November 7, 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 our views on the proposed Draft Rules to implelment the Colorado Privacy Act (Draft Rules) and to participate in stakeholder sessions on the Draft Rules. 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 consumer privacy laws, including the Colorado Privacy Act (CPA).

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.

BSA appreciates the ability to provide feedback on the Draft Rules at multiple stages in the rulemaking process, and we expect to provide additional input throughout the process line with the tiered structure for stakeholder feedback. At this stage, and in advance of the November stakeholder sessions, our comments focus on two critical issues addressed by the Draft Rules:

- ***First, we strongly recommend revising the Draft Rules' approach to the role of processors in fulfilling consumer rights requests.*** The CPA's statutory text allows processors to adopt a range of "technical and organizational measures" to assist a controller in

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

responding to consumer rights requests. However, the Draft Rules are far narrower — and appear to assume that processors will respond to consumer requests sent to them by controllers one-by-one, without recognizing that in many cases a processor can better assist a controller in responding to those requests by building a scalable tool the controller can use to fulfill requests for personal data held by the processor. We strongly recommend revising the Draft Rules to align with the CPA's broader approach.

- ***Second, we encourage you to consider other practical issues involved in creating a system for recognizing universal opt-out mechanisms, including ensuring companies have sufficient time to implement new mechanisms.*** We support the Draft Rules' recognition that there should be a system for recognizing universal opt-out mechanisms that meet the CPA's requirements. We encourage you to address other important aspects of implementing this system, including creating a clear process for developing the public list of universal opt-out mechanisms, soliciting stakeholder feedback as part of that process, and specifying how often the "periodic updates" to that list will be issued, to help companies develop strong compliance programs that align their engineering and other resources accordingly. We also strongly recommend providing nine to twelve months between the time a universal opt-out mechanism is recognized as meeting CPA's requirements and requiring companies to honor that mechanism, to ensure companies can build those mechanisms into their products and services. We therefore recommend the initial list of mechanisms be published no later than October 1, 2023.

I. Role of Processors in Fulfilling Consumer Rights Requests

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 when their personal data is held by processors. However, the Draft Rules do not fully account for the role of processors in handling consumer rights requests, including the ability of processors to assist controllers in responding to consumer rights requests by creating scalable tools the controller may use to fulfill rights requests for data held by the processor. We strongly recommend revising the Draft Rules to better align with the CPA's broader approach to this issue, which can help ensure that consumer rights requests work in practice for data held by processors.

A. The CPA Reflects the Role of Processors

As an initial matter, BSA appreciates the CPA'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 because they 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.[2] 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.[3] Indeed, this longstanding distinction has existed for more than 40 years and is fundamental to leading privacy laws worldwide.[4]

---

[2] 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 CPA 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).

[3] *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).

[4] *See* BSA, Controllers and Processors: A Longstanding Distinction in Privacy (tracing history of the terms controller

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. BSA has therefore supported processor-specific obligations like those in CPA Section 6-1-1305, as well as similar obligations in Connecticut and Virginia.

B. The CPA Recognizes that Processors Play an Assisting Role in Fulfilling Consumer Rights Requests

Under the CPA, controllers are assigned the responsibility of responding to consumer rights requests, including requests to access, correct, and delete their personal data. This is consistent with all other state consumer privacy laws and leading data protection laws worldwide, which place this obligation on companies that decide how and why to collect consumers' personal data — rather than the processors acting on behalf of such companies. For example, under the CPA consumers may submit requests "to a controller" to exercise rights to access, correct, delete, and port their personal data.[5] In response "a controller" is to "inform a consumer" about action taken on those requests.[6] Controllers are also to establish internal processes to allow consumers to appeal denials of such requests.[7]

Of course, consumer rights created by the CPA must be meaningful in practice — including when a controller engages processors to process personal data on its behalf. That is why the CPA's statutory text creates a clear obligation for processors to *assist* controllers in fulfilling consumer rights requests. Under the statute, processors are to "adhere to the instructions of the controller and *assist the controller*" in meeting the controller's obligations, including by "*taking appropriate technical and organizational measures*, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to Section 6-1-1306."[8]

