Business Software Alliance

September 15, 2025

The Honorable Tricia Farley-Bouvier
The Honorable Michael Moore
House and Senate Chairs, Joint Committee on Advanced Information and Technology, the Internet, and Cybersecurity
24 Beacon St.
Room 274
Boston, MA 02133

Dear Chair Farley-Bouvier and Chair Moore,

The Business Software Alliance appreciates the opportunity to share insights from the enterprise software sector on artificial intelligence (AI) and S. 37. 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.[2]

AI is changing the way we live and work, and it has real-world benefits. Realizing the potential of AI requires trusting that the technology is developed and deployed responsibly. Crafting AI legislation that promotes responsible uses of AI and protects against misuse is one of the most important technology issues today, and one we already see governments beginning to tackle, including in the European Union and in Colorado. The most effective way to address this issue is through a single, national law. However, just as states took the lead in adopting consumer privacy laws, we recognize states are again leading with AI legislation.

As you consider how to regulate AI through S. 37, we want to underscore the importance of ensuring any AI legislation creates thoughtful, clear guardrails for companies and protects consumers. To achieve this, we strongly recommend AI legislation:

- Focus on the uses of AI that have the greatest impact on consumers;
- Reflect the different roles and responsibilities of different actors along the AI value chain;
- Ensure strong enforcement; and
- Promote interoperability and incorporate stakeholder feedback.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.
[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

We appreciate the intent of S. 37 and share the goal of helping to ensure that AI is developed and used safely and securely. We believe governments can play a vital role in encouraging best practices and promoting guardrails around the creation and deployment of AI technologies.

We are concerned with S. 37's focus on specific types of AI technology, rather than focusing on high-risk uses of AI. Instead of regulating a specific type of technology, we believe policymakers addressing AI issues should focus on the priorities outlined below.

I. AI Creates Benefits Across Industry Sectors

As you consider how to regulate AI, it is important to recognize that the economic benefits of AI are not limited to one industry sector or one business model. Instead, the promise that AI may one day impact every industry is quickly turning into a commercial reality and driving digital transformation across sectors. Airlines now use AI systems to more efficiently clean planes between flights; farmers use AI to analyze large amounts of weather information to maximize their harvest; manufacturers use AI to test new prototypes; and construction companies build AI-generated "digital twins" of real-life cities to understand the impacts of a proposed design.

Companies in all industries use AI-powered enterprise software, including:

- In healthcare, a large pharmacy chain uses an advanced platform to forecast demand and redistribute medications across thousands of store locations and to deliver near real-time insights and recommendations for pharmacists to provide more personalized advice to patients. This helps managers understand the supply chain, store labor and productivity, patient vaccine scheduling, and prescription pickup processes.

- In manufacturing, a car maker used generative AI technology to redesign a seat bracket, which secures seat belt fasteners to seats and seats to floors, that is 40 percent lighter and 20 percent stronger than the previous iteration. Changes like these can help reduce the amount of material needed to build a car and make vehicles more fuel efficient.

- In agriculture, the research division of an enterprise software provider partnered with a climate risk company to develop software capable of providing more accurate long-range weather predictions. Traditional weather forecasting methods can provide accurate predictions for a seven-day window. By leveraging AI, the researchers are developing new forecasting models to provide accurate predictions of weather trends two to six weeks out from a given date. By providing reliable extended forecasts, these tools will help water managers predict snowpack

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

and water availability for irrigation, hydropower, and other critical agricultural and environmental uses.

Because BSA members work with companies across every sector of the economy, we have unique insights into AI's tremendous potential to further spur digital transformation and the policies that can best support the responsible use of AI. BSA's views are informed by our experience working with member companies to develop the 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 and highlights corresponding risk mitigation best practices.

II. AI Legislation Should Focus on High-Risk Uses of AI

AI legislation should focus on the uses of AI that have the most impact on consumers' lives. 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.

However, when AI systems are used to decide whether consumers are granted or denied important benefits and services, like housing, healthcare, and employment opportunities, companies should be accountable for developing and deploying those systems responsibly.

BSA recommends S. 37 be amended to focus on high-risk uses of AI, particularly 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.

