David M. Stauss, Partner
Shelby E. Dolen, Associate

1801 Wewatta St., Suite 1000
Denver, CO 80202
david.stauss@huschblackwell.com
shelby.dolen@huschblackwell.com

June 21, 2022

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

Re: Response to Pre-Rulemaking Considerations for the Colorado Privacy Act

Mr. Attorney General:

Please accept this letter in response to the Attorney General's Pre-Rulemaking Considerations for the Colorado Privacy Act (CPA). The comments and opinions stated herein are our own and do not represent the comments of our law firm or clients. We have not been compensated by any client to prepare these comments.

About Us

We are Denver-based data privacy and cybersecurity attorneys who counsel clients across a range of industries, including technology, hospitality, financial services, consumers products, and manufacturing. Our clients range from start-ups to multinational Fortune 500 companies.

We advise clients on strategic approaches to comply with existing and emerging U.S. and international privacy and data protection regulations, including the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA).

We specialize in emerging state privacy laws. We manage an online State Privacy Law Tracker and our privacy blog, Byte Back, a leading source for state privacy law developments. We also host a privacy podcast where we interview authors of proposed state privacy laws. This past legislative season, one of our team members was a member of the work group for the Connecticut Data Privacy Act and served as the outside subject-matter expert for the bill's sponsor.

Collectively, we hold numerous accreditations from the International Association of Privacy Professionals, including Privacy Law Specialist (PLS), Certified Information Privacy Professional (U.S. and EU), Certified Information Privacy Technologist, and Fellow of Information Privacy.

Overall Purpose of Our Comments

The purpose of our comments is to identify areas in which the Attorney General's Office may provide additional clarity to consumers and businesses and to ensure, where appropriate, the interoperability of the CPA with other state privacy laws enacted in California, Connecticut, Utah, and Virginia and international privacy laws such as GDPR.

Further clarification on the operability of the CPA will benefit both consumers and businesses. In our experience, our clients pursue compliance with privacy laws like the CPA but meet difficulties due to ambiguities in the laws. On the other hand, as Colorado citizens, we are also mindful – and thankful – that we will benefit from the privacy rights the CPA provides. We hope to ensure that our fellow citizens have ready access to their new privacy rights and means to understand those rights.

Further, interoperability between emerging and existing privacy laws must be a focus of the Office's rulemaking activities. We recently concluded a ten-part article series examining interoperability challenges with the California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (VCDPA), and the CPA. Since that time, two states (Connecticut and Utah) passed privacy laws, adding further complexity for businesses that must comply with various laws. Although CPA compliance will no doubt have its unique aspects, ensuring for as much interoperability as possible should be a goal of the rulemaking process.

Comments

I. Consent

a. Does the CPA allow consumers to revoke consent for the processing of sensitive data and for incompatible purposes?

The CPA refers to consumer consent in multiple contexts, including requiring controllers to obtain consumer consent for the processing of sensitive data, C.R.S § 6-1-1308(7), prohibiting controllers from processing personal data for incompatible purposes without consumer consent, C.R.S. § 6-1-1306(4), and permitting controllers to obtain consumer consent to circumvent a universal opt out, C.R.S. § 6-1-1306(1)(a)(IV)(C).

The CPA defines consent in section 6-1-1303(5); however, the definition does not specify whether consumers may revoke consent to the processing of sensitive data or for the processing of personal data for incompatible purposes. In contrast, the CPA does state that consumers may revoke their consent for the processing of personal data in the context of opt-out signals. C.R.S. § 6-1-1306(1)(a)(IV)(C) ("The web page, application, or other means by which a controller obtains a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data must also allow the consumer to revoke the consent as easily as it is affirmatively provided."). The CPA creates ambiguity by addressing revocation of consent in one context but not addressing revocation of consent for the processing of sensitive data or for the processing of personal data for incompatible purposes.

In comparison, the Connecticut Data Privacy Act requires controllers to "provide an effective mechanism for a consumer to revoke the consumer's consent . . . that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request." Section 6(a)(6). GDPR also specifies that data subjects must be given the right to revoke consent. GDPR Art. 7(3) ("The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."). Other modern international privacy laws contain similar provisions addressing consent. *See, e.g.*, Lei Geral de Proteção de Dados (LGPD), Art. 8, § 5 ("Consent may be revoked at any time, by express request of the data subject, through a facilitated and free of charge procedure, with processing carried out under previously given consent remaining valid as long as there is no request for deletion, pursuant to item VI of the lead sentence of Art. 18 of this Law."); Personal Information Protection Law of

the People's Republic of China (PIPL), Art. 15 ("Where the processing of personal information is based on the individual's consent, the individual has the right to withdraw his consent. Personal information processors should provide convenient ways to withdraw consent. The withdrawal of consent by an individual does not affect the validity of the personal information processing activities that have been carried out based on the individual's consent prior to the withdrawal."); Personal Data Protection Act of Singapore (PDPA), Art. 16(3) ("An organisation must not prohibit an individual from withdrawing his or her consent to the collection, use or disclosure of personal data about the individual, but this section does not affect any legal consequences arising from such withdrawal.").