The CPA therefore allows processors to adopt a range of "technical and organizational measures" to assist controllers in responding to consumer rights requests. That obligation mirrors the obligation imposed on processors not just by other state privacy laws enacted in Connecticut, Virginia, and Utah, but also the obligation imposed by the EU's General Data Protection Directive.[9]

The obligation for processors to assist controllers through "technical and organizational measures" allows the companies to identify a range of measures that a processor can take to assist a controller in responding to consumer rights requests. Those measures will vary depending on the type of services at issue and the scale and sophistication of the companies. Although smaller processors may prefer for their business customers to forward them each individual rights request so that the processor can respond to each one in turn, that process may be unworkable for larger companies that need scalable solutions to quickly and efficiently honor consumer requests. The CPA's statutory language creates

---

and processor and their adoption worldwide), available at https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf.

[5] *See* Colorado Privacy Act Sec. 6-1-1306(1) (emphasis added).

[6] *See* Colorado Privacy Act Sec. 6-1-1306(2).

[7] *See* Colorado Privacy Act Sec. 6-1-1306(3)(a).

[8] *See* Colorado Privacy Act Sec. 6-1-1306(2)(a).

[9] See Connecticut's Personal Data Privacy Act Sec. 7(a)(1) (requiring a processor to assist a controller including by "appropriate technical and organizational measures . . . to fulfill the controller's obligation to respond to consumer rights requests"); Utah's Consumer Privacy Act Sec. 13-61-301(1)(b) (requiring a processor to assist a controller in meeting the controller's obligations "by appropriate technical and organizational measures); Virginia Consumer Data Protection Act, Sec. 59.1-579A.1 (requiring a processor to assist a controller including by "appropriate technical and organizational measures . . . to fulfill the controller's obligation to respond to consumer rights requests"). In California, the statute requires service providers to either execute consumer rights requests forwarded to them by the business or enable the business to do so. See also EU GDPR Article 28.3(e) (requiring controllers and processors to enter into a contracts requiring that the processor "assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights.")

flexibility that allows companies to take either of these approaches, because both the process of responding to one-by-one requests and the creation of scalable tools amount to technical and organizational measures that assist a controller in complying with consumer rights requests. The CPA's flexible approach is critical to ensuring rights requests can be exercised in practice for data held by processors.[10]

C. The Draft Rules Should be Revised to Reflect the Role of Processors in Fulfilling Consumer Rights Requests

Even though the CPA's statutory text permits processors to adopt a range of technical and organizational measures to assist controllers in responding to consumer rights requests, the Draft Rules are far narrower. Most concerningly, the Draft Rules appear to assume that controllers will simply forward consumer rights requests to processors one-by-one. They do not account for a processor's ability to create scalable tools that controllers can use to fulfill consumer rights requests for data held by processors.

We strongly recommend revising the Draft Rules to support scalable approaches to fulfilling consumer rights requests, which will help ensure consumers can exercise those rights in practice.

Consumers should exercise the new rights given to them in the CPA, including the rights to access, correct, and delete information. To make those rights meaningful, however, companies need to be able to respond quickly and efficiently — which often requires creating scalable processes that companies can use to respond to large volumes of requests. For example, a single processor will often serve hundreds or more business customers, each of which acts as a controller of personal data under the CPA. To ensure those business customers can execute consumers requests to access, correct, and delete information held by the processor, a processor can create a scalable tool for the controller to use to access, correct, and delete information in the processor's system. These tools may take a variety of forms, such as dashboards or self-service portals, and assist controllers in responding to large volumes of requests quickly and effectively. Without such scalable tools, controllers may be forced to forward large amounts of consumer rights requests to processors one-by-one. That can create a backlog of requests, slowing down response times and creating the potential for many back-and-forth communications between the two companies about whether each request should be fulfilled.

