November 15, 2024

Senator Rosemary Bayer
Michigan State Capitol
P.O. Box 30036
Lansing, MI 48909-7536

Dear Senator Bayer:

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates your work to improve consumer privacy through SB 659, the Michigan Personal Data Privacy Act. In our federal and state advocacy, BSA works to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data. In the states, we have supported strong privacy laws, such as the consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We appreciate the opportunity to share our feedback on Senate Bill 659. While we commend the legislature's work in advancing consumer privacy legislation, we are concerned that the bill departs from other state privacy laws in ways that do not provide clear benefits to Michigan's consumers. As the legislature continues to debate SB 659, we urge you to ensure that where Michigan departs from those other laws, it does so in a manner that makes a meaningful contribution to the larger landscape in protecting consumers, rather than diverging without a clear advantage for consumer privacy.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Our recommendations focus on key priorities in the legislation:

- Supporting interoperability with other state privacy laws;
- Supporting consumer privacy through practical consent requirements;
- Supporting data minimization provisions that allow consumers to benefit from improved products and services;
- Supporting strong antidiscrimination provisions focused on unlawful activities;
- Supporting strong and exclusive enforcement by the state's Attorney General; and
- Supporting practical requirements for universal opt-out mechanisms.

I. Supporting Interoperability with Other State Privacy Laws

BSA supports privacy protections that are interoperable with other state privacy laws. To date, nearly all states have agreed on the same structural model for protecting privacy – but have adjusted that model to provide different levels of substantive protections for consumers.[2] Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can map obligations imposed by a new law against their existing obligations under other laws.

We appreciate the harmonized approach you have taken in aligning many of SB 659's provisions with existing state privacy laws. BSA supported strong privacy laws in states including Colorado, Connecticut, and Virginia, and has supported state privacy laws across the country that build on the same structural model of privacy legislation enacted in these states. In particular, we support SB 659's focus on establishing new rights for consumers, creating a range of obligations for businesses that require them to handle data responsibly, and focus on consumer-facing data rather than employment data, which can raise distinct and separate privacy concerns.

While many of SB 659's provisions promote harmonization with existing state privacy laws, as discussed below there are key areas in which the bill could further promote interoperability.

II. Supporting Consumer Privacy through Practical Consent Requirements

As currently drafted, Section 21(1)(a) of SB 659 prohibits controllers from "processing personal data concerning a consumer without obtaining the consumer's consent to process the personal data." While companies should provide consumers with information to make informed choices about how their data will be handled, requiring consent for every processing activity would burden consumers, who already confront numerous pop-ups every time they open a product or service. This requirement is also unnecessary, since SB 659 already requires companies to limit their collection of data in Section 21 and requires privacy notices to include a list of processing purposes in Section 25. There is growing recognition[3] that

[2] For additional information on enacted state privacy laws, please see BSA's 2024 Models of State Privacy Legislation, which is attached to this letter.

[3] *See* Center for Democracy & Technology, Notice and Choice are No Longer a Choice (2019), at https://cdt.org/insights/notice-and-choice-are-no-longer-a-choice/ and Electronic Privacy Information

requiring consent for all processing purposes is not effective, as it overwhelms consumers with information and does not provide them with meaningful control over their data. For these reasons, we encourage you to strike this requirement from the bill's language.

Other provisions in SB 659 also overly rely on consent. For example, Section 33(2)(a) provides that obligations imposed on controllers or processors do not restrict their ability to collect, use, or retain data to "conduct internal research to develop, improve, or repair products, services, or technology if the controller or processor conducting that research obtains consent from the consumer." Relatedly, Section 25(1)(g) would require privacy notices to contain information about consumers' ability to consent to the use of their personal data for internal research. Currently, companies regularly disclose when consumers' personal data will be used for such research purposes in their privacy policies. The language in SB 659 would result in consumers receiving consent notices for testing something as simple as an autofill function, which allows consumers to easily populate documents with their personal data. Furthermore, other state privacy laws clearly account for companies' need to use personal data to improve products and develop new products and services, without requiring consent. We urge you to adopt a similar approach in SB 659.

