The Software Alliance

BSA

December 19, 2023

Wisconsin Senate Committee on Shared Revenue, Elections, and Consumer Protection
Wisconsin State Capitol
Madison WI 53708

Chair Knodl, Vice Chair Feyen, and members of the committee,

BSA │ The Software Alliance[1] supports strong privacy protections for consumers and appreciates Wisconsin's efforts to improve consumer privacy through SB642/AB466, relating to consumer data protection. 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. At the state level we have supported strong privacy laws in a range of states, including consumer privacy laws enacted in Connecticut, Texas, 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 SB642/AB466. Our feedback below focuses on BSA's support for SB642/AB466's recognition of two of our core priorities: recognizing the unique role of data processors and creating privacy protections that are interoperable with other state laws.

I. Distinguishing Between Controllers and Processors Benefits Consumers.

Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when

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

and why to collect a consumer's personal data. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction. In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers, while all other state comprehensive privacy laws use the terms controllers and processors.[2] This longstanding distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[3] BSA applauds the incorporation of this globally recognized distinction into SB642/AB466.

Distinguishing between controllers and processors better protects consumer privacy because it allows legislation to craft different obligations for different types of businesses based on their different roles in handling consumers' personal data. Privacy laws should create important obligations for both controllers and processors to protect consumers' personal data — and we appreciate SB642/AB466 recognition that those obligations must reflect these different roles. For example, we agree with the bill's approach of ensuring both processors and controllers implement reasonable security measures to protect the security and confidentiality of personal data they handle. We also appreciate the bill's recognition that consumer-facing obligations, including responding to consumer rights requests and seeking a consumer's consent to process personal data, are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to processors handling personal data on behalf of those controllers. Distinguishing between these roles creates clarity for both consumers exercising their rights and for companies implementing their obligations.

II. Creating Privacy Protections That Are Interoperable

Additionally, we support efforts to ensure that SB642/AB466 promotes uniformity and brings clarity with respect to this critical area of state law. 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 readily map obligations imposed by a new law against their existing obligations under other laws. BSA appreciates the sponsors' efforts to align of many of the bill's provisions with existing comprehensive state privacy laws. BSA has supported numerous state privacy laws, including laws in Connecticut, Texas, and Virginia, which adopt a similar structural model of privacy legislation. In particular, BSA supports

[2] *See, e.g.,* Colorado CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Delaware Personal Data Privacy Act, Sec. 12D-102(9, 24); Florida Digital Bill of Rights Sec. 501.702((9)(a)(4), (24)); Indiana Senate Enrolled Act No. 5 (Chapter 2, Sec. 9, 22); Iowa Senate File 262 (715D.1(8, 21)); Montana Consumer Data Privacy Act Sec. 2(8,18); Oregon CPA Sec. 1(8, 15); Tennessee Information Protection Act 47-18-3201(8, 20); Texas Data Privacy and Security Act Sec. 541.001(8, 23); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

[3] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which helps companies that process data demonstrate adherence to privacy obligations and helps controllers identify qualified and accountable processors. In addition, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data. For additional information on the longstanding distinction between controllers and processors – sometimes called businesses and service providers – BSA has published a summary available here.

SB642/AB466's exclusion of employment data from the bill's scope and in its definition of "consumer."

Additionally, we appreciate SB642/AB466's approach to enforcement, which provides the Attorney General with exclusive authority to enforce the bill. We support strong and exclusive regulatory enforcement by the Attorney General's office, which promotes a consistent and clear approach to enforcement.

We recognize that, as passed in the Assembly, AB466 includes a clear requirement for 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. Under the bill as amended, controllers must honor these mechanisms no later than July 1, 2026. If the Senate bill incorporates this requirement, we strongly encourage the committee to focus on creating a universal opt-out mechanism that functions in practice. It is important to address how companies will understand which universal opt-out mechanism(s) meet the bill's requirements. One way to address this concern is by creating a clear process for developing a public list of universal opt-out mechanisms and soliciting stakeholder feedback as part of that process, similar to the approach contemplated in Colorado's privacy regulations[4] Focusing on the practical aspects of implementing this requirement can help companies develop strong compliance programs that align their engineering and other resources accordingly. We also encourage the committee to focus on recognizing a universal opt-out mechanism that is interoperable with mechanisms recognized in other states.

We appreciate that the global opt-out mechanism provisions in AB466 as amended include an effective date that recognizes the ongoing work surrounding the implementation of similar mechanisms in Colorado and Connecticut. Ensuring that the obligation to honor a universal opt-out mechanism does not take effect until after July 1, 2026, will help companies leverage that ongoing work to better serve consumers in Wisconsin — and help to ensure that consumers in Wisconsin can use opt-out mechanisms they may already be familiar with in other states. Finally, as the committee considers how to ensure any universal opt-out mechanism works in practice, we recommend educating consumers about what universal opt-out mechanisms do in addition to their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer's personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser. Consumers should be aware of this and other limitations.

Thank you for establishing strong consumer privacy protections in Wisconsin and for your consideration of our views. We welcome any opportunity to further engage with the committee on this important topic.

Sincerely,

Matthew Lenz
Senior Director and Head of State Advocacy

[4] *See* Colorado Attorney General's Office, Colorado Privacy Act Rules (final rules) (Mar. 15, 2023), *available at* https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.