The Draft Rules do not fully account for — and at times contradict — the statute's clear recognition that processors may establish a range of "technical and organizational measures" to assist a controller in responding to consumer rights requests, including these scalable tools. Instead, the Draft Rules take the far narrower approach of requiring a controller to either "instruct" or "notify" a processor about a consumer rights request — without anticipating that the controller may be able to use a scalable tool to execute requests itself, even for data held by a processor. Specifically:

- **Draft Rule 4.05A** addresses correction requests and states that a controller is to "instruct all Processors that maintain the Personal Data at issue to make the necessary corrections in their respective systems and to ensure that the personal data remains corrected."

- **Draft Rule 4.06A** addresses deletion requests and states that a controller is to comply with requests by "[n]otifying the Controller's Processors and Affiliates to delete the Consumer's Personal Data obtained from the Consumer."

- **Draft Rule 4.09C** addresses compliance with consumer rights requests broadly, stating that "[w]hen

[10] For more information on a processor's role in consumer rights requests, *see* BSA, Consumer Rights to Access, Correct and Delete Data: A Processor's Role, available at https://www.bsa.org/files/policy-filings/10122022controllerprorights.pdf and attached to this submission.

a controller complies with a Consumer's Personal Data Right request, the Controller shall also notify all Processors that Process the Consumer's Personal Data of the Consumer's request and the Controller's response."

These measures do not reflect the CPA's statutory text, which permits processors to adopt a broader range of measures to assist controllers in handling large volumes of requests.

Recommendation. We strongly recommend revising these provisions to better reflect the statutory text's recognition that processors are to assist controllers by providing "technical and organizational measures" to help the controller in fulfilling its obligation to respond to consumer rights requests. We recommend:

- **Revising Draft Rule 4.05A to state:**

  A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data across all data flows and repositories and implementing measures to ensure that the Personal Data remains corrected. The Controller shall also use the technical and organizational measures established by its ~~instruct all~~ Processors that maintain the Personal Data at issue to make the necessary corrections in their respective systems and to ensure that the Personal Data remains corrected.

- **Revising Draft Rule 4.06A to state:**

  A Controller shall comply with a Consumer's deletion request by:

  1. Permanently and completely erasing the Personal Data from its existing systems, except archive or backup systems, or De-Identifying the Personal Data in accordance with C.R.S. 6-1-1303(11); ~~, and~~

  2. Using the technical and organizational measures established by its Processors to delete the Consumer's Personal Data held by the Processors; and

  3. Notifying the Controller's ~~Processors and~~ Affiliates to delete the Consumer's Personal Data obtained from the Controller.

- **Revising Draft Rule 4.09C to state:**

  When a Controller complies with a Consumer's Personal Data Right request, the Controller shall also use the technical and organizational measures established by its Processors to fulfil requests for Personal Data held by the Processors. ~~notify all Processors that Process the Consumer's Personal Data of the Consumer's request and the Controller's response~~

II. Universal Opt-Out Mechanisms

BSA appreciates that the CPA 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. We also support the Draft Rules' recognition that companies should know which universal opt-out mechanisms meet the CPA's requirements — including by establishing a system for recognizing universal opt-out mechanisms. We encourage your office to continue focusing on the practical issues likely to arise as universal opt-out mechanisms are implemented. Our comments highlight three practical issues:

Operationalizing the List of Universal Opt-Out Mechanisms. We support the Draft Rules' recognition that there should be a system for recognizing the universal opt-out mechanisms that meet CPA's

requirements. We therefore encourage you to retain the requirement for the Colorado Department of Law to maintain a public list of mechanisms that have been recognized to meet this standard. At the same time, the Draft Rules do not explain important elements about how the list will be created, including: (1) the process for determining which mechanisms will be placed on that list, (2) a process for receiving stakeholder input on potential mechanisms, and (3) how often the "periodic updates" to the list will be issued. We strongly suggest considering these practical issues, including by:

- *Creating a clear process for developing the public list of universal opt-out mechanisms*. This process should include seeking stakeholder input before recognizing new mechanisms. For example, the process could include setting a deadline for developers of opt-out mechanisms to seek recognition, then either a public comment period or stakeholder workshop soliciting feedback on the proposed mechanisms, before any mechanism is placed on the public list. Such a process would have the benefit of providing a broader set of information on which to base decisions about whether an opt-out mechanism meets the CPA's requirements than a process lacking stakeholder input. For example, stakeholders may have insight on whether a proposed mechanism is interoperable with mechanisms recognized in other states or if a mechanism may create security concerns. These and other considerations may bear on the factors to be considered in determining which mechanisms to recognize under the Draft Rules.

