August 5, 2022

The Honorable Philip J. Weiser
Office of the Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203

Dear General Weiser:

BSA | The Software Alliance[1] appreciates the opportunity to share informal comments in advance of rulemaking by the Colorado Office of the Attorney General to implement the Colorado Privacy Act. BSA members support strong privacy protections for consumers. 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 advocated for strong privacy laws, including the Colorado Privacy Act.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create the business-to-business technologies that other companies use. 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' personal data.

Our comments focus on three aspects of the Colorado Privacy Act:

- Supporting regulations that adopt a practical approach to implementing universal opt-out obligations;
- Supporting the Act's clear recognition of the different roles of controllers and processors in safeguarding consumers' personal data; and
- Supporting a harmonized approach to implementing core structural aspects of the Act, which can strengthen an interoperable approach to privacy that contributes to clear expectations for consumers and drives strong compliance practices by companies.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, 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. Universal Opt-Out Mechanisms

BSA believes that consumers should have clear and easy-to-use methods to exercise new rights given to them by any new privacy law, including the Colorado Privacy Act.

The Colorado Privacy Act includes a clear requirement for controllers to honor a consumer's use of universal opt-out mechanisms to opt out of sale or targeted advertising as of July 1, 2024. The Act also requires the Attorney General's office to adopt regulations by July 1, 2023, detailing the technical specifications for one or more universal opt-out mechanisms. These technical specifications will be critical to how controllers meet the universal opt-out obligations under the Act — and opt-out mechanisms are the only topic for which the Attorney General's office is *required* adopt regulations. We strongly encourage you to prioritize developing regulations that ensure opt-out mechanisms can be implemented in practice, by both consumers and companies.

The statute contains an important set of requirements for regulations that address the technical specifications for one or more universal opt-out mechanisms, including several requirements focused on how consumers will use those opt-out mechanisms. For example, the Act requires that a universal opt-out mechanism "clearly communicate" a consumer's "affirmative, freely given, and unambiguous choice" to exercise her opt-out rights.[2] In addition, the statute requires that regulations on opt-out mechanisms permit the controller to authenticate the consumer as a resident of Colorado, adopt a mechanism that is "as consistent as possible with any other similar mechanism" required by other states, and require controllers to inform consumers about their opt-out choices, among other requirements. These safeguards are critical to ensuring a universal opt-out mechanism will work in practice and be interoperable with opt-out mechanisms recognized by other states.

At the same time, the Act does not address other practical issues that are likely to arise in the course of implementing opt-out mechanisms — including how a controller will know that a particular mechanism meets the Act's requirements and educating consumers about the limits of opt-out mechanisms. We encourage you to focus on these practical issues as you develop regulations, including leveraging ongoing work by other states and by a broad range of stakeholders in order to develop regulations that support a practical and interoperable approach to universal opt-out mechanisms.

Recommendations:

- *First, we encourage you to focus on opt-out mechanisms that are interoperable with mechanisms recognized in other states.* Although consumers often use the term "global opt out" to refer to the ability to use a single mechanism to opt out of processing by a range of different companies, an opt-out mechanism must also function globally in the geographic sense. There is a real benefit to both consumers and to companies in ensuring that any opt-out mechanism works not just in a single state but can operate across states. This is particularly true given the enactment of Connecticut's new state privacy law, which also clearly requires controllers to honor global opt-out mechanisms as of January 1, 2025, as well as the ongoing rulemaking by the California Consumer Privacy Protection Agency that addresses the use of global opt-out mechanisms in California.

- *Second, we encourage you to consult with stakeholders on practical issues, including how a controller will know that a signal meets the law's requirements.* While it is important to require controllers to honor only certain signals — such as those that meet the set of guardrails in Section 6-1-1313(2) — it is not clear from the Act how a controller will be able to determine that a particular signal meets these requirements, or if that determination will be left to each controller. For example, it is not clear whether the Attorney General's office would publish a list of the signals that meet these requirements and thus identify the specific mechanisms that companies would need to honor. We urge you to work with stakeholders on these types of practical issues. Companies will require time to

[2] *See* Colorado Privacy Act Sec. 6-1-1313(2).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

build tools to respond to global opt-out mechanisms — and focusing on practical issues early on will help to foster the development of tools that work in practice.

