CALIFORNIA CONSUMER PRIVACY ACT
NON-BINDING GUIDANCE

Foreword

The ANA works tirelessly to advocate for and support the needs of members across a wide variety of legislative and regulatory issues at the state and federal levels. One law that has become an area of significant consideration for marketers and consumers is the recently enacted **California Consumer Privacy Act** (CCPA). The law provides important privacy protections for consumers and imposes new responsibilities on data providers, brands, advertisers, and a host of others in the advertising and marketing industry.

In response to the CCPA, the ANA has taken several important steps to help members navigate and interpret the law's requirements and develop strategies to help facilitate compliance. This document, titled the **California Consumer Privacy Act Guidance**, provides a set of **nonbinding** principles and best practices to assist ANA members and the industry in meeting the requirements of the CCPA.

The Guidance was created by ANA member data providers, with assistance from Venable LLP, in order to share recommendations for managing and protecting consumer privacy. It is important to note that there is no one way to meet the CCPA requirements. This document, as the title implies, provides ANA members and the industry with guidance for just one path forward.

The Guidance addresses four distinct situations.

- A model response to a consumer access request made pursuant to the CCPA
- Guidance to an approach to returning household data in response to an access request
- Guidance addressing personal information collection and inferences
- Guidance about verifying a consumer's request to opt out of the sale of personal information

This document also considers certain provisions of the California Attorney General's October 11, 2019, proposed regulations implementing the CCPA. The ANA will update this Guidance document upon finalization of the proposed regulations and as needed thereafter to ensure you have the latest information and direction for moving forward with the CCPA.

Other tools the ANA is making available to members as we all navigate the CCPA include:

- A member-only webinar to discuss the CCPA Guidance is schedule from 2-3 p.m. on Monday, November 25. Register now.
- A mainstage discussion of privacy and the CCPA will take place at the Masters of Data and Technology Conference, March 2-4, 2020

- Regulatory Rumblings Blog post
- ANA Marketing Knowledge Center (content library)
- ANA Government Relations State Privacy Legislation materials

The ANA continues to work on your behalf as we traverse the legal and regulatory landscape. Initiatives such as Privacy for America, established by the ANA, 4As, IAB, and NAI, is a coalition that supports the enactment of federal consumer data privacy and security legislation. If you have questions about the CCPA, Privacy for America, or other state or federal legislation impacting marketers' ability to manage privacy issues, please reach out to:

Dan Jaffe (djaffe@ana.net)	Bill Tucker (btucker@ana.net)
Group EVP	Group EVP
Government Relations	Industry Relations

The Association of National Advertisers ("ANA") California Consumer Privacy Act Guidance (the "Guidance") is designed to provide data providers, a subset of the marketing solutions provider constituency of ANA's membership, with approaches for facilitating compliance with the California Consumer Privacy Act ("CCPA"). The Guidance reflects ANA's long-standing policy of assisting its members with developing strategies for complying with laws and self-regulatory codes that further the ethical and responsible use of data.

ANA strongly supports the underlying goals of the CCPA. Privacy is an important value that deserves meaningful consideration in the marketplace. To that end, ANA has developed this Guidance in an effort to help bring clarity to the data provider industry and further CCPA compliance. The approaches listed in the Guidance represent risk-based suggestions for data providers to consider in the context of efforts to comply with the CCPA.

The Guidance proceeds in four parts, setting forth: (1) a model response to a consumer access request made pursuant to the CCPA; (2) guidance discussing an approach to returning household data in response to an access request; (3) guidance addressing personal information collection and inferences; and (4) guidance about verifying a consumer's request to opt out of the sale of personal information. This Guidance considers certain provisions set forth in the California Attorney General's October 11, 2019 proposed regulations implementing the CCPA and will be updated upon the finalization of those regulations and as needed thereafter.

The Guidance that follows is not legal advice. Companies should follow all developments, including ongoing rulemaking efforts by the California Attorney General, and should consult with their own counsel.