- *Consider specifying a limit for the periodic updates to the list of universal opt-out mechanisms*. The Draft Rules anticipate that the public list of universal opt-out mechanisms will be updated periodically. We encourage your office to consider specifying a limit on how often any such updates may be issued, such as no more than once per year. Creating a regular schedule for any periodic updates can help companies develop regular processes for implementing new mechanisms and devoting their engineering and other resources accordingly.

Ensuring appropriate time for companies to implement newly-recognized universal opt-out mechanisms. For both the initial list and any subsequent updates, we strongly encourage you to ensure there is an appropriate implementation period between the date a mechanism is added to the public list of universal opt-out mechanisms and the date on which companies are to comply with that mechanism. 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. For example, many enterprise software companies rely on regular design cycles to update the design and coding of their products and services; these cycles are generally on set intervals of six months, nine months, twelve months, or eighteen months. Although smaller updates may sometimes be deployed outside of these regular cycles, larger changes are built into a company's products and services through these established processes. To the extent that Colorado recognizes more than one universal opt-out mechanism, implementation becomes even more time-intensive, because companies may either need to design a solution that implements multiple mechanisms or identify multiple design changes needed to implement each mechanism.

The Draft Rules currently anticipate giving companies only three months between identifying a universal opt-out mechanism (on April 1, 2024) and requiring companies to honor that mechanism (on July 1, 2024). *We strongly recommend providing companies nine to twelve months to implement a universal opt-out mechanism — meaning the initial list of mechanisms should be published no later than October 1, 2023.*

Create Additional Mechanisms for Stakeholder Feedback. Because the CPA's requirement to honor universal opt-out mechanisms will impose a new obligation on a range of companies, it is important for the Attorney General's office to ensure the mechanisms functions in practice. We strongly suggest creating opportunities for stakeholder feedback as universal opt-out mechanisms are adopted, such as through stakeholder listening sessions held after the obligation to honor universal opt-out mechanisms takes effect or by undertaking an agency report on these issues. Seeking additional stakeholder

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

feedback can provide important information about whether universal opt-out mechanisms are working as intended.

* * *

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

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

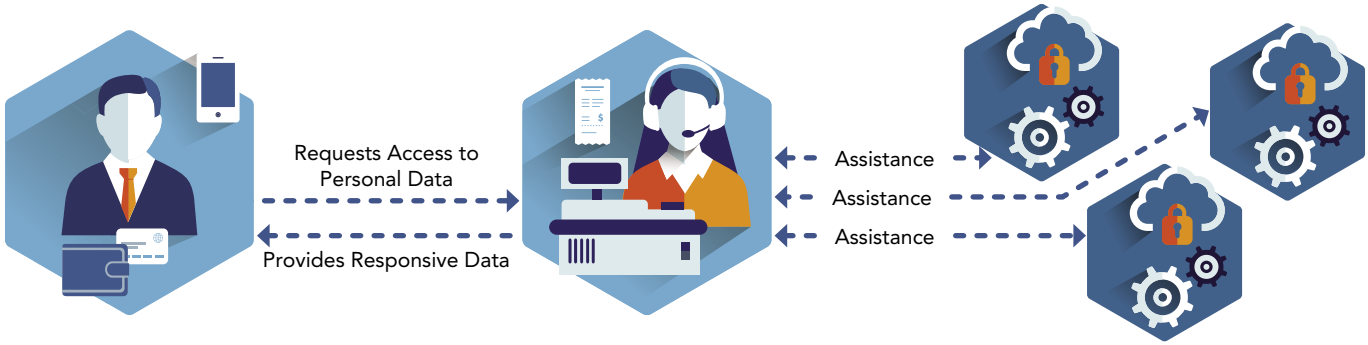
P 202-872-5500
W bsa.org

Consumer Rights to Access, Correct and Delete Data: A Processor's Role

Privacy laws create important new rights for consumers, including the rights to access, correct, and delete their personal data. These rights must function in practice—including when companies rely on processors to help them provide products and services to consumers.

