TO BE PUBLISHED IN THE OFFICIAL REPORTS

OFFICE OF THE ATTORNEY GENERAL
State of California

ROB BONTA
Attorney General

OPINION	:	No. 20-303
of	:	March 10, 2022
ROB BONTA Attorney General	:	
SUSAN DUNCAN LEE Deputy Attorney General	:	

THE HONORABLE KEVIN KILEY, ASSEMBLYMEMBER, has requested an opinion on a question of law arising under the California Consumer Privacy Act of 2018.

QUESTION PRESENTED AND CONCLUSION

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?

Yes, under the California Consumer Privacy Act, a consumer has the right to know internally generated inferences about that consumer, unless a business can demonstrate that a statutory exception to the Act applies.

BACKGROUND

The California Consumer Privacy Act of 2018 (Civil Code, §§ 1798.100 et seq.) is the first law of its kind in the nation.[1] It allows consumers in California the ability to find

[1] As of this writing, a number of other states have passed or are considering similar legislation. (See Scott, *Consumer Privacy Protection Continues to Be a Key Issue for State Lawmakers* (April 2021) vol. 27, No. 7, HR Compliance Law Bull. 1.)

out what information a covered business is holding about them, and to opt out of certain transfers and sales of their personal information.

The question before us asks for clarification of one of the provisions in the CCPA, having to do with the consumer's right to request and receive specific pieces of information collected about them.[2] Before we proceed with a detailed analysis of the question, however, we will take a moment to introduce the general contours of this statutory scheme.[3]

How the CCPA Came To Be

Information privacy law has been developing for decades in the United States, along with the development of internet commerce. In 1998, the Federal Trade Commission published a report titled "Privacy Online: A Report to Congress," which noted that "[g]overnment studies in the United States and abroad recognize certain core principles of fair information practice, widely accepted as essential to ensuring fair collection, use, and sharing of personal information in a manner consistent with consumer privacy interests."[4] Those core principles are:

- Consumers should have notice of an entity's information practices.
- Consumers should have choices about how their information is used.
- Consumers should have access to the information about them that an entity holds.
- An entity should take appropriate steps to ensure the security of the information it holds.
- Fair information-practice rules should incorporate enforcement mechanisms to ensure compliance with core principles.

[2] Civ. Code, § 1798.110, subd. (a).

[3] We note that the CCPA includes a provision allowing a business to "seek the opinion of the Attorney General for guidance on how to comply" with the statute. (Civ. Code, § 1798.155.) This Opinion is not given pursuant to that statute. This Opinion is given under the Attorney General's traditional authority to give opinions on questions of law to specified public officials upon their request. (Gov. Code, § 12519.)

[4] Federal Trade Com., Privacy Online: A Report to Congress (June 1998) at p. 2.

- With respect to children's information, parental controls should be required.[5]

For the next 20 years, information privacy law developed largely on a sector-by-sector basis, with federal statutory schemes designed to regulate the information practices of entities holding large amounts of sensitive consumer information. Well-known examples of such programs include the Health Insurance Portability and Accountability Act, governing information practices of health care providers and insurers;[6] the Gramm-Leach-Bliley Act, governing information practices of financial institutions;[7] and the Children's Online Privacy Protection Act, governing the use of information collected from children under 13.[8] Despite these statutory schemes, more than eight in ten adults in the United States feel they have little or no control over the information collected about them online, according to a 2019 poll by the Pew Research Center.[9]

Starting in 2014, a British political consulting firm called Cambridge Analytica (now defunct) surreptitiously obtained personal information about roughly 87 million Facebook users.[10] Cambridge Analytica then used the information to send targeted political messages during the 2016 presidential campaign.[11] When Cambridge Analytica's conduct began receiving significant press coverage in 2018,[12] there arose a public perception that the time had come to give consumers greater control over the

---

[5] *Id*. at pp. 7-11.

