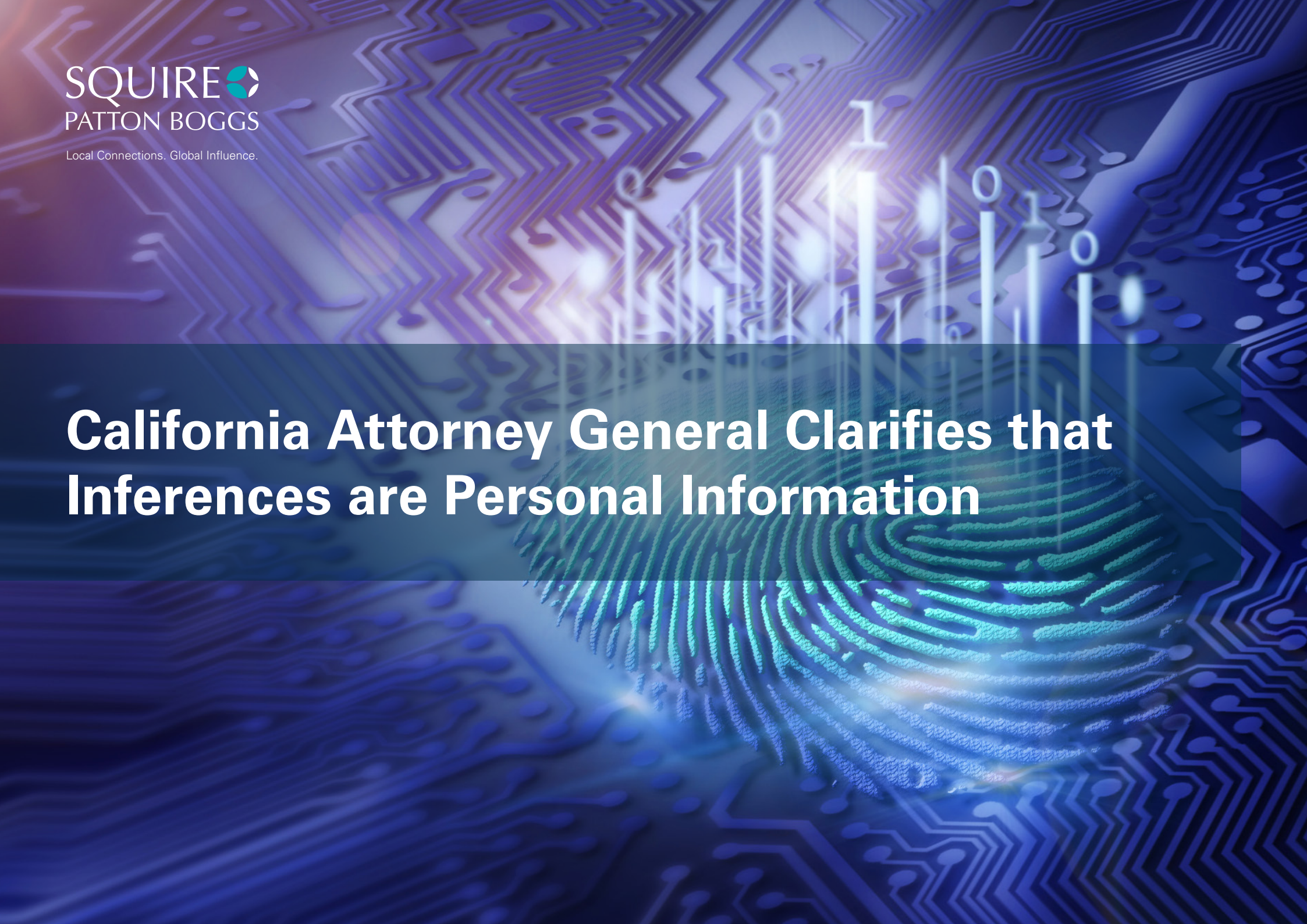

California Attorney General Clarifies that Inferences are Personal Information

On March 10, 2022, California Attorney General Rob Bonta (Attorney General) published the first official opinion interpreting the California Consumer Privacy Act (CCPA) and concluded that the CCPA's right to know includes a business' internally generated inferences about a consumer from either internal or external information sources.

Importantly, the opinion clarifies that inferences made from information that is otherwise exempt from the scope of the CCPA – such as publicly available information – are, in fact, personal information. Finally, the opinion weighs in on the tug of war between consumer privacy rights and businesses' intellectual property and trade secret rights, definitively stating that trade secrets are completely protected from disclosure under the CCPA. These are important conclusions for businesses to consider in order to ensure CCPA compliance in the immediate term and as they ramp up for the implementation of the California Privacy Rights Act of 2020 (CPRA), which becomes fully operative on January 1, 2023, and substantially amends the CCPA.