Although it could be argued that the right to revoke consent is implicit in the CPA, it is not clear that Colorado law supports this position based on analogizing from existing court decisions. *See, e.g.*, *People v. Kennard*, 488 P.2d 563, 564 (1971) (rejecting defendant's attempt to withdraw consent to car search after search had begun); *U.S. v. Simmons*, 179 F.R.D. 308, 312 (D. Colo. 1998) (discussing right to revoke consent to trial by magistrate judge and rejecting revocation under facts of case).

Consequently, we recommend the Attorney General's Office clarify pursuant to its permissive rulemaking whether consumers have the right to revoke consent for processing sensitive data and for incompatible purposes and, if so, how consumers exercise this right and the consequences of such revocation. For example, in Europe, a data subject's revocation of consent requires a controller to also delete the consumer's personal data unless the controller has another lawful basis for the processing of the personal data. *See* European Commission, What if somebody withdraws their consent? Of course, the CPA does not have a GDPR Article 6 equivalent, making a lawful basis for processing analysis moot. However, for CPA purposes, the Attorney General could reason that a controller must delete personal data upon a consumer's revocation of consent unless there is a lawful basis for retaining such personal data pursuant to C.R.S. § 6-1-1304(3).

b. Clarifying how controllers can obtain consumer consent to sell personal data or engage in targeted advertising after receiving an opt-out signal

C.R.S. § 6-1-1306(1)(a)(IV)(B) requires controllers to recognize opt-out signals as requests to opt out of sales and targeted advertising. However, notwithstanding the receipt of that signal, "a controller may enable the consumer to consent, through a web page, application, or a similar method, to the processing of the consumer's personal data for purposes of targeted advertising or the sale of personal data, and the consent takes precedence over any choice reflected through the universal opt-out mechanism." C.R.S. § 6-1-1306(1)(a)(IV)(C). The CPA continues:

> Before obtaining a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data pursuant to this subsection (1)(a)(iv)(c), a controller shall provide the consumer with *a clear and conspicuous notice* informing the consumer about the choices available under this section, describing the categories of personal data to be processed and the purposes for which they will be processed, and explaining how and where the consumer may withdraw consent. The web page, application, or other means by which a controller obtains a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data must also allow the consumer to revoke the consent as easily as it is affirmatively provided.
>
> (Emphasis added)

The CPA does not explain what constitutes a "clear and conspicuous notice" or how controllers should seek such consent from consumers. Privacy professionals may interpret this provision to allow controllers

to obtain consent through the use of cookie consent banners. We request the Attorney General to clarify whether or not the use of such cookie consent banners satisfies the requirements of this section subject to the banner being deployed consistent with the above-noted requirements (i.e., linking to proper disclosures and allowing consumers to revoke their consent) as well as the requirements for "consent" as set forth in the definition of that term in C.R.S. § 6-1-1302(5).

c. International resources analyzing similar definitions of consent

Other data protection authorities have considered similar contours of consent. Although not an exhaustive list, the below resources are worthy of the Attorney General's consideration.

Perhaps the most notable guidance on consent is from the European Data Protection Board in its Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1) (Adopted May 4, 2020). The CPA's definition of consent mirrors GDPR's definition of consent insofar as both definitions require consent to be freely given, specific, informed and unambiguous. Compare C.R.S. § 6-1-1303(5) ("'Consent' means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement"); GDPR Art. 4(11) ("'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her").

The United Kingdom's Information Commissioner's Office has provided extensive guidance. See Information Commissioner's Office, Consent. In addition, the Office of the Privacy Commissioner of Canada has published Guidelines on obtaining meaningful consent (last revised August 13, 2021).

Given that many controllers subject to the CPA will already have driven compliance with these laws, we respectfully recommend that any CPA guidance on the contours of consent be consistent with these interpretations.

II. Consumer Requests

a. What constitutes a "clear and conspicuous method" for exercising consumer opt-out rights?