[6] 42 U.S.C. §§ 1320d; 45 CFR §§ 160, 162, 164.

[7] 15 U.S.C. §§ 6801-6809.

[8] 15 U.S.C. §§ 6501-6506.

[9] Auxier and Rainie, *Key Takeaways on Americans' Views about Privacy, Surveillance, and Data-Sharing* (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

[10] See *In re: Facebook, Inc. Consumer Privacy User Profile Litigation* (N.D. Cal. 2019) 402 F.Supp.3d 767, 776-778.

[11] See Stats. 2018, ch. 55, § 2(f)-(h) (CCPA legislative findings and declarations).

[12] See, e.g., Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, N.Y. Times (Apr. 10, 2018); Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. Times (Apr. 4, 2018); McKenzie, *Facebook's Mark Zuckerberg Says Sorry in Full-Page Newspaper Ads*, N.Y. Times (Mar. 25, 2018).

privacy of their personal information.[13] In this environment, and hard on the heels of the European Union's adoption of a privacy-protective general regulation,[14] advocates in California proposed a comprehensive consumer-privacy ballot measure for the November 2018 ballot.[15] After the proposal gathered momentum, as well as enough signatures to qualify for the ballot, the California Legislature stepped in, proposing legislative action to take the place of the citizens' initiative.[16] The resulting bill became the CCPA.[17] A series of amendments to the statute were adopted late in 2018.[18]

Subsequently, in November 2020, voters approved the Consumer Privacy Rights Act of 2020, amending and building on the CCPA.[19] The CPRA will become fully operative on January 1, 2023.[20] None of the amendments to the CCPA introduced by the CPRA changes the conclusions presented in this opinion.

---

[13] Stats. 2018, ch. 55, § 2(g) (Legislative findings and declarations in support of CCPA citing Cambridge Analytica event as factor motivating consumer desire for better privacy controls). See also Auxier and Rainie, *Key Takeaways on Americans' Views about Privacy, Surveillance, and Data-Sharing* (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/ (three-quarters of U.S. adults said there should be more government regulation of online data than there is).

[14] General Data Protection Regulation, EU 2016/679, https://gdpr-info.eu/ (as of Mar. 9, 2022). The GDPR took effect May 25, 2018 in all European Union member states. Under the GDPR, covered European consumers have various rights over the use of their personal data, including rights to know, to access, to restrict processing, to object, to rectification, to erasure, to data portability, and rights related to automatic decision making. See generally General Data Protection Regulation, ch. 3, https://gdpr-info.eu/chapter-3/ (as of Mar. 9, 2022).

[15] See California Secretary of State, *Proposed Initiative Enters Circulation: Establishes New Consumer Privacy Rights; Expands Liability for Consumer Data Breaches: Initiative Statute* (Dec. 18, 2017), https://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/proposed-initiative-enters-circulation39.

[16] Sen. Jud. Com., analysis of Assem. Bill No. 375 (2017-2018 Reg. Sess.), as amended Jun. 25, 2018, pp. 2-3.

[17] Assem. Bill No. 375 (2017-2018 Reg. Sess.) (enacted Stats. 2018, ch. 55).

[18] See Stats. 2018, chs. 735, 748, 751, 757, 759, 763.

[19] Initiative Measure (Prop. 24) approved Nov. 4, 2020, eff. Dec. 16, 2020.

[20] *Id.* at § 31.

Relevant Provisions of the CCPA

The CCPA applies to businesses that collect information from consumers in California and that either: have gross revenues exceeding $25 million a year; buy, receive, or share for commercial purposes the information of 50,000 or more people a year; or derive 50 percent or more of their annual revenue from selling consumers' personal information.[21] The CCPA defines "personal information" as including "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."[22] The definition exempts information that is "deidentified," as well as "aggregate consumer information,"[23] thus creating a powerful incentive for businesses to store information in forms that reduce the risk of exposing individual consumers' personal information.