Question Presented to the Attorney General

California State Assemblymember Kevin Kiley asked the Attorney General:

Under the California Consumer Privacy Act, does a consumer's right to know the specific pieces of personal information that a business has collected about that consumer apply to internally generated inferences the business holds about the consumer from either internal or external information sources?

Key Takeaways

- In short, the Attorney General concluded that "internally generated inferences that a business holds about a consumer are personal information within the meaning of the CCPA, and must be disclosed to the consumer on request." Opinion No. 20-303 (Opinion), p. 15. This is true even if the information off which the inferences are based is exempt from the CCPA when collected (e.g., publicly available information).
- Arguably, though, businesses do not need to delete internally generated inferences in response to a consumer's request to delete, even if based on personal information collected from the consumer.
- Trade secrets are completely protected under the CCPA, but a business bears the burden of demonstrating that the withheld information is a trade secret. The inference itself might not be a trade secret and would have to be disclosed in response to a request to know; however, the algorithm that a company uses to derive its inferences may be a trade secret and, if so, would not have to be disclosed.
- The CPRA will address this interplay between trade secret and consumer rights, whereby businesses will be required to disclose meaningful information about the logic involved in automated decision-making under the new concept of "profiling" and its related consumer rights, presenting a potential conflict between consumer rights and trade secret rights that may be addressed in upcoming rulemaking.

Contacts

Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Kyle Fath
Partner, Los Angeles
T +1 213 689 6582
E kyle.fath@squirepb.com

Kyle Dull
Senior Associate, New York
T +1 212 872 9867
E kyle.dull@squirepb.com

Opinions of the Attorney General

While the CCPA, under Section 1798.155, provides businesses the opportunity to "seek the opinion of the Attorney General for guidance on how to comply" with the statute, the Opinion was requested by Assemblymember Kiley, a former Deputy Attorney General, under a different statute. Under Section 12519 of the California Government Code, "[t]he Attorney General shall give his or her opinion in writing to any Member of the Legislature . . . when requested, upon any question of law relating to their respective offices." It is important to note that Attorney General opinions are not binding on California courts.[1] However, because the Attorney General is currently the enforcing authority under the CCPA and will continue to enforce the CPRA alongside the new California Privacy Protection Agency (CPPA), businesses should study the Opinion carefully.

Prior to the issuance of the Opinion, businesses had few things to rely on to guide their compliance: (1) the text of the CCPA and implementing regulations; (2) counsel's experience defending businesses in confidential investigations by the Attorney General; (3) the Attorney General's high-level enforcement summaries published last year; (4) public facing documents on the Attorney General's website that provide snippets of unofficial guidance; and (5) the Attorney General's responses to public comments made during the CCPA rulemaking process.

CCPA Applicability and Relevant Definitions

As general background, the CCPA applies to businesses that collect personal information from California consumers and (1) have over US$25 million in gross revenues a year; (2) buy, receive, or share the personal information of 50,000 or more people a year for commercial purposes; or (3) derive more than 50% of their annual revenue from selling consumers' personal information. "Personal information" is defined by the statute to be "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[2]

The CCPA also lists specific types of information that is considered personal information, including identifies, commercial information, geolocation data, internet activity information, geolocation data, and "[i]nferences drawn from any of the information *identified in this subdivision [Section 1798.140(o)] to create a profile about a consumer* reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes," "if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."[3] There are certain types of information identified in Section 1798.140(o) that are explicitly excluded from the definition of personal information, including "publicly available information," and "consumer information that is deidentified or aggregate consumer information."[4] "Inference" is also a defined term, which "means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data."[5]

1 Orange Cty. Empls. Ass'n, Inc. v. Cty. of Orange, 14 Cal. App. 4th 575, 578 (1993) (Reasoning, "[w]hile not binding on us, the opinions of the Attorney General are entitled to great weight.").

2 California Civil Code, Section 1798.140(o)(1).

3 Section 1798.140(o)(1) (emphasis added).

4 Section 1798.140(o)(2)-(3).

5 Section 1798.140(m).

Consumers are granted several rights under the CCPA, including the right to request that a business disclose to the consumer "the specific pieces of personal information [the business] has collected *about* that consumer" ("right to know").[6] Section 1798.110 does not require a business to "[r]eidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information."[7] The CCPA also grants consumers "the right to request that a business delete any personal information about the consumer which the business has collected *from* the consumer."[8] Thus, the two rights apply to distinct types of information: one to information collected *about* the consumer and the other to information collected *from* the consumer.