CCPA GUIDANCE
MODEL RESPONSE TO A CONSUMER ACCESS REQUEST MADE PURSUANT TO THE CALIFORNIA CONSUMER PRIVACY ACT[1]

Date: [Insert date of response, which should be within 45 days of request date]

[Company] provides this response to your request dated [insert date of request] pertaining to [insert name of the consumer], made pursuant to the California Consumer Privacy Act ("CCPA") ("Access Request").[2]

I. CATEGORIES OF PERSONAL INFORMATION COLLECTED ABOUT YOU

[Company] collects personal information about you in its regular course of business. Specific pieces of personal information [Company] has collected about you in the past twelve (12) months are provided in **Appendix A**. In the past twelve (12) months, [Company] has collected the following categories of personal information about you: [Practice Note: Provided below are examples of the types of data that could be reported in this section. Provide the categories as applicable. Underneath **all categories listed below**, insert the business or commercial purpose for collecting the category of personal information as demonstrated in the example under "Personal and online identifiers." Or, if you collect all categories of personal information for the same business and commercial purposes, you may provide a disclosure to this effect in paragraph form here.] [**ALTERNATIVE OPTION**: In the past twelve (12) months, Company has collected the categories of personal information identified in **Appendix B** about you.[3]]

- Personal and online identifiers

  E.g., Name, alias, postal address, online identifiers, IP address, email address, account name, Social Security number, driver's license number, passport number, state identification card number, or similar identifiers [Practice Note: Information in italics throughout this document should not be returned to the consumer; this information is intended to provide you with a description of the types of information that may fall within the listed data element.]

  - **EXAMPLE BUSINESS/COMMERCIAL PURPOSES DISCLOSURE:** We collect personal and online identifiers for business purposes, including [Insert as applicable: internal research, internal operations, auditing, detecting security incidents, debugging, short-term and transient use, fulfilling and improving our services, quality control, and legal compliance]. We collect personal and online identifiers for commercial purposes, including [Insert as

[1] This guidance is not legal advice. Compliance with the CCPA is a novel area. Companies should follow all developments, including ongoing rulemaking efforts by the California Attorney General, and should consult with their own counsel.
[2] Proposed CCPA regulations refer to the access right as a "request to know." Cal. Code Regs. tit. 11, § 999.301(n) (proposed Oct. 11, 2019).
[3] The categories listed in **Appendix B** are derived from the text of the CCPA. These standard terms could be used by industry as data categories.

applicable: sharing such information with our clients who typically use the information for their marketing, advertising, authentication, identity resolution, fraud prevention, and/or fulfillment purposes.]

- Categories of personal information described in Cal. Civ. Code § 1798.80(e)

  E.g., telephone number; signature; physical characteristics or description; insurance policy number; financial information, including financial or payment card account numbers

- Characteristics of protected classifications under California or federal law

  E.g., race; color; religion; sex/gender (includes pregnancy, childbirth, breastfeeding and/or related medical conditions); gender identity, gender expression; sexual orientation; marital status; medical condition; military or veteran status; national origin; ancestry; disability (mental or physical including HIV/AIDS, cancer, and genetic characteristics); genetic information; request for family care leave; request for leave for an employee's own serious health condition; request for Pregnancy Disability Leave; retaliation for reporting patient abuse in tax-supported institutions; age (over 40); etc.[4]

- Commercial or transactions information

  E.g., records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies

- Biometric information

  E.g., per the definition of the term in the CCPA, physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can 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

- Internet or other electronic network activity information

  E.g., browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement

  E.g., online interests, such as information about categories of consumer interests derived from online usage

---

[4] *Protected Classes*, CALIFORNIA STATE SENATE, https://www.senate.ca.gov/content/protected-classes.

- Geolocation data
- Sensory information

  E.g., audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information
- Education information
- Inferences about your predicted characteristics and preferences

  E.g., inferences drawn to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

  E.g., median age, wealth rating and median income
- Other information about you that is linked to personal information above

  E.g., life events, such as consumers who have recently moved or purchased a home

II. CATEGORIES OF SOURCES FROM WHICH YOUR PERSONAL INFORMATION IS COLLECTED

[Company] collects personal information from different sources. In the past twelve (12) months, [Company] has collected personal information about you from the following categories of sources: [Practice Note: Underneath all sources listed below, insert the categories of data listed in Section I that came from the applicable source, *e.g.*, granular categories or "All categories of data listed in Section I were collected from this source."] [**ALTERNATIVE OPTION**: Consider including this information in a chart similar to **Appendix B**.]

