January 18, 2023

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 updated version of the Draft Rules to implement the Colorado Privacy Act (Updated Draft Rules). 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 and we support strong privacy protections for consumers.

This letter updates the comments that BSA provided to your office on December 20, 2022. Because those earlier comments were based on the version of the Draft Rules published prior to the December 21, 2022, revisions, we are sending this letter to reiterate BSA's recommendations and to apply those recommendations to the Updated Draft Rules. Specifically, we focus on:

- Universal Opt-Out Mechanisms;
- Data Protection Assessments;
- Consistency with the CPA's Statutory Text;
- Profiling;
- Sensitive Data Inferences;
- The Role of Processors in Fulfilling Consumer Rights Requests; and
- Privacy Notices.

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.

[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

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.[2] 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.

We encourage your office to prioritize provisions of the Updated Draft Rules that address 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 17 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. The list of opt-out mechanisms should also be updated on a set schedule, so companies can plan their compliance processes accordingly. That approach 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 Updated 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 Updated Draft Rules' approach to these issues either align with or diverge from privacy and data protection laws adopted worldwide.

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 appreciate several changes in the Updated Draft Rules that recognize companies should know which universal opt-out mechanisms meet the CPA's requirements, including through establishing a system for recognizing universal opt-out mechanisms.

We focus on three further recommendations.

First, we strongly urge you to provide more time for companies to implement universal opt-out mechanisms. We appreciate that the Updated Draft Rules provide companies seven months between publication of the initial list and the July 1, 2024, deadline to honor universal opt-out mechanisms. Companies also have six months to implement any mechanisms that are added to the list at a later date.

[2] *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

While this additional time is appreciated, we continue to believe that a longer timeframe for identifying and implementing opt-out mechanisms will create better outcomes for the consumers using these mechanisms. That is because 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. If the public list of mechanisms is issued shortly after a company completes one design cycle, that company may have to implement these mechanisms on an ad-hoc basis — rather than through established practices that can more readily account for privacy and other implications of the new requirements. Indeed, there is widespread recognition that privacy obligations should be designed into a company's products and services — but to implement those privacy-by-design principles, privacy obligations must become part of a company's regular design cycle. Providing companies between nine and twelve months to implement universal opt-out mechanisms maximizes the ability of companies to drive necessary changes through strong, established, and privacy-protective design cycles.

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.

Second, we encourage you to prioritize creating and operationalizing the list of universal opt-out mechanisms. We support the Updated 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 Updated 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) creating a set schedule for "periodic updates" to the list. 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. 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.

  We appreciate that the Updated Draft Rules specifically seek feedback on whether the process for determining which opt-out mechanisms will be recognized should be "fully prescribed" in the rulemaking or if it can be developed later. In our view, the regulations should at minimum specify the framework for determining which opt-out mechanisms will be recognized. For example, the Updated Draft Rules could identify specific steps in that process, which may include setting a deadline for developers of opt-out mechanisms to ask that those mechanisms be considered for inclusion on the list, then providing a specific period of time for staff to review those mechanisms, and allowing for input by stakeholders (including in writing and/or through a public workshop) before a determination is made about whether a mechanism will be placed on the list.

- *Create a set schedule for 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 how often any such updates may be issued, such as no more than once per year. Moreover, the list should be updated on a regular schedule, so that companies can design their compliance practices accordingly. Creating a regular schedule for periodic updates can help companies develop regular processes for

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

implementing new mechanisms and devoting their engineering and other resources to those efforts.

Third, we encourage you to create additional mechanisms for stakeholder feedback on obligations relating to universal opt-out mechanisms after those obligations take effect. 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 these mechanisms function 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.

III. 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 that the Updated Draft Rules make several changes to the regulations' data protection assessment requirements. We strongly encourage further changes, for the two reasons set out in our Dec. 20, 2022, comments.

- *First*, we recommend revising the Updated 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 Updated 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 Updated Draft Rules goes well beyond leading international privacy and data protection laws, which makes it impractical for many companies to use assessments conducted in other judications to satisfy those obligations — since the Updated Draft Rules continue to 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 Updated Draft Rules list a minimum of 13 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 be limited in using assessments conducted under other global privacy laws to satisfy these Colorado-specific requirements.

- *Second*, the Updated Draft Rules' detailed requirements are still 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

The Updated Draft Rules go well beyond implementing these statutory requirements and instead adopt new requirements that create tension with the CPA's text.