C.R.S. § 6-1-1306 provides that a "controller that processes personal data for purposes of targeted advertising or the sale of personal data shall provide a clear and conspicuous method to exercise the right to opt out of the processing of personal data concerning the consumer pursuant to subsection (1)(a)(i) of this section. The controller shall provide the opt-out method clearly and conspicuously in any privacy notice required to be provided to consumers under this part 13, and in a clear, conspicuous, and readily accessible location outside the privacy notice."

The CPA does not provide any additional information on how controllers should comply with this requirement.

Under the CPRA, if a business "sells" or "shares" personal information, the CPRA will require the business to "[p]rovide a clear and conspicuous link on the business's internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information." Cal. Civ. Code § 1798.135(a)(3). If a business subject to the CPRA uses sensitive personal information in a way that triggers the CPRA's sensitive information limitation provision, the business must provide "a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive

Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121." *Id.* § 1798.135(a)(2). The CPRA, however, provides businesses with discretion to "utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information." *Id.* § 1798.135(a)(3). On page 24 of its draft regulations, the California Privacy Protection Agency stated that the alternative opt-out link shall be titled "Your Privacy Choices" or "Your California Privacy Choices."

Cluttering websites with multiple (and potentially confusing) links provides no benefit to consumers or businesses. In fact, it raises the same issues that the prohibition on dark patterns seeks to regulate – i.e., confusing consumers. Given these considerations, we recommend the Attorney General's Office exercise its permissive rulemaking authority to expand on this requirement. In doing so, we suggest the Attorney General's Office issue the following clarifications:

- Businesses subject to the CPRA and CPA and use the CPRA's "Do Not" links are in compliance with the CPA's requirements. More generally, given the emergence of other state privacy laws that could include such provisions, we recommend the Office promulgate a regulation stating that businesses have the discretion to utilize links other laws require to comply with the CPA's requirement so long as the use of such links allow consumers to exercise their opt-out rights.

- Given the CPRA's discretion in allowing businesses in section 1798.135(a)(3) to allow businesses to implement alternative links and the CPA's discretionary language, we recommend the Office encourage controllers to implement "Privacy Centers" or "Privacy Portals" where controllers can provide holistic information to consumers as to their rights and how to exercise them.[1] The use of such landing pages will benefit both consumers and controllers by providing a single page for information rather than risking multiple complicated (and perhaps contradictory) pages of information. This is particularly true for entities subject to multiple state privacy laws and international privacy laws.

    b. *What are "reasonable means to determine that a request to exercise any of the rights in section 6-1-1306(1) is being made by or on behalf of the consumer who is entitled to exercise the rights"?*

C.R.S. § 6-1-1306(1) requires controllers to "authenticate the identity of the consumer making the request" prior to responding to said request. This requirement applies to all CPA rights, including the right to opt out of sales, targeted advertising and profiling, and the rights of access, correction, deletion and data portability. The CPA defines "authenticate" as the "use [of] reasonable means to determine that a request to exercise any of the rights in section 6-1-1306(1) is being made by or on behalf of the consumer who is entitled to exercise the rights." C.R.S. § 6-1-1303(2). The CPA does not further specify what constitutes "reasonable means." The Attorney General's Office should exercise its permissive rulemaking authority to clarify what controllers should do to authenticate requests.

In making this determination, we suggest that the Attorney General implement a flexible approach that allows controllers to authenticate the consumer's identity based on the circumstances of the request as opposed to prescriptive standards. For example, in its Guidelines 01/2022 on data subject rights – Right of access § 3.2, ¶¶ 64-78 (Version 1.0, adopted 18 January 2022), the EDPB discusses flexible standards

[1] *See, e.g.*, https://www.marriott.com/about/privacy.mi; https://privacy.zillowgroup.com/.

for authenticating right of access requests under GDPR Article 15. The CCPA regulations are more prescriptive – e.g., requiring two or three data points to be verified depending on the type of request. 11 CCR § 7062. Clarifying that the CPA requires a flexible authentication standard will benefit businesses by providing them with discretion to authenticate requests based on the way in which they interact with consumers. It also allows for businesses to adapt their authentication processes to emerging technologies.

Finally, we recommend that controllers should not be required to authenticate opt-out requests to the same level as other requests. While the CPA requires that such requests be authenticated, neither California nor Connecticut require that opt-out requests be authenticated. SB 6, Sec. 4(c)(4) ("A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request."); Cal. Civ. Code § 1798.120 (CPRA right to opt out of sales and sharing); 11 CCR § 7026(g) ("A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.").