The definition of "personal information" is broad, specifically including personal identifiers (such as name, date of birth, Social Security number), as well as information about education, employment, travel, health, credit, banking, Internet Protocol addresses, online transactions, online searches, biometric data, or geolocation data.[24] Most relevant to our present purposes, the definition also includes "inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[25]

The CCPA endows California residents with new rights of control over the personal information that covered businesses hold about them. California consumers now have:

- The right to know what personal information a business collects about them, and how the business uses and shares that information.[26]

[21] Civ. Code, § 1798.140, subd. (c)(1)(A)-(C).

[22] Civ. Code, § 1798.140, subd. (*o*)(1).

[23] Civ. Code, § 1798.140, subd. (*o*)(3).

[24] Civ. Code, § 1798.140, subd. (*o*).

[25] Civ. Code, § 1798.140, subd. (*o*)(1).

[26] Civ. Code, §§ 1798.100, subd. (a), 1798.115, 1798.140, subd. (t)(1).

- The right to delete the personal information that a business collects from them (with specified exceptions for operational and legal necessity).[27]

- The right to opt out of the sale of their personal information.[28]

- The right to non-discrimination, meaning that consumers who exercise their rights under the CCPA are entitled to receive the same service and price as consumers who do not.[29]

Businesses have corresponding duties. First, a business must provide notice of what categories of personal information it will collect about the consumer and of the purposes for which that information will be used.[30] This notice must be provided at or before the point at which the business collects information from the consumer. If the business sells personal information, then the notice at collection must include a "Do Not Sell My Personal Information" button that allows consumers to opt out of the sale of their personal information.[31] A business's privacy policies must inform consumers of their rights to know, to delete, to opt out, and not to be discriminated against.[32] Businesses must provide fresh notices to consumers when their information practices change.[33]

Businesses have a duty to respond to verifiable consumer requests within 45 to 90 days.[34] If a business is unable to comply completely with a request, it is still obliged to provide as much information as it can. For instance, if a business cannot provide specific pieces of information to the consumer, it must provide information about the categories of information it collects.[35] If a business cannot provide either specific or category information to the consumer, it must refer the consumer to its privacy policy.[36] Furthermore, if a business denies a consumer's request to know "in whole or in part,

---

[27] Civ. Code, § 1798.105.

[28] Civ. Code, § 1798.120.

[29] Civ. Code, § 1798.125.

[30] Civ. Code, § 1798.100, subd. (b); see §§ 1798.110, subd. (c), 1798.130, subd. (a)(5).

[31] Cal. Code Regs., tit. 11, § 999.305(b)(3), (4).

[32] Civ. Code, § 1798.130, subd. (a)(5).

[33] Civ. Code, § 1798.100, subd. (b); Cal. Code Regs., tit. 11, § 999.305(a)(5), (6).

[34] Civ. Code, § 1798.130(a)(2); see also § 1798.130, subd. (a)(3), (4) (discussing verification of requests); Cal. Code Regs., tit. 11, §§ 999.323 – 999.325 (same).

[35] Cal. Code Regs., tit. 11, § 999.313(c)(1).

[36] Cal. Code Regs., tit. 11, § 999.313(c)(2).

because of a conflict with federal or state law, or an exception to the CCPA," the business must explain the basis for its denial.[37]

There are a number of significant exceptions to the CCPA. First, the CCPA does not apply to government entities or nonprofit organizations, and excludes information that is freely available from government sources, such as vital statistics, real estate records, and professional licenses.[38] The CCPA also contains a set of nuanced exceptions for certain categories of information—such as medical records, credit reporting, banking, and vehicle safety records—that apply when the information is governed by another privacy-protecting statute.[39]

Section 1798.145 also incorporates carve-out provisions designed to relieve businesses from undue burdens and common legal binds:

> (a) The obligations imposed on businesses by this title shall not restrict a business' ability to:
> (1) Comply with federal, state, or local laws.
> (2) Comply with a civil, criminal, or regulatory inquiry . . .
> (3) Cooperate with law enforcement agencies . . .
> (4) Exercise or defend legal claims.
> (5) Collect, use, retain, sell, or disclose information that is deidentified . . .
> (6) Collect or sell a consumer's personal information if every aspect of that conduct takes place solely outside California. . . .