Recommendation. Part 8 of the Updated Draft Rules should be further revised to require data protection assessments that align with the CPA's requirements, rather than requiring companies to address each of 13 topics identified in the Updated Draft Rules. Revising the Updated Draft Rules' 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.6 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.6 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.

2. ***Draft Rule 8.04.A.10 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 Updated 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.

3. ***Draft Rule 8.04.A.8 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 Updated 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 Updated Draft Rules to apply the statutory obligation directly, without the linguistic differences currently reflect in Draft Rule 8.04.A.8.

IV. 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 Updated Draft Rules that appear to go beyond the statute's text. We suggest revising these aspects of the Updated 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."[3] 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 Updated Draft Rules should be revised to adopt the statute's clear language.

[3] *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.").

- **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, the Updated Draft Rules appear to require controllers to disclose the *names* of those third parties. Specifically, Draft Rule 7.03.E.1.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. In contrast, the December 21, 2022, revisions updated Draft Rule 8.04.A.4.c to require the "names *or* categories" of companies receiving personal data be included in a data protection assessment. The same change should be made in Draft Rule 7.03.E.1.e.

- **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"

Documentation obligations for data minimization, secondary uses, and individual rights requests. The Updated 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~~ ma~~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.

Security measures. The CPA requires controllers to "take *reasonable measures* to secure personal data during both storage and use from unauthorized acquisition." The Updated Draft Rules go beyond this statutory obligation, requiring that "[r]easonable and appropriate administrative, technical, organizational, and physical safeguards *must*" achieve certain outcomes, including protecting against unauthorized or unlawful access to or use of personal data and ensuring the confidently, integrity, and availability of personal

data. That goes far beyond the CPA's requirement that companies take "reasonable measures" to secure personal data.

> **Recommendation**: Draft Rule 6.09.C should be revised to focus on requiring companies to adopt measures "reasonably designed" to secure personal data. We recommend revising this provision to state: "Reasonable and appropriate administrative, technical, organizational, and physical safeguards must be reasonably designed to:"

V. Profiling

The Updated 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.

The Updated 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 is used for Profiling"; (2) clarifying when the right to opt out of profiling applies (in Draft Rules 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 13 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 Updated Draft Rules appear to require controllers to conduct data protection assessments that include not only the 13 topics in Draft Rule 8.04, but also 12 new topics contained in Draft Rule 9.06.G. 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.G.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.2. If this provision is retained, however, we recommend revising it to focus on "categories" of personal data that were or will be used, rather than "specific types" of such data, in line with the December 21, 2022, revisions to Draft Rule 8.04.A.2.

- ***Draft Rule 9.06.G.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.G.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.8 (requiring companies to address "benefits" of processing and describe how they outweigh identified risks). We recommend deleting this duplicative requirement.

- ***Draft Rule 9.06.G.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~~."

VI. Sensitive Data Inferences

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

Under the Updated 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 Updated 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 Updated 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 Updated 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 Updated 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 reconsidered.*** 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:

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

VII. 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

We appreciate several changes made in the December 21, 2022, revisions that better account for the role of processors in handling consumer rights requests. In our view, these changes will better 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 retaining these changes, which better align the Updated Draft Rules with CPA's approach to this issue. In our view, these changes can help to ensure that consumer rights requests work in practice for data held by processors.

In particular, BSA supports changes to Draft Rules 4.05, 4.06, and 4.09, which require Controllers to use "technical and organizational measures" or a "process" established by processes to fulfill individual rights requests for data held by a processor. This approach aligns with the CPA's text, which recognizes that processors can adopt a range of "technical and organizational measures" to assist controllers in responding to consumer rights requests. It also mirrors the obligation imposed on processors not just by other state privacy laws enacted in Connecticut, Virginia, and Utah, and the obligation imposed by the EU's GDPR.[4] Moreover, this approach recognizes that different measures may be best suited to assist a controller depending on the type of services at issue and the scale and sophistication of the companies.[5]

VIII. Privacy Notices

The Updated Draft Rules revise the regulations' approach to privacy notices. We appreciate this change, which avoids requiring controllers to identify *each purpose for which the controller processes personal data* and then to list five types of information about data processed for each of those purposes. As explained in our Dec. 20, 2022, comments, we have several concerns with the prior approach, including the likelihood that it could lead to longer privacy policies that increase consumer confusion.

We strongly recommend retaining the approach in the Updated Draft Rules, which does not require companies to organize privacy policies by processing purpose.

* * *

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
Managing Director, Policy

---

[4] *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.")

[5] 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.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org