The Software Alliance

BSA

April 24, 2024

The Honorable Julie Gonzales
Colorado State Capitol
200 East Colfax Avenue
Denver CO 80203

Dear Chair Gonzales:

BSA | The Software Alliance appreciates the opportunity to share insights from the enterprise software sector on artificial intelligence (AI) generally and SB 205. BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing cutting edge services, and their products are used by businesses of all sizes across every sector of the economy. AI is much more than robots, self-driving vehicles, or social media; it is used by companies large and small to create and improve the products and services they provide to consumers, to streamline their internal operations, and to enhance their capacity to make data-informed decisions. BSA members are on the leading edge of providing businesses-to-business tools that help companies leverage the remarkable benefits of AI.[2]

As leaders in the development of enterprise AI, BSA members have unique insights into the technology's tremendous potential to further spur digital transformation in the private and public sectors and the policies that can best support the responsible use of AI, especially high-risk uses of AI. BSA's views are informed by our recent experience with members developing BSA Framework to Build Trust in AI,[3] a risk management framework for mitigating the potential for unintended bias throughout an AI system's lifecycle. Built on a vast body of research and informed by the experience of leading AI developers, the BSA Framework outlines a lifecycle-based approach for performing impact assessments to identify risks of AI bias and highlights corresponding risk mitigation best practices. BSA's extensive experience has helped us identify effective policy solutions for addressing AI risks.

We outline several priorities below that we believe policymakers should focus on when examining AI. We also make a number of specific recommendations to SB 205 to help ensure the legislation

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

[3] *See* BSA | The Software Alliance, Confronting Bias: BSA's Framework to Build Trust in AI, *available at* https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

is workable in practice and generally encourage continued alignment between SB 205 and Connecticut SB 2.

I. Focus on High-Risk Uses of AI

BSA commends you and the committee for focusing on high-risk uses of AI in SB 205. We recommend policymakers focus on AI systems that determine an individual's eligibility for housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance. These systems have the potential to affect important life opportunities — and are a key area for policymakers to address. In contrast, many everyday uses of AI present few risks to individuals and create significant benefits, like helping organize digital files, auto-populate common forms for later human review, improve a company's ability to forecast supply chain issues, and detect, prevent, and respond to cybersecurity threats.

The provisions in Sections 6-1-1602 and 6-1-1603 of SB 205 create a strong foundation for addressing the risks posed by high-risk uses of AI. We have several recommendations for improving these provisions so that they work in practice.

a. **The definition of consequential decision should be revised.** While we appreciate that high-risk uses are tied to consequential decisions, to avoid overbroad application, we recommend focusing the definition of this term on eligibility determinations, changing "access to, or the availability, cost, or terms of" to "eligibility for and results in the provision or denial of" in the definition. Focusing consequential decisions on eligibility determinations and the actual extension or denial of public goods and services helps capture the key aspects of these decisions that have the most impact to consumers' lives.

b. **The list of information the developer provides to a deployer about a high-risk AI system should be revised to reflect the developer's role.** Subsection 2 of Section 6-1-1602 outlines the information a developer must share with a deployer. However, it includes disclosure of an item that would not be within the purview of developers. Specifically, the bill requires developers to explain how an individual can monitor a high-risk AI system when it is used to make, or is a substantial factor in making, a consequential decision. Because developers design, code, or produce AI systems, and deployers use AI systems, they have access to different types of information. In this instance, deployers are best positioned to provide information about how consequential decisions are made and how an individual can monitor the system once deployed.

c. **The bill's requirements for developers and deployers to report when a high-risk AI system has caused algorithmic discrimination should be eliminated.** Subsection 5 of Section 6-1-1602 requires developers to inform all known deployers and the Attorney General when they discover or are informed by a deployer that a deployed high-risk AI system has caused algorithmic discrimination. Additionally, Subsection 6 of Section 6-1-1603 requires deployers to inform the Attorney General when a high-risk AI system has caused algorithmic discrimination. As an initial matter, such requirements envision an ongoing post-deployment relationship with the deployer, which may not be the case. Further, one deployer's use of the high-risk system in a discriminatory manner does not render all other uses discriminatory, and such notice would often be irrelevant to another deployer's use of the system. We suggest aligning with the version of Connecticut SB 2 released on April 23 and striking these requirements.

II. General-Purpose AI Models

The bill's approach to regulating developers of general-purpose AI models raises concerns. As an initial matter, the bill's approach is not risk-based and instead singles out a specific kind of technology to regulate, rather than focusing regulation on particular uses of the technology. Such an approach is overbroad and does not prioritize AI-related uses that pose the most significant risks to consumers. We recommend aligning with the version of Connecticut SB 2 released on April 23 and striking this section.

III. Risk Management Programs

BSA appreciates SB 205's recognition of the importance of risk management programs. Companies should create and maintain risk management programs that help them identify and mitigate risks. Risk management programs establish repeatable processes for companies to identify and mitigate potential risks that can arise throughout the lifecycle of an AI system.