Some of these provisions are relevant to our analysis of the question, below.

Regulation, Enforcement, and the Future of the CCPA

The Legislature enacted the CCPA late in 2018 and the statute became operative January 1, 2020.[40] The delayed operative date allowed time for the business community and privacy professionals to adjust to the new rules and for the administrative rulemaking process to run its course. The Legislature adopted a number of amendments to the Act before it became operative.[41]

---

[37] Cal. Code Regs., tit. 11, § 999.313(c)(4).

[38] Civ. Code, § 1798.140, subd. (*o*).

[39] Civ. Code, § 1798.145, subds. (c), (d), (e), (g).

[40] Stats. 2018, c. 55 (A.B.375), § 3, eff. Jan. 1, 2019, operative Jan. 1, 2020.

[41] See Westlaw, Practical Law Practice Note w-017-4166, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

The CCPA directed the Attorney General to adopt regulations by July 1, 2020, as needed to address an extensive list of issues including refining definitions and establishing procedures for businesses to verify and comply with requests.[42] Most relevant for present purposes is the provision authorizing the Attorney General to establish "any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights."[43]

Throughout 2019 and well into 2020, the Department of Justice gathered and analyzed a mass of information and public comment in preparation for proposing final regulations.[44] The Attorney General submitted proposed regulations and supporting materials to the Office of Administrative Law for its consideration in June 2020, and the regulations became operative on August 14, 2020.[45] A set of amendments to the regulations went into effect March 15, 2021.[46] The regulations do not specifically address the question presented here.

The Attorney General's power to enforce the CCPA took effect on July 1, 2020.[47] The Attorney General has authority to seek injunctive relief and civil penalties, with enhanced penalties for intentional violations of the statute.[48] Consumers have a limited private right of action under the statute for a data breach caused by a business's failure to use reasonable security measures, but not for any other violations of the statute.[49]

The Consumer Privacy Rights Act of 2020, which was approved by voters as Proposition 24 in November 2020, amends and builds on the CCPA.[50] The CPRA goes into effect on January 1, 2023, and enforcement is slated to begin July 1, 2023 under the

---

[42] See generally Civ. Code, § 1798.185.

[43] Civ. Code, § 1798.185, subd. (a)(3).

[44] See Rulemaking Files available at https://oag.ca.gov/privacy/ccpa/regs (as of Mar. 9, 2022).

[45] Cal. Code Regs., tit. 11, § 999.300 (history); see generally Cal. Code Regs., tit. 11, §§ 999.300-999.341.

[46] Cal. Code Regs., tit. 15, §§ 999.306, 999.315, 999.326, 999.332.

[47] Civ. Code, § 1798.185, subd. (c).

[48] Civ. Code, § 1798.155, subd. (b).

[49] Civ. Code, § 1798.150.

[50] Initiative Measure (Prop. 24) approved Nov. 4, 2020.

newly formed California Privacy Protection Agency.[51] The CPRA will adjust the threshold size for businesses covered by the statute, exempting more small businesses going forward. The new law will also expand consumer privacy rights in ways generally consistent with the European Union rules, including enhanced protection for sensitive personal information, and a right to request corrections to inaccurate personal information. The amendments to the CCPA introduced by the CPRA do not change the conclusions presented in this opinion.

