December 20, 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 implement the Colorado Privacy Act (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. This letter supplements our Nov. 7 written comments and the feedback BSA provided during the Nov. 10 virtual stakeholder session.[2] We address five issues not included in our prior feedback:

- Sensitive Data Inferences;
- Organizing Privacy Notices Around Processing Purposes;
- Data Protection Assessments;
- Profiling; and
- Consistency with the CPA's Statutory Text.

[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.

[2] *See* BSA Comments on Draft Rules to Implement the Colorado Privacy Act, Nov. 7, 2022, *available at* https://www.bsa.org/files/policy-filings/11072022coagpriv.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

In addition, the last two sections of this letter contain our recommendations on two issues that were the focus of BSA's prior comments:

- The Role of Processors in Fulfilling Consumer Rights Requests
- Practical Issues in Implementing Universal Opt-Out Mechanisms

On each issue, we have provided specific recommendations for revising the Draft Rules. We are also attaching a document containing our recommendations in the form of a redline.

I. Importance of Colorado Privacy Act

At the outset, we want to recognize that the CPA will create strong new privacy protections for consumers. The statute creates new high-water marks for companies handling personal data, including providing consumers with new ways to exercise rights over their personal data, clearly requiring companies to honor universal opt-out mechanisms, expressly prohibiting companies from obtaining consent based on dark patterns, and extending the statute's protections to nonprofit organizations. These requirements will add to consumer privacy protections included in other state privacy laws, creating additional safeguards on companies that collect and use consumers' personal data.

BSA supported the CPA's passage and we have applauded its sponsors for creating a bill that sets a strong new model for protecting consumer privacy.[3] Consumers today share their personal data with countless businesses in the course of using everyday products and services, both online and offline. Consumers deserve to know their personal data is being used responsibly. We appreciate the work of both the Colorado legislature and the Colorado Attorney General's Office in strengthening consumer privacy protections by enacting and implementing the CPA.

While our comments on the Draft Rules address a range of topics, we encourage your office to prioritize provisions of the Draft Rules addressing the CPA's key requirements. Specifically, we encourage you to prioritize the Draft Rules' treatment of universal opt-out mechanisms, which create a long list of practical and technical issues that companies must address. There are 18 months before the CPA's obligation to honor universal opt out mechanisms takes effect — and we encourage your office to promptly finalize the Draft Rules addressing universal opt-out mechanisms as well as the public list of mechanisms that companies will be required to honor, so that companies can understand their obligations and begin adopting technical mechanisms to implement them. Indeed, the CPA recognizes this issue is both important and time-consuming to operationalize, because it is the *only* topic on which the statue specifically requires the Attorney General's office to issue rules. The CPA also delays the requirement for companies to comply with universal opt-out mechanisms until July 1, 2024, a full year after the remainder of the statute takes effect. The more time companies have to implement these obligations, the better they can integrate the necessary changes into established processes for updating products and services and ensure those products are designed with privacy in mind. That approach also creates more thorough compliance practices for companies and better outcomes for consumers than if companies must rush to comply with new obligations shortly before a statutory deadline.

More broadly, our comments also focus on a range of topics on which the Draft Rules appear to depart from both the CPA's text and the approach that leading international privacy laws take on similar issues. BSA members have extensive experience with protecting personal data in compliance with data protection and privacy laws across the globe and we would welcome an opportunity to further discuss with your office how the Draft Rules' approach to these issues either align with or diverge from privacy and data protection laws adopted worldwide.

[3] *See* BSA Applauds Passage of Colorado Privacy Act, June 8, 2021, *available at* https://www.bsa.org/news-events/news/bsa-applauds-passage-of-colorado-privacy-act.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

II. Issues Not Addressed in Previous BSA Comments

We recommend revisions to a range of provisions in the Draft Rules, including five areas not addressed in BSA's prior comments. For each area, we have provided specific recommendations for revising the text of the Draft Rules. We are also attaching a redline that reflects those recommendations.

a. Sensitive Data Inferences

The Draft Rules address "sensitive data inferences" but provide little clarity around this term.