Inferences Under the CCPA

As noted by the Attorney General, inferences are "personal information" if (1) drawn from information identified in Section 1798.140(o); and (2) "used to 'create a profile about a consumer,' or in other words to predict a salient consumer characteristic." Opinion, p. 11.

In analyzing the first prong, the Attorney General is quick to point out that "the information identified in [Section 1798.40(o)]" not only includes personal information as defined in that section, as well as the enumerated categories, but also information referred to Section 1798.40(o) that is exempt from the CCPA – namely, publicly available information, deidentified information and aggregate consumer information.

The Attorney General points out that "[a] business might draw an inference about a consumer based in whole or in part on publicly available information, such as government identification numbers, vital records, or tax rolls." Opinion, p. 12. Under the CCPA, according to the Attorney General, the publicly available information need not be disclosed, but the inference derived from that publicly available information must be disclosed to the consumer. In reaching this conclusion, the Attorney General noted "the Legislature's concern about the exploitive tendencies of collecting masses of information and using it to identify and affect unwitting consumers." Opinion, p. 12. As a result, inferences derived from information that is otherwise exempt when initially collected becomes personal information (as long as the second prong is met, as discussed below).

This second prong rules out situations where a business is using inferences for reasons other than predicting, targeting or affecting consumer behavior. In order to clarify this point, the Attorney General provides a helpful example discussing the use of zip codes. A business might obtain a nine-digit zip code to facilitate the delivery of an item by combining information obtained from the customer and the consumer's online postal information.

The Attorney General reasons, "if the zip code is merely deleted and not used to identify or predict the characteristics of a consumer, in our view that would not give rise to a disclosable inference within the meaning of the statute. On the other hand, when a business processes personal information to make an inference about the consumer's propensities, then the inference itself becomes part of the consumer's profile, and must be disclosed." Opinion, p. 12. In other words, if the zip code is deleted and not used to identify or predict the characteristics of a consumer – such as their affluence – the opinion states that it would not turn the inference into personal information. Thus, when a business creates inferences or buys inferences, "those inferences constitute a part of the consumer's unique identity and become part of the body of information that the business has "collected about" the consumer, and are, therefore, in the scope of what must be disclosed in response to request to know specific pieces. Opinion, p. 13.

Notably, the Opinion appears to tacitly endorse retention of internally generated inferences following a deletion request, even if they are based on information collected directly *from* the consumer. Companies that carry out the totally legitimate practice of retaining information not collected directly from the consumer should, of course, ensure that their privacy policy and communications with consumers about consumer requests are clear about the scope of information that is being deleted – namely, that it only applies to information collected *from* the consumer.

6 Section 1798.110(a)(5) (emphasis added).

7 Section 1798.110(d)(2).

8 Section 1798.105(a) (emphasis added).

What Does This Mean for Trade Secret Protection?

In addressing the concern that the disclosure of internally generated interests might reveal trade secrets, the Attorney General opined that, "While the algorithm that a company uses to derive its inferences might be a protected trade secret, the CCPA only requires a business to disclose individualized products of its secret algorithm, not the algorithm itself." Opinion, p. 13.

Trade secret protection has been a topic of consideration as it applies to its interaction with the CCPA and, as discussed below, will continue to be under the CPRA. During the CCPA rulemaking process, the Attorney General did not promulgate rules on trade secret protection because "the Attorney General was not presented with any concrete examples of situations where inferences are themselves trade secrets, or where the disclosure of inferences would expose a business's trade secrets." Opinion, p. 14. However, the Opinion provides businesses with guidance in this area.

Under California's Uniform Trade Secrets Act, a trade secret is:

> Information, including a formula, pattern, compilation, program, device, method, technique or process, that:
>
> 1. Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
> 2. Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[9]

In other words, a trade secret is information that is valuable because it is unknown to others and which the owner has attempted to keep a secret.[10] The "trade secret is not the idea or fact itself, but information tending to communicate (disclose) the idea or fact to another."[11] There is a strong argument to be made that the method for calculating the inferences be protected as a trade secret.[12] The Attorney General notes just that, reasoning "the algorithm that a company uses to derive its inferences might be a protected trade secret, the CCPA only requires a business to disclose individualized products of its secret algorithm, not the algorithm itself." Opinion, p. 14.

9 Cal. Civ. Code. Section 3426.1(d).

10 Abba Rubber Co. v. Seaquist, 235 Cal. App. 3d 1, 18 (1991).

11 Altavion Inc. v. Konica Minolta Systems Laboratory Inc., 226 Cal. App. 4th 26, 54 (2014).

12 See Brocade Communications Systems, Inc. v. A10 Networks, Inc., 873 F. Supp. 2d 1192, 1214-16 (N.D. Cal. 2012) (Reasoning that "confidential customer-related information including customer lists and contact information, pricing guidelines, historical purchasing information, and customers' business needs/preferences" present a strong argument to be protected under California law as a trade secret.).

