February 28, 2022

The Honorable Jan Schakowsky, Chair
The Honorable Gus Bilirakis, Ranking Member
Subcommittee on Consumer Protection and Commerce
Committee on Energy & Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Re: Hearing on "Holding Big Tech Accountable: Legislation to Protect Online Users"

Dear Chair Schakowsky, Ranking Member Bilirakis, and Members of the Subcommittee:

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the bills that will be addressed at the Subcommittee's March 1 hearing, *Holding Big Tech Accountable: Legislation to Protect Online Users*.

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services.

SIIA's comments focus on two of the five bills listed for that hearing: H.R. 6580, the "Algorithmic Accountability Act of 2022" (AAA), and H.R. 6416, the "Banning Surveillance Advertising Act of 2022" (BSAA). These comments are intended to reflect high-level input on the AAA and BSAA. They do not reflect the totality of our comments and we would welcome the opportunity to discuss both bills in further detail with you and your staff.

Comments on H.R. 6580 – The Algorithmic Accountability Act of 2022

We are pleased by the introduction of the AAA. The bill reflects a serious engagement with the challenging issues presented by artificial intelligence (AI) in a range of private sector activities. We believe the focus on impact assessments for the most high-risk applications of automated decision making is an important step towards fostering responsible, trustworthy, and ethical AI while protecting innovation. Importantly, automated decision systems have the potential to improve fairness outcomes over existing human-based-decision processes and any rules should support the development of these systems.

The use of impact assessments is widespread in the private sector, particularly among those companies that would be considered "covered entities" under the AAA. We believe that any statutory framework should complement efforts currently underway, such as the efforts by the National Institute of Standards and Technology (NIST) to create a framework for trustworthy AI, and provide guidance not only to the

private sector but to the Federal Trade Commission (FTC) and other federal agencies that will have a role in any regulatory framework that arises out of the AAA.

We provide the following comments in a spirit of improving the legislation as it proceeds through the House. We believe the edits proposed will help to foster innovation and minimize the regulatory burden on companies, support the overarching goals of protecting individuals, improve outcomes relative to existing human-based processes for sensitive decisions, ensure a more efficient allocation of limited government resources and technical expertise, and support regulatory interoperability.[1]

1. Incorporate an Explicit Risk-Based Framework for Categorizing Automated Decision Systems

The global nature of the innovation economy and the real possibility that foreign jurisdictions and non-federal jurisdiction in the United States may enact binding rules before the U.S. government does underscore the importance of Congress advancing a framework that is compatible with terminology and accepted best practices. The breadth of work on risk-based approaches to managing automated decision systems means that a legislative framework taking a different approach or using unique terminology could generate challenges for regulatory interoperability.

Because of this, we recommend amending the AAA to incorporate a risk-based framework for regulating automated decision systems. While we appreciate the distinction between systems used to render "critical decisions" and systems used in other manners, we believe, following a growing literature of practice and expert analysis in this area, that a risk-based framework is critical to improve regulatory interoperability, promote development of responsible AI, minimize implementation challenges for the government and private sector alike, and provide stronger and more meaningful protections to individuals.

A risk-based framework recognizes that automated decision systems present different risks depending on where, when, and how they are used; the level of human judgment involved in their application; the potential impact of systems on individuals; and the development stage of the system. A risk-based framework has broad consensus among academics, civil society, private industry, and lawmakers who have grappled with the challenges of automated decision making.[2] This is the approach being taken by NIST, which has embarked on an ambitious, expert-driven process to establish a risk management framework for AI that reflects input from a range of stakeholders, including from across the interagency and the general public.[3] It also forms the core of the proposed Artificial Intelligence Act under

---

[1] The carve out for "passive computing infrastructure" (section 2(13)) is too limited to address this concern. The bill defines "passive computing infrastructure" to exclude any intermediary technology that influences a decision – even if the decision is ultimately made by a human.

[2] See, e.g., OECD, *Framework for Classification of AI Systems* (Feb. 22, 2022); Future of Privacy Forum, *Automated Decision Making Systems: Consideration for State Policymakers* (May 12, 2021); Ada Lovelace Institute, *Regulation to innovate* (Nov. 2021).