III. Supporting Data Minimization Provisions that Allow Consumers to Benefit from Improved Products and Services

While we appreciate the legislature's focus on creating privacy protections that are right for Michigan, we are concerned that SB 659 creates a data minimization requirement that restricts companies from providing improved products and services to consumers.

Section 19(e) would require controllers to "limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer to whom the data pertains, and consistent with the consumer's reasonable expectations." That standard is more restrictive than most other states, in ways that may inadvertently harm Michigan consumers. In fifteen other states, privacy laws require controllers to limit the collection of personal data to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer." California's privacy law similarly requires that a business' "collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." SB 659's language can prevent companies from improving how existing products work, or developing new products as old ones become obsolete.

We urge you to modify SB 659's approach to data minimization. Instead, controllers should be required to "limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer to whom the data pertains, or ~~and~~ consistent with the consumer's

Center, EPIC to House Committee: Notice and Choice Does Not Protect Privacy (2023), at https://epic.org/epic-to-house-committee-notice-and-choice-does-not-protect-privacy/.

reasonable expectations." This change will help to ensure that consumers in Michigan can continue to benefit from improved products and services.

IV. Supporting Strong Antidiscrimination Provisions Focused on Unlawful Activities

SB 659's antidiscrimination provision should also be revised, to clearly focus on unlawful discrimination. Section 21(1)(e) of the bill prohibits controllers from collecting, processing, or transferring "personal data in a manner that discriminates against an individual or otherwise denies an individual the full and equal enjoyment of goods and services because of religion, actual or perceived race, color, national origin, ancestry, sex, sexual orientation, gender identity, or physical or mental disability." BSA strongly supports the objective of this provision, and we recognize the importance of ensuring that technology is not used to discriminate. However, as currently written, this provision creates uncertainty for companies implementing a new obligation because it is not clearly tied to activities that are unlawful under state and federal laws. We strongly recommend revising this provision to prohibit controllers from collecting, processing, or transferring personal data "in a manner that unlawfully discriminates against an individual" on the bases set out in the bill.

V. Supporting Strong and Exclusive Enforcement by the State's Attorney General

BSA supports strong and exclusive regulatory enforcement by a state's Attorney General, which promotes a consistent and clear approach to enforcing new privacy obligations. State Attorneys General have a track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies.

We encourage you to support consistency with other state privacy laws in SB 659's enforcement provisions by establishing exclusive enforcement authority in the state Attorney General and clarifying that nothing in the law establishes a private right of action under it or any other law. Effective enforcement is important to protecting consumers' privacy, ensuring that businesses meet their obligations, and deterring potential violations.

VI. Supporting Practical Requirements for Universal Opt-Out Mechanisms

To ensure companies can comply with SB 659's requirements, we strongly encourage you: (1) recognize universal opt-out mechanisms already recognized in other states and (2) adopt a delayed implementation date for any universal opt-out mechanism requirement.

Section 14(1) of SB 659 would require controllers to honor a consumer's use of a universal opt-out mechanism to exercise new rights to opt out of targeted advertising or the sale of their personal data. If the bill retains this requirement, we strongly encourage you to focus on recognizing a universal opt-out mechanism that is interoperable with mechanisms recognized in other states. Interoperability is essential in ensuring that any universal opt-out mechanism is workable and allows consumers to effectuate their rights across state lines.

We also recommend delaying the implementation date for any universal opt-out mechanism recognized in SB 659 for one year after the bill's effective date. Companies will require time to build tools to respond to global opt-out mechanisms — and ensuring sufficient lead time to implement those obligations can foster the development of stronger practices for honoring opt-out mechanisms. Ensuring companies have one year to honor a universal opt-out mechanism will help companies leverage their work in complying with other mechanisms to better serve consumers in Michigan.

Thank you for your continued leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Olga Medina
Director, Policy

CC: Senator Mary Cavanagh

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org