What Is the Impact on CPRA Compliance?

Notably, the Attorney General opines that the CPRA's amendments to the CCPA "do not change the conclusions presented in this opinion." Opinion, p. 9. However, it is unclear whether this is accurate considering the CPRA's new concept of profiling and automated decision-making, and required rulemaking in the area, will almost certainly bear upon the Opinion's conclusions regarding disclosure of algorithms or aspects thereof.

By way of background, the CPRA's new concept of profiling means "any form of automated processing of personal information, as further defined by [the CPRA's regulations], to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[13] Certainly, there is some overlap as to what may constitute an inference used to create a profile as it is currently defined under the CCPA, and the definition of profiling under the CPRA.

The CPRA provides consumers additional access and opt-out rights as it relates to profiling. In particular, businesses will need to provide consumers with "access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes" and the CPRA requires regulations be issued on this area.[14] In September 2021, the California Consumer Privacy Protection Agency (CPPA) published an invitation for preliminary comments on proposed rulemaking, specifically addressing this section of the CPRA. The CPPA sough comment on (1) what activities constitute automated decision-making technology and profiling; (2) when consumers should be allowed to access such information; (3) the scope of the consumer's opt-out right; and (4) any related procedures. The public comments are now available on the CPPA's website.

As it relates to this new access right, the definition of meaningful information might require businesses to disclose at least some of the details of the algorithm involved in automated decision-making, which, at least in some respects, conflicts with the Attorney General's statement regarding disclosure of algorithms upon which inferences are based. Nonetheless, perhaps we can take this recent opinion as an indication of the Attorney General's potential position on the interplay between trade secrets and disclosing information about the algorithms involved in profiling or automated decision-making under the CPRA. Of course, we must take that with somewhat of a grain of salt because the new CPPA will be the agency issuing regulations this time around, and enforcing alongside the Attorney General.

Importantly, the CPPA is also tasked with issuing regulations to establish "exceptions necessary to comply with state or federal law, including, but not limited to, those related to trade secrets and intellectual property rights…with the intention that trade secrets should not be disclosed in response to a verifiable consumer request."[15] Therefore, it seems this tug of war between consumers' privacy and companies' intellectual property rights will continue, but perhaps we will have more clarity when we have CPRA's implementing regulations.

What About Inferences Under Virginia and Colorado's Law?

Neither the Virginia Consumer Data Protection Act (VCDPA) nor the Colorado Privacy Act (CPA) include inferences as an enumerated category of personal data, though their definitions of personal data are broad and very well may include inferences drawn about a consumer. As to access and deletion rights in Virginia and Colorado, both rights would apply to internally generated inferences under the CPA, but under the VCDPA, a consumer could cause deletion but not obtain a copy. Colorado does not draw a distinction between the two rights as they both apply to "personal data concerning the consumer."[16] Virginia, however, draws a distinction between personal data subject to the right to know and right to delete. Under the VCDPA, a consumer has the right to make a request "[t]o obtain a copy of the consumer's personal data *that the consumer previously provided to the controller*."[17] A Virginia consumer has the right to request that a controller "delete personal data provided by or obtained about the consumer."[18] Thus, the scope of consumer rights as to right to know and delete are different between the three state laws. Of course, this applies to data beyond inferences. Companies will have to decide if they are going to apply the highest level of consumer rights to all, or apply only state-specific requirements where that benefits the company.

Conclusion

Internally generated inferences that a business holds about a consumer are personal information within the meaning of the CCPA, regardless of the source of the information on which the inferences are based, and must be disclosed to the consumer on request. Certainly, businesses should evaluate the extent to which they are creating internally generated inferences and how they are classifying them differently, if at all, based on the source of such information, as well as how such inferences are implicated with respect to consumer requests to know and delete. It appears settled for now that any algorithm used in generating inferences is not required to be disclosed in response to a request to know, but the extent to which that will change, if at all, might be addressed in the forthcoming CPRA regulations. As a result, businesses have some work to do in the immediate term to address the issues raised in the opinion but should also pay attention as the CPRA rulemaking process progresses.

13 CPRA Section 1798.140 (z).

14 Section 1798.185(a)(16).

15 CPRA Section 1798.185(a)(3).

16 Colorado Privacy Act, Section 6-1-1306(1)(d)-(e).

17 Virginia Consumer Data Protection Act, Section 59.1-573(A)(4) (emphasis added).

18 Section 59.1-573(3) (emphasis added).

SQUIRE PATTON BOGGS

squirepattonboggs.com

51064/03/22