[3] See NIST, AI Risk Management Framework Concept Paper (Dec. 13, 2021); NIST, A Proposal for Managing and Identifying Bias in Artificial Intelligence (June 2021).

consideration in the European Parliament, efforts in Canada, and legislative efforts in several U.S. states.[4] And, many SIIA members have already implemented measures to assess automated decision systems during development and use phases using risk-based frameworks.[5]

With this background, we consider the AAA to provide a framework for requiring impact assessments, summary reports, additional transparency measures, and training for "high risk" applications of automated decision systems – what the bill describes as "critical decisions." Following are additional recommendations that we believe will help to focus the scope of the AAA to achieve this goal.

2. *Focus the Definitions of "Automated Decision System" and "Augmented Critical Decision Process"*

First, we recommend that the AAA focus on automated decision systems that render decisions without human input. As written, the AAA would include the use of automated decision systems that *assist* in human decision-making. Uses of systems in that way do not present the same level of risk as those that are rendered without human involvement. While there may be value in requiring impact assessments of certain such systems to minimize the potential for algorithmic bias in the systems relied on by humans, under a risk-based approach, those requirements should be tailored to the potential risk.

To address this, for high-risk applications—those that are used in rendering "critical decisions"—we recommend focusing the definition of "automated decision system" to apply to fully automated systems without a human in the loop. Including any decisions that utilize automated decision systems even if a human ultimately makes the decision—i.e., those without a human "check"—is likely to generate a significant volume of impact assessments and reporting that do not present the same heightened risk to individual legal rights that fully automated systems may present. This will lead to significant burdens on limited government resources as well as the private sector. Even a regulatory body with increased funding and staff will have difficulties assessing the potential reporting volume.

We believe this concern can be addressed with revisions to two definitions, as follows:

(1) AUGMENTED CRITICAL DECISION PROCESS.—The term ''augmented critical decision process'' means a process, procedure, or other activity that solely employs an automated decision system to make a critical decision.
(2) AUTOMATED DECISION SYSTEM.—The term ''automated decision system'' means any

[4] See, e.g., European Commission, Proposal for a Regulation laying down harmonised rules for artificial intelligence (Apr. 21, 2021); Government of Canada, Directive on Automated Decision Making (Apr. 1, 2021) (cf. Government of Canada, Algorithmic Impact Assessment Tool); U.S. Food and Drug Administration, Artificial Intelligence and Machine Learning in Software as a Medical Device (Sept. 22, 2021); California Assembly Bill 13: *Public Contracts: automated decision systems* (last amended July 15, 2021).

[5] See, e.g., Jared Council, *How Adobe's Ethics Committee Helps Manage AI Bias*, Wall Street Journal (May 5, 2021); Adobe, Ethical Approach to AI; Google, Building a responsible regulatory framework for AI.

system, software, or process (including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques) that solely uses computation (excluding passive computing infrastructure) to make~~, facilitate, or inform~~ a decision or judgment.

In addition, we would urge a close review of the legislative text to ensure that the processes and procedures required of what we refer to as "high risk" systems are not applied more generally to all automated decision systems, as appears in several provisions within section 3(b). By way of example, the California legislature last year introduced Assembly Bill 13, which would distinguish between high and low risk automated decision systems and apply to systems that " substantially assist or replace human discretionary decisionmaking and that materially impacts natural persons."[6]

3. Clarify the Definition of "Critical Decision"

Second, we recommend clarifying the definition of "critical decision" to align better with our current understanding of congressional intent, that is, on decisions that have a direct and potentially significant effect on legal or other material rights. The definition currently lacks a guiding principle and does not reflect how automated decision systems can be used in the categories listed in section 2(8) in ways that do not raise high-risk concerns. There are countless routine uses of automated decision systems that may "relate to" issues around access, cost, terms, and availability that have no material impact on legal rights, the availability of services, and anti-discrimination, such as systems used to change utility rates to reflect inflation and other fixed costs; models used by financial investors; and online travel booking tools. As others grappling with these challenges have recognized, automated decision systems that do touch on material rights may not always have significant impacts on those rights.[7]

We propose the following revision to section 2(7) to address this:[8]

(7) CRITICAL DECISION.—The term ''critical decision'' means a decision or judgment that has ~~any~~ a direct legal or similarly significant effect on a consumer's life and relates to ~~access to or the cost, terms, or availability of~~ —eligibility determinations about or the cost or terms of --"

[6] California Assembly Bill 13. The notice for preliminary comments on the proposed rulemaking under California Privacy Rights Act of 2020 also included questions about how the legislature can tailor policy to a risk-based standard and the legislature is in the process of codifying this. SIIA comments can be found here.