Under the Draft Rules, the definitions of both "sensitive data inferences" and the related term "revealing" appear intended to treat information as a sensitive data inference only when the information is *actually used* to infer sensitive personal data about an individual — rather than when the information merely *could be used* to infer sensitive personal data. That reflects the reality that information actually used to infer sensitive data is itself sensitive. We suggest several edits to clarify this result in the Draft Rules.

If these terms are not clarified and are instead read broadly to capture information from which sensitive data *could be inferred* rather than information from which sensitive data is *actually inferred*, this term would sweep in a much broader range of information. That broad approach would create at least two concerning results that undermine the CPA's goal of increasing consumer privacy protections:

- *First*, treating information as a "sensitive data inference" if it merely *could be used* to infer sensitive personal data about an individual can create incentives to process more sensitive data about consumers. If information is treated as sensitive regardless of whether it is *actually* used to infer sensitive personal information about an individual, there are few incentives for companies not to make sensitive inferences when they have information capable of doing so. Conversely, clarifying that information is only a "sensitive data inference" if it is *actually* used to indicate sensitive personal data creates the opposite incentive — and encourages companies to limit the amount of sensitive personal data they infer about individuals, even if they have information capable of inferring sensitive personal data about their consumers. Clarifying the narrow definition of this term therefore creates better incentives to protect consumer privacy.

- *Second*, reading the definition of "sensitive data inference" broadly could greatly increase the number of consent requests that consumers receive. Clarifying that information is only a "sensitive data inference" when it is *actually used* to infer sensitive personal information helps to reduce such consent requests — but still ensures consumers are asked for consent when their information is used to infer sensitive personal information about them. We appreciate that Section 6.10.B sets out rules intended to limit consent requests for the collection and use of sensitive data inferences. At the same time, there may not be a need to create different consent rules for sensitive personal data and sensitive personal data inferences if the Draft Rules are revised to clearly state that information is only a sensitive data inference when it is *actually used* to infer sensitive personal data. This approach also helps to achieve the result that appears to be intended by the Draft Rules: preventing companies from sidestepping the CPA's consent requirements by collecting information about a consumer without consent and then using that information infer sensitive personal data that would otherwise require consent.

We strongly recommend clarifying the Draft Rules to emphasize that information is a sensitive data inference when it is *actually used* to infer sensitive information about an individual.

Recommendations: We recommend clarifying the definitions of both "Revealing" and "Sensitive Data Inferences" and also revising Section 6.10, which applies these terms.

1. ***Draft Rule 2.02's definition of Revealing should be revised.*** The examples included in the definition of "revealing" should be revised to more clearly reflect that a sensitive data inference is one *actually used* to indicate sensitive data. We recommend revising the second example to state:

> While web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, creates a profile that is used to indicate~~s~~ an individual's sexual orientation ~~and~~ is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

2. ***Draft Rule 2.02's definition of Sensitive Data Inference should be revised***. This definition should be revised to more clearly reflect that a sensitive data inference is one *actually used* to indicate sensitive data. We recommend revising the definition to state this term:

> means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status

3. ***Draft Rule 6.10.B should be revised.*** This provision creates consent exceptions for sensitive data inferences. We suggest reconsidering whether this section is necessary. If the definitions are revised in line with our recommendations above, to clearly state that information is only a sensitive data inference when it is *actually used* to infer sensitive personal data, there may not be a need to create separate consent obligations for sensitive personal data inferences.

4. ***Draft Rule 6.10.B.3 should be either deleted or, alternatively, revised.*** If Section 6.10.B is retained, we suggest revising Section 6.10.B.3 to focus on transferring data to third parties, rather than to processors. Under the CPA, processors are subject to a range of safeguards that ensure they handle data in line with a controller's instructions. Sharing with processors therefore does not create the privacy risks intended to be addressed by this provision, which should instead focus on third parties. We recommend revising Draft Rule 6.10.B.3 to state:

> The Personal Data and any Sensitive Data Inferences are not transferred, sold, or shared with any ~~Processors, Affiliates, or~~ Third-Parties; and

b. Requirement to Organize Privacy Notices Around Processing Purposes

The Draft Rules take a new approach to privacy notices. In doing so, the Draft Rules diverge from other state privacy laws and from industry standards by requiring privacy notices be organized around each purpose for which personal data is processed. We recommend reconsidering this approach, which may counterproductively lead to longer privacy policies instead of clearer notices to consumers.