ANALYSIS

Introduction

Assemblymember Kiley asks whether a consumer's right to receive the specific pieces of personal information that a business has collected about that consumer applies to internally generated inferences. For purposes of the CCPA, "inference" means "the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data."[52] An inference is essentially a characteristic deduced about a consumer (such as "married," "homeowner," "online shopper," or "likely voter") that is based on other information a business has collected (such as online transactions, social network posts, or public records). Some businesses create inferences using their own proprietary methods, and then sell or transfer the inferences to others for commercial purposes.[53] Examples drawn from academic papers in 2018 show that seemingly innocuous data points, when combined with other data points across masses of data, may be exploited to deduce startlingly personal characteristics.[54] Studies show,

---

[51] 2020 Cal. Legisl. Service Prop. 24, § 31. The new agency will have rulemaking authority under the CPRA (Civ. Code, § 1798.185, operative Jan. 1, 2023), as well as power to enforce the CPRA through administrative actions (Civ. Code, § 1798.199.40, subd. (a), operative Jan. 1, 2023). The Attorney General will retain authority to enforce the statute through civil investigative and enforcement powers. (Civ. Code, § 1798.199.90, operative Jan. 1, 2023.)

[52] Civ. Code, § 1798.140, subd. (m).

[53] Beckett, *Everything We Know About What Data Brokers Know About You* (Jun. 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

[54] Lally, *Examples of Data Points Used in Profiling* (2018) available at https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf (as of Mar. 9, 2022), and as an attachment to Privacy International, *A Snapshot of Corporate Profiling* (Apr. 9, 2018) (attachment labeled Data Points Used in Tracking) https://www.privacyinternational.org/long-read/1721/snapshot-corporate-profiling.

among other things, that a person's date and place of birth, in combination with public databases, can be used to predict their social security number; phone data can be used to predict friendships with 95 percent accuracy; data about mobile phone behavior (such as running out of battery) can be used to predict credit-worthiness; and Facebook "likes" can be used to predict a wide array of sensitive personal attributes such as age, gender, race, ethnicity, sexual orientation, political views, and personality traits.[55]

As discussed below, the plain language of the statute, as well as the legislative history, persuade us that the CCPA purposefully gives consumers a right to receive inferences, regardless of whether the inferences were generated internally by the responding business or obtained by the responding business from another source. At the same time, the CCPA does not require businesses to disclose their trade secrets in response to consumers' requests for information.

The CCPA Generally Requires Businesses to Disclose Internally Generated Inferences to Consumers.

As always when we undertake to interpret a statute, we start by examining the text, giving the language its usual meaning in order to understand the intent of the legislators. The words of a statute must be construed in context and sections relating to the same subject must be harmonized to the extent possible.[56] Here, the logical entry point to the text is the CCPA's definition of "personal information." Personal information, as noted briefly above, includes "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."[57] But that is just the beginning of the definition. The section goes on from there to add both breadth and specificity, extending to eleven subparts. The language most relevant to our analysis directs that:

> (*o*)(1) . . . Personal information includes, but is not limited to, the following 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:
> [. . .]
> (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

---

[55] See *id.* at pp. 5, 8-11.

[56] See, e.g., *Dyna-Med, Inc.* v. *Fair Employment & Housing Com*. (1987) 43 Cal.3d 1379, 1386-1387.

[57] Civ. Code, § 1798.140, subd. (*o*)(1).

This text makes the initial stage of our analysis straightforward. "Inferences" are themselves "personal information" for purposes of the CCPA (and therefore disclosable) when two conditions exist. First, the inference is drawn "from any of the information identified in this subdivision." Second, the inference is used to "create a profile about a consumer," or in other words to predict a salient consumer characteristic.