As currently drafted, S. 37 broadly regulates developers of certain AI models. Specifically, S. 37 applies to covered models, meaning AI models that meet certain computing power and cost thresholds. By regulating these models broadly, S. 37 ignores the context in which these AI models are deployed. For example, covered models could one day be deployed in a wide range of contexts, from critical infrastructure or health care, to helping individuals

[3] *See* BSA's Framework to Build Trust in AI (June 2021), *available at* https://ai.bsa.org/confronting-bias-bsas-framework-to-build-trust-in-ai.

create new recipes or draft emails. Each of these use cases will present different safety and security risks, and broadly regulating these models fails to recognize how the unique circumstances in which AI models are deployed will influence risk mitigation approaches. We recommend S. 37 focus on high-risk uses of AI to address the most important impacts AI has on consumers' lives.

For these high-risk scenarios, new safeguards are important—and legislation can leverage tools that already exist to help companies identify and mitigate potential risks. BSA supports requiring companies that develop or deploy AI for high-risk uses to: (1) adopt risk management programs; and (2) conduct impact assessments. These measures can help companies identify and mitigate risks when AI makes important decisions about consumers—and increase trust that AI is developed and used responsibly. In particular:

- 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. One way for companies to establish risk management programs is by using the AI Risk Management Framework (AI RMF), developed by the National Institute of Standards and Technology (NIST). The AI RMF builds on NIST's work creating frameworks for managing cybersecurity and privacy risks. Ultimately, effective AI risk management programs should support cross-company coordination to promote the identification and mitigation of risks across the lifecycle of an AI system.

- Impact assessments are a key part of a meaningful risk management program. Both developers and deployers should use impact assessments as a tool for the responsible development and use of high-risk AI systems—and each type of company should conduct an impact assessment that reflects their role in developing or deploying the AI system. 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 in other fields, they can be readily adapted to help companies identify and mitigate AI-related risks.[4]

III. AI Legislation Should Distinguish Between Different Entities in the AI Ecosystem

[4] *See* BSA, Impact Assessments: A Key Part of AI Accountability (Aug. 1, 2023), *available at* https://www.bsa.org/policy-filings/impact-assessments-a-key-part-of-ai-accountability.

The AI supply chain is evolving, and AI legislation should not create one-size-fits-all requirements when companies have very different roles.

All companies that develop and use high-risk systems have responsibilities to manage AI risks, but those obligations must reflect the role of each type of company, since each will know different information about an AI system and will be able to take different actions to identify and mitigate risks. Legislation should reflect these differences, to create obligations that work in practice to safeguard consumers.

Distinguishing between these two types of entities based on 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.

We appreciate that S. 37 recognizes the unique role developers play in the AI ecosystem, however, the bill does not account for AI deployers and holds developers of covered models responsible for obligations outside of their purview, including by making covered model developers responsible for covered model derivatives, and is unworkable in practice as a result. For example, determining whether a covered model potentially enables critical harm will largely depend on the context in which the covered model is deployed and mitigation measures undertaken by the deployer, which is often a different entity than the developer of the model. Requiring covered model developers to account for the specific harms included in the bill assumes developers have access to information they often do not and are not positioned to mitigate. Additionally, S. 37 requires developers to incorporate full shutdown capabilities into their models and potentially holds developers liable for downstream uses over which they have no control.

IV. AI Legislation Should Ensure Strong Enforcement

We appreciate that S. 37 grants exclusive enforcement authority to the Attorney General.

Strong enforcement is needed in any AI legislation. Granting the Attorney General exclusive enforcement authority helps that office establish clear guidance and a consistent approach to enforcing the bill's requirements. Exclusive governmental enforcement by a single regulator ensures companies know how to implement the legislation's obligations—and avoids the conflicting interpretations and confusion likely to arise if courts reach different conclusions about how companies are to apply a bill's obligations.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

V. AI Legislation Should Promote Interoperability and Incorporate Stakeholder Feedback

Massachusetts is home to global companies, and your legislation will be most effective when it is interoperable with other approaches to AI regulation. Global companies can better serve their customers when they build strong compliance programs that work across markets. We appreciate the work of Massachusetts's lawmakers to share information with legislators in other states. We also encourage you to continue working with stakeholders as you develop your legislation, to understand how your AI law will work in practice, across a range of different industries and uses.

* * *

Thank you for allowing us to provide the enterprise software sector's perspective on S. 37. We welcome the opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Meghan Pensyl
Director, Policy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org