Under the Draft Rules, a controller would be required to identify *each purpose for which it processes personal data* — and then list five types of information about data processed for each of those purposes, including the categories of personal data processed for that purpose, the categories of personal data that the controller sells or shares for that purpose, and the categories of third parties to whom the controller sells or shares personal data for that purpose. We have three concerns with this approach:

- *First*, these requirements will lead companies to create even longer privacy policies. For example, if one company processes personal data for 12 different purposes, it would be required to create a new privacy policy listing those 12 purposes and — for each purpose — providing a list of five types of information. That adds up to at least 60 required disclosures, since this format prevents companies from combining similar disclosures. The result is duplicative, and extremely long, privacy notices to consumers. This format also departs from the way that many companies structure their existing privacy policies, which focus on the types of information a company

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

collects and uses, the types of entities with which they share personal information, instructions on how individuals may exercise rights in their personal data, and other information such as the security measures a company adopts to safeguard personal data and how an individual may contact the company. Even for companies that strive to make those disclosures as clear and succinct as possible, doing so remains challenging. The new format in the Draft Rules would create additional challenges, rather than additional clarity.

- *Second*, the new format may lead to companies to create a separate Colorado-specific privacy policy. As a result, companies may have both a main privacy policy that applies to multiple jurisdictions and a separate policy only for Colorado residents. That may not only confuse consumers, but also fragment a company's efforts to update and maintain its privacy policies. When companies have a single privacy policy that applies across jurisdictions, they can focus resources on maintaining and updating the single policy. Spreading those resources among multiple privacy policies fragments those compliance efforts. It is also not clear that creating separate privacy policies meaningfully advances consumer privacy, since it may simply result in more — and longer — privacy policies for consumers to sort through from each company.

- *Third*, this format appears in tension with the CPA's text, which does not suggest that notices are to be structured around processing purposes. Section 6-1-1308 of the CPA requires controllers to provide consumers with a "meaningful privacy notice" that includes five types of information. Those are: (1) the "categories of personal data collected or processed"; (2) the "purposes for which the categories of personal data are processed"; (3) how and where consumers may exercise their new rights; (4) the "categories of personal data that the controller shares with third parties, if any"; and (5) the "categories of third parties, if any, with whom the controller shares personal data." There is no indication in the statute that privacy notices should be structured around the purpose for which data is processed. Rather, those purposes are simply one of five types of information required to be in a privacy notice. Indeed, structuring a privacy notice around the purpose for which personal data is processed may prevent companies from succinctly disclosing other information the CPA requires be included in an assessment, including the categories of personal data collected or processed, the categories of personal data shared with third parties, and the categories of third parties with whom personal data is shared. For these types of information, the CPA requires companies to make disclosures by category — rather than dividing those disclosures by processing purpose.

Recommendation: Section 6.03 should be revised to avoid requiring companies to organize privacy notices around each processing purpose.

c. Data Protection Assessments

Data protection assessments are an important component of data protection programs. BSA has supported a range of state privacy laws that require controllers to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks that may arise from those activities and to adopt appropriate mitigation measures. We appreciate the Draft Rules' recognition that data protection assessments can be important accountability mechanisms, but strongly encourage revising the Draft Rules' approach to data protection assessments for two reasons.

- *First*, we recommend revising the Draft Rules to promote the use of data protection impact assessments across jurisdictions and to avoid applying CPA-specific documentation requirements. In many cases, companies have already established processes for conducting and documenting privacy-related risk assessments, including under global privacy laws like the EU's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD). We appreciate the Draft Rules' recognition in Section 8.02.B that when a controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulations, it may also satisfy the CPA's obligations. However, in practice the level of

detail in the Draft Rules makes it impractical for many companies to use assessments conducted in other judications to satisfy those obligations — because the Draft Rules impose a range of Colorado-specific requirements that diverge from international requirements. For example. a data protection impact assessment conducted to comply with EU obligations is required to address four topics under GDPR Article 35.7. In contrast, the Draft Rules list a minimum of 18 topics to be addressed by a data protection assessment, creating a specific checklist that is far more granular than leading global standards. As a practical matter, companies may therefore be required to conduct Colorado-specific assessments unless the Draft Rules are revised.