[7] In this regard, the work done by Canada's Treasury Board provides a worthwhile comparison. See Government of Canada, Responsible use of artificial intelligence (AI) (resource page); Government of Canada, Directive on Automated Decision Making (Apr. 1, 2021).

[8] A similar approach is taken by the EU GDPR. Article 22 of the GDPR protects consumers from decisions "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." GDPR, Art. 22.

4. Ensure Expert Involvement in the Development of Impact Assessment Requirements

We appreciate the AAA's mandate for the FTC to seek input from NIST, the National Artificial Intelligence Initiative (NAII), and the Office of Science and Technology Policy (OSTP).[9] Given the expertise embedded in those agencies and their substantial work to date on the issues reflected in the AAA, we would urge Congress to create a greater role for those agencies in developing regulations to guide impact assessments for algorithmic decision making and a regulatory structure for reviewing those assessments and summary reports. Other agencies, such as the Department of Education, will be essential for understanding appropriate requirements for assessments on high-risk education technology systems.

We also encourage Congress to explicitly align the AAA with the risk-based framework that NIST is currently developing. As noted above, this effort benefits from deep engagement with experts within and outside of government. It represents the most comprehensive effort by the U.S. government to provide guidance to industry and is expected to be finalized in 2023.[10] This approach also will enable the FTC to to align rulemaking with state-of-the-art processes and procedures being incorporated already in the private sector to minimize bias and foster responsible, trustworthy AI.

5. Refine the Definition of "Biometrics"

In addition, we would urge Congress to revisit the AAA's definition of biometrics contained in section 2(3). This definition goes well beyond definitions in use in other jurisdictions. We advise the Subcommittee to compare this definition to the one in H.R. 6796, another bill that will be addressed at the March 1 hearing, and also to consider the points that SIIA has made in a recent submission to OSTP.[11]

Comments on H.R.6414 – The Banning Surveillance Advertising Act of 2022

To the extent that there is a concern about targeted advertising that occurs without transparency or user consent, we recommend proceeding through focused rulemaking or legislation around privacy and to prevent specific abuses. SIIA strongly supports a comprehensive federal privacy law that would address concerns about how consumer data is used, provide needed clarity for businesses and consumers alike, and foster a stronger innovation environment in the United States while maintaining our global competitiveness.

The BSAA does not come remotely close to meeting this standard. The scope of its proposed ban on "surveillance advertising" , notwithstanding the carve out for "contextual advertisements," would prohibit a large amount of advertising on the internet that results from user-identified preferences and consent.

---

[9] Sections 3(b)(1), 7(a); see also section 7(b)(3).

[10] NIST has also proposed a model that shapes nine principles that can reaffirm user trust in artificial intelligence: accuracy, reliability, resiliency, objectivity, security, explainability, safety, accountability, and privacy. NIST, *Trust and Artificial Intelligence* (Mar. 2021).

[11] SIIA, Comments on RFI for Public and Private Sector Uses of Biometric Technologies (Jan. 14, 2022).

The internet of today and the free online services made available to consumers are reliant on advertising, including personalized or targeted advertising. Targeted advertising is a widespread practice and not one that is the exclusive domain of the large technology companies identified in the Petition. Indeed, numerous U.S.-based retailers have their own ad networks and ad tech. Disruption of that advertising will certainly cause damage to small- and medium-sized companies and consumer welfare. In a contextual-only world where advertisers are looking for the right context to target ads, publishers with the largest and most varied web presence will have the biggest range of context for advertisers to target. The inevitable result would be less revenue for smaller publishers and creators (such as bloggers, newsletter publishers, and video content creators) and developers who rely on ads for funding. This will in turn reduce the diversity of content available online as they find it difficult to find contextually relevant advertisers. The effect of what Accountable Tech is proposing would be to shut down large swaths of the internet, increase costs of consumers who would be forced to pay subscription fees to access services that they now enjoy for free, and require small and medium sized businesses to develop entirely new means to reach consumers.

In addition, we have significant concerns about the proposed inclusion of a private right of action. As seen in the context of private enforcement of state privacy laws, a private right of action for statutory damages can generate an enormous amount of litigation leading to costs that are passed on to consumers. The potential for litigation relating to online advertising is exponentially greater and we strongly urge Congress to hold hearings on this issue, and gather further input from the public, prior to proceeding with markup.

Conclusion

We appreciate your consideration of our views. We look forward to working with the Subcommittee members and staff as these bills proceed in Congress.

Respectfully submitted,

Paul Lekas
Senior Vice President, Global Public Policy
Software & Information Industry Association (SIIA)