- Apparel & Accessory Companies
- Automotive Companies
- Business to Business Companies
- Parenting Product Companies
- Consumer Packaged Goods Companies
- Inquiries About Products or Services
- Consumer Survey Companies
- Surveys from Consumers/Self-Reported Data
- Data Compiling Companies
- Health and Wellness Product and Service Companies

- Electronics Companies
- Financial Services Companies
- Food & Beverage Companies
- Gift Product Companies
- Lifestyle & Interest Product Companies
- Not for Profit Organizations
- Public or Government Entities[5]
- Publishing Product Companies
- Telecommunications Companies
- Travel, Leisure & Entertainment Companies

III. CATEGORIES OF THIRD PARTIES TO WHOM YOUR PERSONAL INFORMATION WAS SOLD, BY CATEGORY OF PERSONAL INFORMATION

In the past twelve (12) months, [Company] has sold the following categories of personal information about you to the following categories of third parties: [Practice Note: Underneath all categories of third parties listed below, insert the categories of data listed in Section I that were sold to the applicable third party, *e.g.*, granular categories or "All categories of data listed in Section I were sold." Also insert the business or commercial purposes for which such information was sold.] [**ALTERNATIVE OPTION**: Consider including this information in a chart similar to **Appendix B**.]

- Advertising/Marketing Companies
- Advertising Networks[6]
- Internet Service Providers
- Apparel & Accessory Companies
- Automotive Companies
- Business Services/Agencies

[5] Per proposed CCPA regulations, businesses must disclose government entities from which public records are obtained as sources. Cal. Code Regs. tit. 11, § 999.301(d) (proposed Oct. 11, 2019).

[6] Proposed CCPA regulations define "categories of third parties" as "types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers." Cal. Code Regs. tit. 11, § 999.301(e) (proposed Oct. 11, 2019). The enumerated examples of categories of third parties are included in this list, in addition to others.

- Business to Business Companies
- Parenting Product Companies
- Communication Services Companies
- Consumer Packaged Goods Companies
- Consumer Services Companies
- Health and Wellness Product and Service Companies
- Marketing Data Companies
- Data Analytics Providers
- Operating Systems and Platforms
- Social Networks
- Consumer Data Resellers
- Educational Institutions & Companies
- Electronics Companies
- Energy and Utility Companies
- Financial Services Companies
- Food & Beverage Companies
- Gift Product Companies
- Lifestyle & Interest Product Companies
- Manufacturing Companies
- Not for Profit Organizations
- Publishing Product Companies
- Technology/Computer Software Companies
- Telecommunications Companies
- Travel, Leisure & Entertainment Companies
- Affiliates not under the [Company] brand

- Public or Government Entities[7]

IV. CATEGORIES OF THIRD PARTIES TO WHOM YOUR PERSONAL INFORMATION WAS DISCLOSED FOR A BUSINESS PURPOSE, BY CATEGORY OF PERSONAL INFORMATION [Practice Note: This section pertains to personal information that has been disclosed for a business purpose. If you do not disclose personal information for a business purpose, omit this section.]

In the past twelve (12) months, [Company] has also disclosed personal information about you for our business operations purposes. [Company] has disclosed the following categories of personal information about you to the following categories of third parties: [Practice Note: Underneath all categories of third parties listed below, insert the categories of data listed in Section I that were disclosed for a business purpose to the applicable third party, *e.g.*, granular categories or "All categories of data listed in Section I were disclosed for a business purpose." Also insert the business or commercial purposes for which such information was disclosed.] [**ALTERNATIVE OPTION**: Consider including this information in a chart similar to **Appendix B**.]

- Service Providers[8]
- Affiliates not under the [Company] brand
- Public or Government Entities[9]
- Advertising Networks[10]
- Internet Service Providers
- Data Analytics Providers
- Operating Systems and Platforms
- Social Networks
- Consumer Data Resellers
- [Insert other "categories of third parties" as applicable. This term means types of entities that do not collect personal information directly from consumers, including

[7] Per proposed CCPA regulations, businesses must disclose government entities as categories of third parties to whom personal information was sold. Cal. Code Regs. tit. 11, § 999.301(e) (proposed Oct. 11, 2019).
[8] This category is optional, as service providers are not third parties per the CCPA's definitions of the terms. Cal. Civ. Code §§ 1798.140(v), (w).
[9] Per proposed CCPA regulations, businesses must disclose government entities as categories of third parties to whom personal information was disclosed for a business purpose. Cal. Code Regs. tit. 11, § 999.301(e) (proposed Oct. 11, 2019).
[10] Proposed CCPA regulations define "categories of third parties" as "types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers." Cal. Code Regs. tit. 11, § 999.301(e) (proposed Oct. 11, 2019). The enumerated examples of categories of third parties are included in this list, in addition to others.

but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers. Cal. Code Regs. tit. 11, § 999.301(e) (proposed Oct. 11, 2019).]