- *Second*, the Draft Rules' detailed requirements are at odds with the CPA's language, which already addresses the content of data protection assessments. Section 6-1-1309(3) of the CPA states that assessments are to "identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that the controller can employ to reduce the risks." These statutory obligations reflect the content of data protection assessments conducted in other jurisdictions. Moreover, the statute already adds to those global obligations by imposing a targeted set of Colorado-specific obligations: requiring controllers to factor into the assessment the use of de-identified data and the reasonable expectation of consumers, as well as the context of the processing and the relationship between the controller and the relevant consumer. The Draft Rules go well beyond implementing these statutory requirements and instead adopt new requirements that create tension with the CPA's text.[4]

Recommendation. Part 8 of the Draft Rules should be revised to require data protection assessments that align with the CPA's requirements, rather than requiring companies to address each of 18 topics identified in the Draft Rules. Revising the Draft Rules' obligations on data protection assessments to more closely align with the CPA's text will also help to ensure that companies devote resources to data protection assessments that can be leveraged across jurisdictions. Specifically, we recommend:

1. ***Draft Rule 8.04.A.3 should be revised to focus on the "types" of Personal Data to be processed, rather than the "specific types" of personal data***. This revision would help to clarify that companies can conduct risk assessments that focus on a category of personal data without conducting a risk assessment on each type of personal data that may fall into that category.

2. ***Draft Rule 8.04.A.6 should be revised to focus on the categories of third parties, affiliates, and processors that will have access to personal data, rather than specific names***. Rather than requiring controllers to identify processors by name and assess risks posed by a specific processor, a data protection assessment should focus on categories of processors (e.g., cloud service providers, communications platform providers) and encourage controllers to assess the risks associated with engaging that category of processor — which will also help ensure the controller adopts measures that mitigate risks across processors, rather than creating mitigation measures that may only work for one processor. A single controller may rely on dozens or more processors; if an existing processor is no longer able to serve that controller (e.g., it suffers a data breach or stops providing a certain service) the controller will need to hire a new processor to replace it. Requiring a data protection assessment to identify the name of each processor is at odds with this business reality and fails to focus controllers on adopting safeguards that apply across different processors that may perform the same function.

[4] Of the 18 topics the Draft Rules require a data protection assessment to include, only three appear to align with the CPA's text: (1) Draft Rule 8.04.A.7, which requires the assessment to take into account the "relationship between the Controller and the Consumer(s) whose Personal Data will be Processed"; (2) Draft Rule 8.04.A.8, which is largely aligned with the statute but focuses on "expectations" of consumers rather than "reasonable expectations"; and (3) Draft Rule 8.04.A.15, which is also largely aligned with the statute but differs from the CPA's text in important ways.

3. ***Draft Rule 8.04.A.8 should be revised to focus on the "reasonable expectations" of consumers, rather than their "expectations."*** This recommendation brings the language closer to the statutory text in the CPA, which requires a controller to "factor into" a data protection assessment "the reasonable expectations of consumers."[5] We suggest revising Draft Rule 8.04.A.8 to state: "The reasonable expectations of the Consumer(s) concerning how their Personal Data will be used, including expectations based on privacy notices, Consent disclosures and unique vulnerabilities."

4. ***Draft Rule 8.04.A.9 should be deleted***. This provision would require a data protection assessment to include descriptions of how a controller will request consent under the CPA, provide opt-out rights under the CPA, and describe how the controller will review web interfaces for potential dark patterns. Including these Colorado-specific provisions significantly limits the ability of companies to leverage privacy assessments they have conducted in other jurisdictions to satisfy obligations under the CPA.