In explaining its thinking behind 11 CCR § 7026(g), the Attorney General stated:

> Unlike requests to know and requests to delete, the CCPA does not require requests to opt-out to be verified. In drafting these regulations, the OAG considered how best to ensure that consumers are empowered to exercise their rights under the CCPA while also acknowledging that there could be potential for abuse. The proposed regulation balances these concerns by placing minimal barriers to a consumer's ability to opt-out, while providing businesses the ability to deny requests that they believe are fraudulent as long as they inform the consumer and document their good-faith and reasonable belief. See § 999.315(h).

California Attorney General's Office, FSOR Appendix A: Summary and Response to Comments Submitted During 45-Day Period, Response to Comment 617.

Here, the CPA clearly states that authentication is required for opt-out requests such that matching the standard in California and Connecticut is not possible. However, the approach of those statutes evidences that requiring the same level of authentication for such requests is unnecessary and, in fact, is unlikely to benefit consumers or businesses.

III. Privacy Notices

The CPA requires controllers to provide consumers with a "reasonably accessible, clear and meaningful privacy notice" that includes certain identified information. C.R.S. § 6-1-1308(1)(a). The CPA does not otherwise define what constitutes an accessible, clear, and meaningful privacy notice.

With respect to website accessibility, it has become commonplace for businesses to provide privacy notices to consumers through the use of a link in a persistent website footer using the word "privacy." This approach is consistent with existing laws. *See* 11 CCR § 7011(b) ("The privacy policy shall be posted online through a conspicuous link using the word 'privacy' on the business's website homepage or on the download or landing page of a mobile application."); California Attorney General's Office, *Making*

Your Privacy Practices Public at 9 (2014); Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679* (as last revised and adopted on 11 April 2018) (hereinafter "Transparency Guidelines" ("Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.").

For mobile applications, it is commonplace for privacy policies to be accessible through the menu or a similar feature. *See* 11 CCR § 7011(b) ("A mobile application may include a link to the privacy policy in the application's settings menu."); California Attorney General's Office, *Making Your Privacy Practices Public* at 9 (2014); Transparency Guidelines ("For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than "two taps away" (e.g. by including a "Privacy"/ "Data Protection" option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.").

The Attorney General's office should confirm the above standards satisfy the CPA's "reasonably accessible" requirement.

With respect to the CPA's "clear and meaningful" standards, we refer the Office to the Article 29 Working Party's Transparency Guidelines as well as ICO guidance. The California Attorney General's Office also adopted comparable guidance for the CCPA. *See* 11 CCR § 7011(b).

Although the above standards are well-developed, the passage of multiple state consumer privacy laws since the CCPA's effective date could create confusion as to whether controllers must provide state-specific privacy disclosures. Such an approach would inevitably result in elongating already lengthy privacy policies, to the detriment of both consumers and controllers. To that end, we recommend the Office exercise its discretionary rulemaking authority to specify that controllers may (and are encouraged to) provide CPA disclosures in conjunction with other state and international disclosures.

IV. Definition of Biometric Data

The CPA requires controllers to obtain consumer consent for the processing of sensitive data. C.R.S. § 6-1-1308(7). The CPA defines sensitive data to include "biometric data that may be processed for the purpose of uniquely identifying an individual," C.R.S. § 6-1-1303(24)(b); however, the CPA does not define "biometric data."

The CPA's failure to define biometric data is unique among the five states that have passed similar legislation. See Cal. Civ. Code § 1798.140(c) (defining biometric information); Va. Code Ann. § 59.1-575; Utah Code Ann. § 13-61-101(6); Connecticut Senate Bill 6, § 1(3).

Given that the CPA requires controllers to obtain consent for the collection of biometric data, it is crucial to define what constitutes biometric data. Colorado's breach notification statute contains a definition of biometric data, however, the definition is unlikely to work for purposes of the CPA because it is restricted to information used "for the purpose of authenticating the individual when he or she accesses an online account." C.R.S. § 6-1-716(1)(a).

We recommend the Attorney General's Office exercise its permissive rulemaking authority to define biometric data consistent with the definition Connecticut provides:

> "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

Connecticut's definition of biometric data is generally consistent with the GDPR's interpretation. For example, GDPR Recital 51 provides, in relevant part: "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

Connecticut's definition also is consistent with European Data Protection Board guidance as reflected in paragraphs 73-75 of *Guidelines 3/2019 on processing of personal data through video devices* (Version 2, adopted January 29, 2020). Paragraph 74 states, in relevant part: "The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual."

