October 18, 2023

The Honorable Ed Neilson
127 Irvis Office Building
P.O. Box 202174
Harrisburg, PA 17120-2174

Dear Representative Neilson:

BSA | The Software Alliance[1] supports strong privacy protections for consumers and appreciates the Commerce Committee's work to improve consumer privacy HB1201, the Pennsylvania Consumer 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. At the state level we have supported strong privacy laws in a range of states, including 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, and their business models do not depend on monetizing users' data.

We appreciate the opportunity to share our feedback on HB1201. Our recommendations below focus on BSA's core priorities in privacy legislation: clearly distinguishing between controllers and processors, establishing practical obligations for processors, creating workable universal opt-out mechanisms, and ensuring HB1201's interoperability with other state laws.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

## I. Distinguishing Between Controllers and Processors Benefits Consumers.

We support HB1201's clear recognition of the unique role of data processors. 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 and why to collect a consumer's personal data. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction by assigning important — and distinct — obligations to both processors and controllers.[2] In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers.[3] 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.[4] BSA applauds Representative Neilson for incorporating this globally recognized distinction into HB1201.

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 HB1201's 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.

---

[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] *See, e.g.*, Cal. Civil Code 1798.140(d, ag).

[4] 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.

## II. The Bill's Provisions Giving Controllers an Opportunity to Object to Processors' Use of Subcontractors Should be Revised.

While HB1201 recognizes the important distinction between controllers and processors, we are concerned that some aspects of the bill could inadvertently limit processors' ability to provide consumers and businesses with the products and services they request, reduce their ability to safeguard those services, or even create privacy and security risks for consumers.

Specifically, Section 6(b)(4) creates significant concerns. It requires contracts between a controller and processor give the controller an "*opportunity to object*" to the processor's subcontractors.

We recognize the need for a consumer's data to be protected regardless of whether the data are held by a processor or by the processor's subcontractor. However, we strongly recommend a different approach: requiring processors to *notify* a controller about the use of a subcontractor and pass on the processor's obligations to that subcontractor — but not requiring controllers have the *opportunity to object* to subcontractors. This issue is particularly important, because of the frequency with which processors engage subcontractors to provide services requested by controllers. In many cases, processors will rely on dozens (or more) of subprocessors to provide a single service and may need to replace a subcontractor quickly if the subcontractor is not able to perform a service due to operational, security, or other issues. Requiring that controllers have an opportunity to object slows down the delivery of services and products to consumers, without clear benefits to privacy. Indeed, if a processor needs to switch subcontractors quickly because of a security issue, the delay involved in providing a controller the opportunity to object to a new subcontractor may expose consumers' data to security and privacy risks.

Instead of creating an opportunity for controllers to object to a processor's subcontractors, we recommend revising HB1201 to require a processor to notify a controller about subprocessors and pass on obligations to subcontractors via contract. This approach ensures consumers' personal data remain protected.

## III. Consider Practical Issues Involved in Creating a System for Recognizing Universal Opt-Out Mechanisms.

We believe that consumers should have clear and easy-to-use methods to exercise new rights given to them by any new privacy law. Like the state privacy laws enacted in Colorado and Connecticut, HB1201 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 Section 5(e)(1)(ii), controllers must honor these mechanisms no later than January 1, 2026.

If the bill retains this requirement, we strongly encourage you 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 HB1201'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.[5] 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 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 appreciate that HB1201 includes an effective date that recognizes the ongoing work surrounding the implementation of global opt-out mechanisms in Colorado and Connecticut. Ensuring that HB1201's obligation to honor a universal opt-out mechanism does not take effect until after January 1, 2026 will help companies leverage that ongoing work to better serve consumers in Pennsylvania — and help to ensure that consumers in Pennsylvania can use opt-out mechanisms they may already be familiar with in other states.

Finally, as you consider 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.

## IV. Promote an Interoperable Approach to Privacy Legislation.

Finally, BSA appreciates your efforts to align of many of HB1201's provisions with the Connecticut Data Privacy Act (CTDPA). BSA supported the Connecticut privacy law and consumer privacy laws adopted in Colorado and Virginia, which build on the same structural model of privacy legislation enacted in Connecticut. 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.

In particular, we support HB1201's exclusion of employment data from the bill's scope and in its definition of "consumer." While the bill excludes employment data in these contexts, it includes "professional or employment-related" information in the definition of "personal data" in Section 2. Rather than defining this term through a list approach, we recommend adopting a definition of "personal data" as information that "is linked or reasonably linkable to an identified or identifiable individual." HB1201 already includes a definition of the term "identified or identifiable individual," which aligns with the definition of this term in other state privacy laws. Finally, we support HB1201's approach to enforcement, which provides the Attorney General with exclusive authority to enforce the bill, which we believe will help promote a consistent and clear approach to enforcement.

We commend the drafting of HB1201's provisions in a manner that is interoperable with protections included in other state privacy laws, which helps drive strong business compliance practices that can better protect consumer privacy.

[5] *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.

Thank you for the opportunity to provide our perspective in establishing strong consumer privacy protections. BSA would be happy to provide further perspective on this legislation as it progresses through the legislative process.

Sincerely,

Matthew Lenz

Senior Director and Head of State Advocacy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org