISIONS THAT MEET SPECIFIED STANDARDS.

ESA and its members have been at the forefront of using innovative technologies to protect their users and promote positive gameplay and player safety. For example, automated technologies can help detect and prevent security incidents, cheating, fraud, harassment, bullying, and other unlawful or malicious activity. Any federal privacy framework should permit and incentivize ESA members to continue this critical work, which has overwhelming benefits for consumers. Accordingly, any requirements imposed on ADMT in a federal privacy framework should only apply to solely automated decisions that produce legal or other similarly significant effects. A federal privacy framework should also preempt any ADMT requirements in state comprehensive privacy statutes or other state laws.

This approach would align with enacted U.S. state privacy laws, which almost uniformly adopt a categorical "solely automated" standard in determining the applicability of ADMT requirements and only apply to decisions that produce "legal or other similarly significant effects."[16] If a human is involved in producing or reviewing a decision, that decision is not "solely automated" and should not be subject to any ADMT restrictions. Furthermore, any restrictions or requirements on ADMT – like consumer access or deletion rights – should be subject to exceptions that reflect the nature of ADMT systems. For example, deletion rights should not be understood to require businesses to retrospectively remove an individual's lawfully acquired personal data from ADMT that has previously been trained on that data, which may be technically impossible.

* * *

ESA appreciates the opportunity to share its insights and suggestions with the Privacy Working Group and is committed to protecting consumers' personal information. ESA welcomes the opportunity to work with your staff on this important issue. Please do not hesitate to contact John Miceli at jmiceli@theesa.com with any questions.

[16] *See, e.g.*, Tex. Bus. & Comm. Code § 541.051(b)(5)(C); Ky. Rev. Stat. Ann. § 367.3615(2)(e); Fla. Stat. § 501.705(e)(3).