All five state consumer privacy laws in the US and leading privacy laws worldwide adopt the same structure: requiring consumers to submit requests to the company that decides how and why to process the consumers' data (i.e., the company acting as the controller of the data) and then requiring that company to work with processors that handle data on its behalf (e.g., service providers) to fulfill requests for data held by those processors. This structure is critical to ensuring that consumer rights work in practice.

How it Works: A Consumer's Request to Access Personal Data



CONSUMER

Submits request to access, correct, or delete personal data.

CONTROLLER

Responds to the request, including by working with its processors to execute requests involving data held by the processors.

This obligation falls on the controller, because that company decides how and why to process consumers' data—including by hiring processors to handle the data on its behalf. Each controller may rely on dozens or more processors to provide the products and services it offers to consumers.

PROCESSORS

Play an assisting role. A processor's job is to help a controller fulfil the controller's obligation to respond to consumer requests for data held by the processor.

Different Responsibilities for Controllers and Processors Reflect Their Different Roles

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide how and why to collect consumers' data, which act as controllers of that data, and (2) businesses that process the data on behalf of a controller and pursuant to its instructions, which act as processors of that data.

In California, the state privacy law refers to these companies as businesses and service providers, while Colorado, Connecticut, Utah, and Virginia all use the terms controller and processor. Privacy laws should impose strong obligations on both controllers and processors to safeguard consumers' personal data—but those obligations must reflect the different roles these companies have in processing consumers' information. Consumer-facing obligations, like responding to consumer rights requests, are appropriately placed on controllers, which decide how and why to process consumers' personal data.

WHY PLACE THIS OBLIGATION ON CONTROLLERS?

All five state privacy laws recognize that controllers—which decide how and why to process a consumer's data—should have the obligation to respond to consumer rights requests. This is because a controller:

- Decides how and why to collect consumers' data
- Typically interacts with consumers
- Makes important decisions required to fulfill a rights request, including:
  - what data sets to provide to its consumers in response to an access request;
  - whether data sought to be corrected is actually inaccurate; and
  - if other statutory exceptions apply—like whether data should not be deleted because it is subject to a legal hold.

WHY NOT REQUIRE PROCESSORS TO RESPOND TO CONSUMERS?

All five state privacy laws require processors to assist a controller in responding to rights requests. They do not require processors to respond directly to consumers, because a processor:

- Does not typically interact with consumers—and may be unable to confirm the identity of a person submitting a rights request.
- Does not make the decisions required to respond to a rights request. For example, a processor that stores data for other companies (like a cloud service provider) would generally not know:
  - what data sets each business customer provides to its consumers in response to an access request;
  - whether data sought to be corrected is actually inaccurate; or
  - if other statutory exceptions apply—like whether data should not be deleted because it is subject to a legal hold.

How to Assist? State Laws Recognize Two Options for Processors

Under all five state privacy laws, processors can fulfil their obligation to assist a controller in responding to consumer rights requests in either of two ways:

- **First, a processor can respond one-by-one to requests from the controller to provide information in response to each request the controller receives.** This option requires the companies to communicate about each request—and ensure that the controller has determined that no exception to the request applies and that the controller has specified what information should be provided, corrected, or deleted in response to the request. As a result, this one-by-one approach becomes more difficult with higher volumes of consumer rights requests.
- **Second, a processor can create a scalable tool that the controller can use to respond to requests.** This allows the companies to create an efficient approach to fulfilling large volumes of consumer rights requests seeking data held by processors. For example, a cloud service provider may create a dashboard that its business customers can use to pull information sought by consumer access requests, or to execute requests to correct or delete personal data held by the processor. This creates a streamlined approach to fulfilling to large amounts of consumer rights requests, without the need for back-and-forth communication about each individual request.