5. ***Draft Rule 8.04.A.11 should be revised to focus on the risks identified in the CPA's statutory text***. Specifically, the CPA's obligation to conduct a data protection assessment is triggered by processing that "presents a heightened risk of harm to a consumer." Draft Rule 8.04.A.11 creates a separate list of risks, which do not align with the statute's definition of "heightened risks." We recommend revising this provision to align with the risks identified in the statute, rather than creating a new set of risks for controllers to consider.

6. ***Draft Rule 8.04.A.14 should be deleted***. This provision would require a data protection assessment to address Colorado-specific requirements around sensitive data inferences. As noted above, we suggest reconsidering whether these requirements serve the broader purposes of the CPA. Even if those substantive requirements remain in the Draft Rules, however, requiring them to be addressed in a data protection assessment further limits the ability of companies to leverage privacy assessments conducted in other jurisdictions to satisfy obligations under the CPA.

7. ***Draft Rule 8.04.A.15 should be revised to mirror the CPA's statutory text***. This provision is similar to the CPA's requirement that a data protection assessment must "identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that the controller can employ to reduce the risks." However, the Draft Rules deviate from this statutory language in important ways, such as by dropping the reference to benefits that flow "directly and indirectly" and eliminating the consideration of benefits "to the public" more broadly. This statutory language is the cornerstone of the CPA's obligation to conduct data protection assessments. We strongly recommend revising the Draft Rules to apply the statutory obligation directly, without the linguistic differences currently reflect in Draft Rule 8.04.A.15.

d. Profiling

The Draft Rules contain significant obligations for controllers that engage in profiling, which is defined by the CPA as "any form" of automated processing of personal data "to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." The CPA creates two obligations for companies engaged in profiling. First, it creates a right for consumers to opt out of profiling. Second, it creates an obligation for companies that engage in profiling to conduct data protection assessments when the profiling presents a "reasonably foreseeable risk" of four types of harm.

[5] *See* CPA Sec. 6-1-1309(3).

The Draft Rules build on these statutory obligations by: (1) creating new transparency requirements (in Draft Rule 9.03), to "ensure that Consumers understand how their Personal Data may be used for Profiling"; (2) clarifying when the right to opt out of profiling applies (in draft Rule 9.04 and 9.05), by distinguishing between "human involved automated processing" and "human reviewed automated processing," and (3) creating detailed requirements around data protection assessments on profiling activities, including specifying 12 topics that must be included in such assessments, in addition to the 18 topics required in all data protection assessments under Draft Rule 8.04. Our comments focus on this third requirement.

For processing that involves profiling, the Draft Rules appear to require controllers to conduct data protection assessments that include not only the 18 topics in Draft Rule 8.04, but also 12 new topics contained in Draft Rule 9.06A.F. These additional topics include the benefits of automated processing over manual processing, an explanation of the training data and logic used to create the profiling system, the name of any software used and copies of any internal or external evaluations of its accuracy and liability, the degree and details of human involvement, how the profiling system is evaluated for fairness and disparate impact along with the results of any such evaluations, and safeguards for any data sets produced by or derived from the profiling. In addition, Draft Rule 8.05.C requires data protection assessments for profiling be refreshed "at least annually" and include an "updated evaluation for fairness and disparate impact." As with the data protection assessment obligations contained in Draft Rule 8.04, these profiling-specific obligations appear to exceed the data protection assessments envisioned by the CPA. We recommend revising Draft Rule 9.06 to align with the CPA's broader obligations.

Recommendations:

- ***Rule 9.06.F.1 should be deleted***. This provision would require data protection assessments to identify the "specific types of Personal Data" used in profiling or decision-making processes. We recommend deleting it, because it duplicates requirements already imposed on all data protection assessments under Draft Rule 8.04.A.3. If this provision is retained, however, we recommend revising it to focus on "types" of personal data that were or will be used, rather than "specific types" of such data, in line with our comments on Draft Rule 8.04.A.3.

- ***Draft Rule 9.06.F.2 should be deleted***. This provision refers to "automated decision-making systems" which are not the focus of the CPA. The CPA instead focuses on "profiling," which it defines as "any form of automated processing of personal data to evaluate, analyze or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." We recommend deleting this provision, which goes beyond the CPA.