In contrast, the definitions in Virginia and Utah's laws exclude certain types of information considered to be biometric data including facial and voice recognition. *See* Virginia Joint Commission on Technology and Science, Virginia Consumer Data Protection Act Work Group, 2021 Final Report at 7 ("Delegate Hayes summarized the events leading to the creation of the Work Group. He noted that legislation in Washington state was a starting model for the effort to pass similar data privacy legislation in the Commonwealth and added that two important strategic distinctions that led to the successful passage of the Virginia Consumer Data Protection Act (VCDPA), as opposed to similar legislative efforts in other states other state efforts, remain the exclusion of facial recognition and the enforcement of the law by the Attorney General."); Taylor Kay Lively, *Facial Recognition in the United States: Privacy Concerns and Legal Developments*, SECURITY TECHNOLOGY, December 1, 2022 ("Unlike California and Colorado, Virginia's Consumer Data Protection Act (effective Jan. 2023) excludes facial recognition").

Alternatively, the Attorney General could look to the definition of biometric information set forth in the CPRA:

> "Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

See Cal. Civ. Code 1798.140(c).

However, the CPRA's definition is lengthy and creates ambiguity through its reference to "keystroke patterns or rhythms" and "gait patterns or rhythms."

V. Reasonable Limitations on Access Requests

C.R.S. § 6-1-1306(1)(b) provides consumers with "the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data."

Although this right is written in the absolute, we recommend the Attorney General's Office exercise its permissive rulemaking authority to clarify that this right does not require controllers to disclose information protected by C.R.S. § 6-1-716 or trade secrets as defined in C.R.S. § 7-74-102(4). These recommendations are consistent with the CCPA and further the goal of protecting consumers.

a. Data breach exception

With respect to the first recommendation, CCPA regulation 11 CCR 7024(d) specifically forbids businesses from providing information in response to requests to know that California's breach notification statute covers:

> A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.

In its Final Statement of Reasons, the California Attorney General's Office explained that this provision "benefits consumers by providing them with information to make privacy decisions while protecting them from the harms that could result from the unauthorized disclosure of this sensitive personal information." *See* California Attorney General's Office, Final Statement of Reasons at 26.

The types of personal information subject to Colorado's breach notification statute, C.R.S. § 6-1-716, are comparable to the types of information that California prohibits businesses from disclosing in response to requests to know. For example, Colorado's breach notification statute covers Social Security numbers, driver's license numbers, biometric data, medical information, and certain types of financial information. Even if a controller authenticates a consumer request, there is still a risk the request is fraudulent. Thus, there is a benefit to consumers to protecting this sensitive information from disclosure in response to access requests. In addition, there is not a significant benefit to consumers by requiring controllers to disclose this type of information as consumers should already have access to this information. Therefore, requiring a controller to confirm that is has collected a consumer's Social Security number rather than disclosing a consumer's Social Security number, provides the same benefit to the consumer since they presumably already know their Social Security number.

b. Protection of trade secrets

The California Attorney General's Office recently issued an opinion on whether the CCPA requires businesses to disclose inferences in response to requests to know. *See* Opinion of Rob Bonta, No. 20-303

(March 10, 2022). In responding to the question in the affirmative, the California Attorney General carefully noted that the "CCPA does not require businesses to disclose their trade secrets." *Id.* at 14. The Office grounded its decision in Cal. Civ. Code § 1798.145(a)(1) which states that "[t]he obligations imposed on businesses by this title shall not restrict a business' ability to: [c]omply with federal, state, or local laws." *Id.* at 14; *see also id*. at 15 (noting that CPRA amends this language to specifically refer to trade secrets); Stauss, Rogers, Dolen, *CCPA Update, California Attorney General Issues Opinion on Disclosure of Inferences*, ByteBackLaw, March 15, 2022.

After the California Attorney General's Office issued this opinion, Connecticut amended its proposed privacy legislation to specifically recognize that controllers do not have to disclose trade secrets in response to requests to know and data portability requests. *See* SB6, Sec. 4(a).

Like California and Connecticut, Colorado law protects trade secrets. The CPA, like California, also provides that it does not restrict a controller's "ability to: . . . comply with federal, state, or local laws, rules, or regulations." C.R.S. § 6-1-1304(3)(a). Therefore, clarifying that the CPA does not require controllers to disclose trade secrets is consistent with California and Connecticut and reasonably protects controllers from unintended harm.

Very truly yours,

By: _____
David M. Stauss

_____
Shelby E. Dolen