Risk management is particularly important in contexts like AI, privacy, and cybersecurity, where the combination of quickly evolving technologies and highly dynamic threat landscapes can render traditional approaches to compliance ineffective. Risk management programs have two key components: (1) a governance framework of policies, procedures, and personnel that support the company's risk management function, and (2) a scalable process for performing impact assessments that identify and mitigate risks of an AI system.

One way for companies to establish risk management programs is by using the AI Risk Management Framework (AI RMF), which was released earlier this year by the National Institute of Standards and Technology (NIST).[4] The AI RMF builds on NIST's work creating frameworks for managing cybersecurity and privacy risks.[5] The AI RMF helps companies incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products. Ultimately, effective AI risk management programs should support coordination across the company, to promote the identification and mitigation of risks throughout the lifecycle of an AI system.

IV. Impact Assessments

BSA commends the recognition of impact assessments in SB 205 as an important tool for fostering accountability and building trust in AI. BSA recognizes that performing impact assessments is a key part of creating a meaningful risk management program. Impact assessments have three purposes: (1) identifying potential risks that an AI system may pose, (2) quantifying the degree of potential harms the system could generate, and (3) documenting steps taken to mitigate those risks.[6] Impact assessments are already widely used in a range of other fields, including privacy, as an accountability mechanism that demonstrates a product or system has been designed in a manner that accounts for the potential risks it may pose to the public.

Because impact assessments already exist today, they can be readily adapted to help companies

[4] NIST AI Risk Management Framework, available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[5] See NIST, Cybersecurity Framework, Questions and Answers, (discussing federal agency use of the NIST CSF), available at https://www.nist.gov/cyberframework/faqs.
[6] See BSA, Impact Assessments: A Key Part of AI Accountability, available at https://www.bsa.org/files/policyfilings/08012023impactassess.pdf.

identify and mitigate AI-related risks.[7] In our view, when AI is used in ways that could adversely impact civil rights or access to important life opportunities, the public should be assured that such systems have been thoroughly vetted and will be continuously monitored to account for the risks associated with unintended bias. Companies, both developers and deployers, should use impact assessments as a tool for the responsible development and use of high-risk AI systems.

V. Distinguishing Different Actors in the AI Ecosystem

BSA appreciates that SB 205 differentiates between different actors in the AI ecosystem, including AI developers and AI deployers. Much like privacy and security laws worldwide distinguish between different types of companies that handle consumers' personal data, AI laws should distinguish between developers and deployers to ensure that legal frameworks accurately assign obligations to a company based on its role in the AI ecosystem.

A developer is the company that designs, codes, or produces an AI system, such as a software company that develops an AI system for speech recognition. A deployer, in contrast, is the company that uses an AI system, such as a bank that uses an AI system either developed internally or by a third party to make loan determinations. Each type of company will have access to different types of information about an AI system and will be positioned to take different actions to mitigate the risks associated with the AI system. AI policies that distinguish between these roles can ensure that the appropriate company within the various real-world AI supply chains can identify and mitigate risks.

Distinguishing between these two types of entities based on of their role in the AI ecosystem can ensure companies are better able to fulfill their obligations and better protect consumers. For example, a developer would be able to describe the features of data used to train an AI system, but it generally would not have insight into how the AI system is used after another company has purchased and implemented the AI system. Instead, the deployer using the system is generally best positioned to understand how the AI system is being used, whether that use aligns with its intended use, whether and how to incorporate human oversight, the outputs from the AI system, any complaints received, and real-world factors affecting the system's performance.

VI. Enforcement

BSA commends SB 205 for granting exclusive enforcement authority to the Attorney General. Exclusive enforcement by the Attorney General helps ensure a consistent approach to enforcement. We also appreciate that the bill does not create a private right of action and expressly states that it does not create a private right of action under any other law.

Additionally, BSA understands that the Office of the Attorney General has significant experience conducting rulemaking processes, including to implement the state's consumer privacy law. However, we recommend policymakers prioritize creating clear statutory requirements in SB 205 that do not require a broad rulemaking process. Establishing strong and clear guardrails within the

[7] For example, three state privacy laws already require companies to conduct impact assessment for specific activities, including processing sensitive personal data, engaging in targeted advertising, or selling personal data; seven more state privacy laws will soon do so. Colorado, Connecticut, and Virginia already impose these requirements. See Colorado Privacy Act, Colo. Rev. Stat. Tit. 6, Art. 1, Pt. 13 §§ 6-1-1301–6-1-1313; Connecticut Data Privacy Act Conn. Gen. Stat. Tit. 42, Ch. 743jj, Sec. 42-515-525; Virginia Consumer Data Protection Act; Va. Code Tit. 59.1, Ch. 53, § 59.1-575-585. State privacy laws in California, Delaware, Florida, Indiana, Kentucky, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, and Texas will also require impact assessments for certain activities Globally, privacy and data protection laws worldwide use impact assessments as a tool for improving accountability.

legislation is important for businesses to understand their obligations and for consumers to know what to expect from companies.

* * *

Thank you for allowing us to provide the enterprise software sector's perspective. We welcome the opportunity to serve as a resource and further engage with you or a member of your staff on these important issues.

Sincerely,

Meghan Pensyl

Meghan Pensyl
Director, Policy