- ***Draft Rule 9.06.F.3 should be deleted***. This provision would require companies to address the benefits of automated processing over manual processing for the stated purpose. However, this weighing of risks and benefits is already required for all data protection assessments under Draft Rule 8.04.A.15 (requiring companies to address "benefits" of processing) and Draft Rule 8.04.A.10 (requiring companies to identify alternative processing activities). We therefore recommend deleting this duplicative requirement.

- ***Draft Rule 9.06.F.5 should be deleted or, alternatively, revised***. This provision would require controllers to include an explanation of the training data and logic used to create the profiling system. However, if the controller has purchased an AI-based system from a separate company that developed it, the controller may have limited information about the training data and logic used to create that system. Requiring controllers that deploy AI-based systems to assess the training data conflates the distinct roles of companies that develop and deploy those systems. We therefore recommend deleting this requirement. Alternatively, if the provision is retained, we recommend it be revised to reflect that a controller may have limited insight into this information. Specifically, we recommend revising the text to state: "When reasonably available to the Controller, information that

explains ~~An explanation of~~ the training data and logic used to create the Profiling system, ~~including any statistics used in the analysis, when available~~."

e. Ensuring Consistency with CPA's Statutory Text

The CPA empowers the Attorney General to promulgate regulations "for the purpose of carrying out" the statute. However, there are several areas of the Draft Rules that appear to go beyond the statute's text. We suggest revising these aspects of the Draft Rules to avoid creating regulations that either exceed the statute or conflict with the statute's requirements. These include:

Timing for responding to opt-out requests. Draft Rule 4.03.A.1 states that a controller is to respond to an opt-out request no later than 15 days after receipt. That obligation conflicts with the CPA's statutory text, which clearly states that controllers should inform consumers of actions taken on their request "without undue delay and, in any event, within forty-five days after receipt of the request."[6] The statute imposes this timeline on both opt-out requests and on requests to access, correct, delete, and port a consumer's personal data. The Draft Rules should be revised to adopt the statute's clear language.

- **Recommendation**: Draft Rule 4.03.A.1 should be revised in line with the CPA's text, to state that a Controller shall comply with an opt-out request by "Ceasing to Process the Consumer's Personal Data for the Opt-Out Purpose(s) without undue delay ~~as soon as feasibly possible~~, but no later than forty-five ~~fifteen~~ (~~1~~45) days from the date the Controller receives the request, unless an extension is sought pursuant to C.R.S. 6-1-1306(2)(a)."

Disclosure of third parties with which data is shared. While the CPA requires companies to disclose the *categories* of third parties with which data is shared, in several places the Draft Rules appear to require controllers to disclose the *names* of those third parties. Specifically, Draft Rule 7.03.E.e would require controllers to disclose the names of third parties and affiliates that would receive sensitive personal data in requesting consent to process that data. Similarly, and as noted above, Draft Rule 8.04.A.6 would require data protection assessments to include the names of third parties, affiliates and processors that have access to personal data.

- **Recommendation**: Draft Rule 7.03.E.1.e should be revised to state: "Categories of all third parties who will have access to the Personal Data~~, and names of all Third Parties and Affiliates receiving the Sensitive Data~~ through Sale or sharing. Names of Processors, as defined in C.R.S. 6-1-1306(19) are not required; and"

Requirements to refresh consent. Draft Rule 7.08 requires controllers to "refresh" consent at "regular intervals" based on the context and scope of the original consent, sensitivity of the personal data collected, and the reasonable expectations of the consumer. For sensitive data, consent must be refreshed at least annually. These obligations do not appear in the CPA. Rather, the Draft Rules prioritize consent-based safeguards on data protection above other forms of safeguards included in the CPA. The CPA recognizes that consent is one important safeguard in processing consumers' personal data — and we fully support requiring consent when companies process sensitive data, as required by the CPA. However, the Draft Rules have the potential to exponentially increase the amount of consent requests that consumers receive, which may lead to more consumer fatigue and frustration with repeated consent requests. Rather than taking the CPA's approach of focusing consent requests on sensitive or unexpected practices, the Draft Rules may cause consumers to pay less attention to consent requests because they will receive more of them. That does not further consumer privacy.