CCPA GUIDANCE
HOUSEHOLD DATA[11]

Below we provide guidance on responding to a consumer access request involving household data.[12] The California Consumer Privacy Act ("CCPA") requires a business to provide a California consumer with access to the personal information it has collected about that consumer, which includes information reasonably capable of being associated with the consumer or the consumer's household.[13] This guidance provides a suggested approach for businesses to contend with the requirement to provide household-level data in response to a CCPA access request when such data may reveal personal information about another member of the household—a consumer that is not the subject of the access request. As discussed in more detail below, a business should return: (1) personal information reasonably capable of being associated with the individual that is the subject of the verified request and (2) aggregate household-level data that is associated with the requesting consumer only and no other consumers that are part of the same household, if a consumer that does not maintain a password protected account with the business makes an access request.

I. Legal Standard. The term personal information means "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*."[14] "Household" means "a person or group of people occupying a single dwelling."[15] The CCPA requires a business that collects personal information about the consumer to disclose that information to the consumer upon a verifiable request.[16] Businesses must verify a consumer request for household information pursuant to Article 4 of the proposed CCPA regulations.[17]

If all consumers in a household jointly request access to "specific pieces of information for the household," the business must comply with the request so long as all the members of the household have been verified pursuant to the requirements under the proposed regulations.[18] If a consumer does not maintain a password protected account with a business, the business is not required to return specific household data to the requestor. Instead, the business may provide "aggregate household information" in response to a consumer access request if the consumer does not maintain an account with the business.[19] The CCPA defines "aggregate" as "information that relates to a group or category of consumers, from which individual consumer

---

[11] This guidance is not legal advice. Compliance with the CCPA is a novel area. Companies should follow all developments, including ongoing rulemaking efforts by the California Attorney General, and should consult with their own counsel.
[12] Proposed CCPA regulations refer to the access right as a "request to know." Cal. Code Regs. tit. 11, § 999.301(n) (proposed Oct. 11, 2019).
[13] Cal. Civ. Code §§ 1798.100, 110, 115, 130, 140(o)(1).
[14] *Id*. at § 1798.140(o)(1) (emphasis added).
[15] Cal. Code Regs. tit. 11, § 999.301(h) (proposed Oct. 11, 2019).
[16] Cal. Civ. Code § 1798.100, 110.
[17] Cal. Code Regs. tit. 11, §§ 999.323 – 326 (proposed Oct. 11, 2019).
[18] *Id*. at § 999.318(b).
[19] *Id*. at § 999.318(a).

identities have been removed, that is not linked or reasonably linkable to any consumer or household."[20]

II. Suggested Approach. The proposed regulations do not define the terms "aggregate household information," which may be returned upon the request of a consumer that does not maintain a password protected account with the business, or "specific pieces of information for the household," which may be returned only if all members of the household jointly request the information and are verified pursuant to the proposed regulations. However, the CCPA's definition of "aggregate" implies that such information cannot be linked or reasonably linkable to any one consumer. As a result, businesses should consider returning the personal information that is reasonably capable of being associated with the requesting consumer *and* household-level data that is associated *only* with the requesting consumer in response to an access request. Businesses should not return household-level data to a consumer if such data might reveal personal information about another member of the household and thereby adversely affects the privacy of another member of the household.

Depending on the type of household-level data involved, returning household-level data in response to a consumer's access request could jeopardize the privacy rights the CCPA extends to other members of the consumer's household. For example, a business may hold aggregate data about the income of a particular household in California. A business may determine that if it were to provide this aggregate household-level income data in response to a request from a consumer that has another roommate in her or his household, such household-level income data could reveal personal information about the roommate's income to the requesting consumer. This result may not be privacy protective, as it has the potential to inadvertently divulge information about consumers to members of their households. In particularly extreme circumstances, such as domestic violence situations or cases where a consumer may share a household with an abusive spouse, the CCPA requirement to return household-level data to consumer could present a safety risk in addition to being contrary to consumers' privacy rights. On the other hand, some types of household level data may not create this type of risk to other household members' privacy rights. For example, a business might reasonably determine that returning information about the likely presence of a pet in the household is not likely to result in adverse privacy impacts to other members of the household.