As to the first condition, an inference must be drawn from "information identified in this subdivision," that is, subdivision (o) of Civil Code section 1798.140. Subdivision (o) identifies a vast array of information, including but not limited to:

- personal identifiers (such as names, addresses, account numbers, or identification numbers);
- customer records;
- characteristics of protected classifications (such as age, gender, race, or religion);
- commercial information (such as property records or purchase history);
- biometric information;
- online activity information;
- geolocation data;
- "audio, electronic, visual, thermal, olfactory, or similar information";
- professional or employment information; education information;
- and inferences drawn from any of the above.[58]

We can see that this array includes not only information typically obtained directly from consumers (such as address and income), but also many kinds of information that are a matter of public record (such as information on property listings and tax rolls). Subdivision (o) draws no distinction between public and private sources. It follows that, for purposes of responding to a request to know, it does not matter whether the business gathered the information from the consumer, found the information in public repositories, bought the information from a broker, inferred the information through some proprietary process of the business's own invention, or any combination thereof.[59] If the business

[58] Civ. Code, § 1798.140, subd. (*o*)(1)(A)-(K).

[59] Cf. Civ. Code, § 1798.140, subd. (*o*)(2) ("personal information" does not include public records).

holds personal information about a consumer, the business must disclose it to the consumer on request.

We emphasize that, once a business has made an inference about a consumer, the inference becomes personal information—one more item in the bundle of information that can be bought, sold, traded, and exploited beyond the consumer's power of control. Accordingly, inferences satisfy the first condition of the "personal information" inquiry regardless of whether they have been generated internally by the responding business or received from another source.

The second condition of a disclosable inference, that the personal information must be used to "create a profile about a consumer," narrows the set of inferences that must be disclosed. It rules out situations where a business is using inferences for reasons other than predicting, targeting, or affecting consumer behavior. For instance, a business might combine information obtained from a consumer with online postal information to obtain a nine-digit zip code to facilitate a delivery and completion of a particular transaction. But 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. 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. Under the CCPA, the inference must be disclosed to the consumer, even if the public information itself need not be disclosed in response to a request for personal information.[60]

Our reading of the text is confirmed by evidence of legislative purpose. The Senate Judiciary Committee's analysis of the CCPA bill spotlights the Legislature's concern about the exploitive tendencies of collecting masses of information and using it to identify and affect unwitting consumers. The analysis specifically referred to the practices of Cambridge Analytica, in which a certain app—presented to Facebook users as a personality test—was used to gather masses of personal information.[61] The information was then used to draw inferences about millions of individuals, including

---

[60] Compare Civ. Code, § 1798.140, subd. (*o*)(1)(K) with Civ. Code, §1798.140, subd. (*o*)(2).

[61] See *In re: Facebook, Inc. Consumer Privacy User Profile Litigation, supra,* 402 F.Supp.2d at 777.

their political party and voting behavior, and those inferences were used to target political advertising for the purpose of influencing the outcome of the 2016 presidential election.[62]

But Cambridge Analytica is far from the only example of mischief resulting from the creation and use of inferences by businesses. Inferences are one of the key mechanisms by which information becomes valuable to businesses, making it possible to target advertising and solicitations, and to find markets for goods and services. In some cases, marketing tactics are so tailored that they feel intrusive or unsettling to consumers.[63] In other cases, consumers may never know that they are being excluded from seeing certain ads, offers, or listings based on discriminatory automated decisions.[64] In almost every case, the source as well as the substance of these inferences is invisible to consumers.[65] In light of all these circumstances, inferences appear to be at the heart of the problems that the CCPA seeks to address.

The Requestor's letter suggests an argument that inferences need not be disclosed to consumers because inferences are information that has been generated internally by a business, not collected from the consumer within the meaning of Civil Code section 1798.110, subdivision (a). That subdivision states: "A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer . . . [t]he specific pieces of personal information it has collected about that consumer." We disagree with that argument.

Tellingly, the CCPA gives consumers the right to receive all information collected "about" the consumer, not just information collected from the consumer.[66] When a business creates (or buys or otherwise collects) inferences about a consumer, 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. Thus, in light of the plain meaning of section 1798.140, subdivision (o), inferences must be disclosed to the consumer upon request.

