April 9, 2024

The Honorable Rebecca Bauer-Kahan
Assembly Privacy and Consumer Protection Committee
1020 N Street
Room 162
Sacramento CA 95814

Dear Chair Bauer-Kahan:

BSA | The Software Alliance appreciates the opportunity to share insights from the enterprise software sector on artificial intelligence (AI) generally and AB 2013 and AB 3204. 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.

[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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

When examining AI, we believe policymakers should focus on high-risk uses of AI, meaning AI that is used to make consequential decisions about an individual's eligibility for important services and benefits. In crafting legislation, policymakers should (1) clearly define the types of companies and types of decisions subject to the legislation, (2) require both developers and deployers of high-risk AI systems to conduct impact assessments, recognizing that the content of those assessments should be different based on whether a company is a developer or a deployer, and (3) require both AI developers and AI deployers to adopt risk management programs, to ensure companies have policies and personnel in place to identify and mitigate risks across the lifecycle of an AI system.

While we support the goal of promoting transparency, AB 2013's and AB 3204's focus on the data used to train AI systems, broad scope, and expansive requirements present several concerns, which are discussed in more detail below.

I. AB 2013

AB 2013 requires developers to post detailed documentation on their website about the data used to train an AI system. This approach creates at least four distinct concerns:

First, the number of companies and AI systems that would be subject to AB 2013's requirements is immense. AI is rapidly changing how we live and work, and virtually every company in the state will likely develop and/or use AI systems in some way. Since the legislation does not adopt a risk-based approach, even mundane uses of AI, like AI-powered spell check or translation apps, would be subject to AB 2013's granular disclosure requirements. Further, because AI is used across every sector, the bill's obligations will reach far beyond the tech industry to any company developing AI systems for health care, financial services, retail inventory management, and more.

Second, "developers" are required to post information about "each dataset" used in the development of the system. This requirement creates at least two practical concerns. As an initial matter, it is overbroad because the definition of developer includes any company that "substantially modifies" an AI system – without recognizing that some modifications will not involve training the AI system but may instead modify other aspects of the system. Moreover, requiring a developer to disclose information about "each dataset" used to develop an AI model may require the developer to provide information it does not have – since a developer may re-train an existing model that was initially trained by another company. Instead, a developer could be required to provide information about its own activities, focusing only on the datasets that developer used to train the model.

Third, developers are required to publicly disclose granular information about each dataset used in the development of the AI system, including (1) the source or owner of the dataset; (2) a clear definition of each category associated to data points within the dataset; (2) the time period during which the data in the dataset was collected; (4) the dates the dataset was first and last used during the development of the AI system; and (5) whether the dataset was purchased or licensed by the developer or is in the public domain. Given the vast amounts of data that are used to develop many AI systems, requiring such detailed information about each dataset is unduly burdensome and may cause disclosure of trade secrets or other confidential information. Further, using significant amounts and different types of data often results in AI systems that are sufficiently trained and tested. Requirements to publicly disclose comprehensive details about each dataset may unintentionally provide an incentive to not fully train or test AI systems, resulting in AI systems that are less safe and less secure.

Fourth, it's unclear what benefit to consumers AB 2013's public disclosures provide, given the bill's broad scope and detailed requirements could result in incredibly lengthy documentation. Further, the type of information required to be disclosed is likely to be of limited utility to a consumer. For

example, the source and time period for data collection will not provide information about the impact the AI system has on the consumer.

For these reasons, we suggest you focus on a risk-based approach that would provide consumers and businesses with transparency regarding when AI is used for high-risk purposes.

II. AB 3204

AB 3204 requires companies that use personal information to train AI to register with the state as a "data digester." Given how rapidly AI is evolving to improve our daily lives and business practices, most companies will develop and/or use AI in some manner. The bill defines "data digester" so broadly as to include virtually any company that incorporates AI into its business offerings, since doing so often requires further training of the AI system. It is unclear what benefit the bill's broad registry of data digesters provides to consumers or the state.

While we understand that California established a similar fund and registry for data brokers, the context in which AI systems are developed and used is fundamentally different, including because AI systems are developed and used across all industries. Rather than creating the data broker-style fund and registry envisioned in AB 3204, we strongly recommend the legislature focus on creating new guardrails for companies that develop and deploy AI systems for high-risk uses, in line with our comments above.

* * *

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

cc: Assembly Privacy and Consumer Protection Committee

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org