- **Recommendation**: Draft Rule 7.08 should be deleted.

[6] *See* CPA, Sec. 6-1-1306(2) (stating a controller "shall inform a consumer of any action taken on a request under subsection (1) of this section [creating opt-out rights and rights to access, correct, delete, and port personal data] without undue delay and, in any event, within forty-five days after receipt of the request.").

Documentation obligations for data minimization, secondary uses, and individual rights requests. The Draft Rules impose significant new documentation obligations not found in the CPA's text. Specifically: (1) Draft Rule 6.07.A requires controllers to document assessments of their data minimization obligations; (2) Draft Rule 6.08.D requires controllers to document assessments of certain secondary uses; and (3) Draft Rule 6.11.A-B require controllers to maintain records of consumer rights requests. These obligations are not found in the CPA's text — despite the statute's recognition that controllers should conduct and document data protection assessments, which the statute anticipates focusing on the benefits, risks, and mitigation measures related to processing that constitutes a heightened risk of harm. Creating new documentation requirements goes well beyond the CPA.

- **Recommendation**: We recommend revising all three documentation obligations.

  Draft Rule 6.07.A should be revised to delete the documentation requirement. We recommend revising the language to state: "To ensure all Personal Data collected is reasonably necessary for the specified purpose, Controllers shall carefully consider each Processing purpose and determine the minimum Personal Data that is necessary, adequate, or relevant for the express purpose or purposes. ~~Such assessment shall be documented according to 4 CCR 904-3, Rule 6.11.~~"

  Draft Rule 6.08.D should be deleted.

  Draft Rule 6.11.B should be revised, ***including to avoid the implication that controllers should indefinitely retain all consumer rights requests***. We recommend revising the language to state: "Controllers shall ~~maintain a record of all Data Rights requests made pursuant to C.R.S. § 6-1- 1306 with which the Controller has previously complied. Such records shall be~~ mak~~d~~e available records maintained under Rule 6.11.A at the completion of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data to ensure any new Controller continues to recognize the Consumer's previously exercised Data Rights.

III. Issues Addressed in BSA's Prior Comments

These comments build on the comments that BSA's Nov. 7 comments, which focus on the role of processors in fulfilling consumer rights requests and the importance of addressing practical issues involved in implementing universal opt-out mechanisms. Both issues raise key concerns for BSA members, and we spoke to both issues during the Nov. 10 stakeholder session on consumer rights requests.

We want to reiterate the importance of these issues, which are critical to ensuring new rights given to consumers by the CPA function in practice. We repeat our prior comments below, including our recommended revisions to the Draft Rules. These issues are also addressed in the accompanying redline.

a. 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

1. 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.[7] 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.[8] Indeed, this longstanding distinction has existed for more than 40 years and is fundamental to leading privacy laws worldwide.[9]

BSA also recognizes that processor-specific obligations are important to build consumers' trust that their 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 the state privacy laws recently enacted in Connecticut and Virginia.

2. 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.[10] In response "a controller" is to "inform a consumer" about action taken on those requests.[11] Controllers are also to establish internal processes to allow consumers to appeal denials of such requests.[12]

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."[13]

---

[7] 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).

[8] *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).

[9] *See* BSA, Controllers and Processors: A Longstanding Distinction in Privacy (tracing history of the terms controller and processor and their adoption worldwide), available at https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf.

[10] *See* CPA Sec. 6-1-1306(1) (emphasis added).

[11] *See* CPA Sec. 6-1-1306(2).

[12] *See* CPA Sec. 6-1-1306(3)(a).

[13] *See* CPA Sec. 6-1-1306(2)(a).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

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 GDPR.[14]

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 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.[15]

3. 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

[14] *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.")

[15] 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.

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 4.05.A** 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 4.06.A** 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 4.09.C** addresses compliance with consumer rights requests broadly, stating that "[w]hen 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 three changes:

- ***Draft Rule 4.05.A should be revised 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.

- ***Draft Rule 4.06.A should be revised 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.

- ***Draft Rule 4.09.C should be revised 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~~

b. 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 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