- *Third, we encourage you to prioritize educating consumers about what opt-out signals do — and what they do not do.* As states support the use of universal opt-out mechanisms, it is important for consumers to understand the scope of what opt-out mechanisms do as well as their limits. For example, if a consumer uses a browser-based mechanism to opt out of sale and targeted advertising, the browser effectuates those requests with respect to activity that occurs within the browser. But the browser-based mechanism may not be able to convey requests to opt out of processing that occurs outside of the browser, such as when the consumer uses a mobile device or interacts with a company in person. Consumers should be aware of what opt-out mechanisms do — and do not do — so they may better use them as one method for exercising their rights under the Act, without mistakenly relying on opt-out mechanisms in situations where they do not apply.

- *Fourth, we encourage you to work with other states and regulatory agencies*. In the next two years, there will be a significant focus among a broad range of industry, government, and advocacy stakeholders in developing methods for complying with global opt-out requirements. As Connecticut and California continue their own efforts to address the use of opt-out mechanisms, we encourage you to leverage the ongoing engagement by stakeholders and other regulators, to further support an interoperable approach to opt-out mechanisms in Colorado's regulations.

II. The Roles of Controllers and Processors

We appreciate the Colorado Privacy Act's clear recognition of the unique role of data processors, which process data on behalf of other companies and pursuant to their directions. As enterprise software companies, BSA members often act as processors that handle data on behalf of their business customers; those business customers, in turn, act as controllers that decide how and why to process consumers' personal data.[3]

Every state that has enacted a comprehensive consumer privacy law has distinguished between controllers and processors – and assigned important, but distinct, obligations to both types of companies.[4] Indeed, this distinction is fundamental to leading privacy and data protection laws worldwide.

Privacy laws make this distinction for good reason. Clearly assigning obligations to both controllers and processors helps companies understand their obligations. More importantly, distinguishing between these roles helps consumers by ensuring their personal data is protected not only when it is processed by a consumer-facing company they interact with (acting as a controller), but also when that company uses vendors and service providers (acting as processors) to process the data. BSA supports placing strong obligations on both controllers and processors — but those obligations must fit these different roles in order to fully protect consumers' personal data. For example, we appreciate the Colorado Privacy Act's

[3] Of course, when BSA members collect data for their own business purposes, they are not acting as a processor but instead act as a controller for such activities. For instance, a company that operates principally as a processor will nonetheless be treated as a controller if it collects data for the purposes of providing a service directly to consumers. The Colorado Privacy Act appropriately recognizes that companies may act in these different roles at different times, with respect to different processing activities. *See* Colorado Privacy Act Sec. 6-1-1305(7) (stating that determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed).

[4] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1306 (Responsibility According to Role); Connecticut's Personal Data Privacy Act Sec. 7; Utah's Consumer Privacy Act Sec. 13-61-301 (Responsibility According to Role); Virginia Consumer Data Protection Act, Sec. 59.1-577 (Responsibility According to Role; Controller and Processor). California similarly distinguishes between these roles, which it calls businesses and service providers. *See* Cal. Civil Code Sec. 1798.140(ag) (defining service providers and requiring service providers and businesses to enter into contracts that limit how service providers handle personal information).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

recognition that consumer-facing obligations, such as responding to consumer rights requests and seeking a consumer's consent to process sensitive personal data, are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to processors that handle data on behalf of controllers.[5] Other obligations, such as adopting reasonable security measures to safeguard personal data, are appropriately placed on both types of companies.

BSA also recognizes that processor-specific obligations are important to build consumers' trust that personal data will remain protected when it is held by processors, which handle that data on behalf of other companies. BSA has therefore supported processor-specific obligations like those in Section 6-1-1305 of the Colorado Privacy Act, as well as similar obligations in Connecticut and Virginia state privacy laws.

Recommendation:

- *We strongly recommend that any regulations under the Colorado Privacy Act continue to reflect the important distinction between controllers and processors*.

III. Prioritizing a Harmonized Approach to Regulations

While states will naturally develop laws and regulations that are different in how they protect consumers, we want to emphasize the value of contributing to a set of state privacy laws and regulations that work together and share core structural commonalities. This approach not only helps businesses understand how their obligations change across jurisdictions — and map those obligations to one another — but also creates a broader set of shared expectations among consumers.

The Colorado Privacy Act shares many important structural similarities with the new privacy laws in Connecticut, Virginia, and Utah. As you issue regulations to implement the Colorado Privacy Act, we encourage you to prioritize harmonizing structural aspects of those regulations with other leading state privacy laws — and ensure that any regulations departing from these core structural provisions are done 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.

Recommendation:

- *We strongly recommend prioritizing regulations that ensure the Colorado Privacy Act is interoperable with other leading state and global privacy laws.*

* * *

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 your office on these important issues.

Sincerely,

Kate Goodloe
Senior Director, Policy

[5] For additional information on the distinction between controllers and processors, BSA has published a two-pager available here.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org