---

[62] *Ibid.*

[63] See Bill Analysis, Sen. Com. On Jud., AB 375 (2017-2018 Reg. Sess.), as amended June 25, 2018, pp. 1-2, 16.

[64] See Lally, *supra*, at pp. 28-39.

[65] Inferences can be especially painful for consumers who are tagged with incorrect or outdated inferences of a sensitive nature, such as pregnancy or substance addiction.

[66] Civil Code, § 1798, subd. (a)(5) ("A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer . . . [t]he specific pieces of personal information it has collected about that consumer.")

The CCPA Does Not Require Businesses to Disclose their Trade Secrets

The opinion request also suggests that internally generated inferences may constitute a business's intellectual property. A similar concern came up repeatedly during the rulemaking process, with commenters suggesting that disclosure of internally generated inferences could reveal trade secrets.[67] But 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. 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.

It is beyond the scope of this opinion to address whether any particular kind or class of internally generated inference might be protected from disclosure because it constitutes a trade secret. Under California's Uniform Trade Secrets Act,[68] a trade secret is essentially information that derives independent economic value from not being generally known to the public or others who can obtain economic value from its use or disclosure, and as to which the owner exerts reasonable efforts to maintain secrecy.[69] In order to show the existence of a trade secret, an owner must identify the secret with "reasonable particularity."[70] The Act permits a person to sue for injunctive relief and damages when their protected trade secrets are obtained by "improper means." Under the Act, the burden is on the trade secret holder to prove both the existence of a trade secret, and somebody's use of improper means to obtain it.[71] "Improper means" does not include reverse engineering.[72]

While we cannot answer fact-specific questions about whether particular inferences could be protected as trade secret, we can answer the general legal question whether the CCPA requires businesses to disclose trade secrets: It does not. We believe the most relevant language is this: "The obligations imposed on businesses by this title shall not restrict a business' ability to: Comply with federal, state, or local laws."[73] The CPRA

[67] Records of official rulemaking are available at https://oag.ca.gov/privacy/ccpa/regs (as of Mar. 9, 2022).

[68] See Civ. Code, § 3426.1, subd. (d).

[69] Civ. Code, § 3426.1, subd. (b).

[70] Code Civ. Proc., § 2019.210 (pleading requirement for trade secret claim).

[71] See Civ. Code, § 3426.1.

[72] Civ. Code, § 3426.1, subd. (a).

[73] Civ. Code, § 1798.145, subd. (a)(1). To date the Attorney General has not found it necessary to promulgate regulations specifically related to intellectual property.

amends the scope of the Attorney General's rulemaking slightly, to include "any exceptions necessary to comply with state or federal law, *including those relating to trade secrets and intellectual property rights . . . with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.*"[74]

California law protects intellectual property, including trade secrets, as demonstrated by its adoption of the Uniform Trade Secrets Act. The text of both the CCPA and the CPRA contain language indicating an intent to protect intellectual property. When a trade secret exists, the CCPA will not require its disclosure to a consumer. However, a business that denies a request "in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA" must explain the nature of the information and the basis for its denial.[75] A blanket assertion of "trade secret" or "proprietary information" or the like would not suffice; the general import of the regulations is that a business must respond to requests in a meaningful and understandable way.[76]

In sum, we conclude 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. A business that withholds inferences on the ground that they are protected trade secrets bears the ultimate burden of demonstrating that such inferences are indeed trade secrets under the applicable law.

---

[74] Civ. Code, § 1798.185, subd. (d)(3) (emphasis added), as amended by Initiative Measure Prop. 24, § 21, approved Nov. 3, 2020, eff. Dec. 16, 2020, operative Jan. 1, 2023.

[75] Cal. Code Regs., tit. 11, § 999.313(c)(5).

[76] See generally Cal. Code Regs., tit. 11, §§ 999.305(a)(2) (disclosures must be easy to read and understandable to consumer), 999.306(a)(2) (same), 999.307(a)(2) (same), 999.308(a)(2) (same).