In addition to the practical concerns inherent in returning household-level data in response to a consumer's CCPA access request, the CCPA states that "[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers."[21] As such, the CCPA itself acknowledges the fact that effectuating certain consumer rights under the law could adversely affect others. Revealing household-level data, even in the aggregate, is an example of such a situation. Returning aggregate household-level data could put the privacy of another member of a requesting consumer's household at risk. Businesses should not be required to sacrifice consumer privacy

[20] Cal. Civ. Code § 1798.140(a).
[21] Cal. Civ. Code § 1798.145(l).

in the name of attempting to achieve clear compliance with the CCPA, and should have reasonable discretion to evaluate the privacy risk arising for a particular type of household data disclosure.

III. Returning Household-Level Data Associated Only with the Requesting Individual. Subject to Section II, because the term personal information includes household-level data, businesses should return both (1) personal information associated with the consumer that is the subject of an applicable CCPA access request and (2) household-level data associated *only* with the requesting individual. A business should have discretion to determine whether any personal information or household-level data that is reasonably capable of being associated with a consumer that is not the subject of a request should be returned based on its potential impacts to the privacy of other members of the household.

The proposed regulations note that a "household" may consist of a *group* of people occupying a single dwelling.[22] However, businesses should reasonably refrain from providing household-level data that is associated with *other* members of a household in response to a specific consumer's access request if such household-level data could have negative privacy implications to other members of the household. In certain circumstances, providing such information could reveal private information or information that may highlight characteristics of and facts about another individual in a household.

Finally, businesses should differentiate between household-level data and personal information associated only with the requesting consumer and household-level data and personal information about another member of the household that is not the subject of a given CCPA access request. For example, in a household composed of Consumer A, Consumer B, and Consumer C, a business should return household-level data associated with Consumer A only and Consumer A's personal information in response to a CCPA access request from Consumer A. Businesses should not return personal information about Consumer B or Consumer C or household-level data associated with Consumer B or Consumer C in response to Consumer A's access request.

[22] Cal. Code Regs. tit. 11, § 999.301(h) (proposed Oct. 11, 2019).

CCPA GUIDANCE
PERSONAL INFORMATION COLLECTION AND INFERENCES[23]

This guidance considers whether business-generated, modeled, and inferred data businesses create, receive, and sell or disclose about consumers are subject to an access request under the California Consumer Privacy Act ("CCPA").[24] While not clear under the text of the law, a reasonable reading of the law, consumer expectations, business proprietary information, and operational practicalities suggest that such inference-related data does not have to be returned to a consumer under the CCPA's obligation to provide the categories and specific pieces of personal information collected about the consumer because these sections of the CCPA are tied to the *collection* of personal information, not just any personal information held about a consumer.[25] However, if a business "collects" inference-related data, such as receiving or buying inferred data from another entity, the business should include such data as part of its response to a verified consumer access request. Additionally, if a business sells its proprietary inferences to a third party or discloses such inferences for a business purpose, the business should disclose that it has sold and/or disclosed inferences pursuant to the CCPA requirement to provide the categories of personal information that the business sold and disclosed about the consumer for a business purpose.[26]

I. Inferences Businesses Create Themselves Are Not "Collected." Businesses create modeled data, business-generated data, and inferences about consumers from the personal information they collect about consumers in the regular course of business. A reasonable interpretation of the CCPA is that this inferred data need not be returned to a consumer in the context of a CCPA access request for information collected by the business because the inferences are created by the business itself and are not "collected".

"Personal information" under the CCPA is "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."[27] Such information explicitly includes "[i]nferences drawn from any [consumer personal] information to create a profile about a consumer reflecting the consumer's preference, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[28] However, the CCPA access right requires a business to give a consumer access to the "categories of personal

[23] This guidance is not legal advice. Compliance with the CCPA is a novel area. Companies should follow all developments, including ongoing rulemaking efforts by the California Attorney General, and should consult with their own counsel. Note that the California Attorney General has issued proposed regulations to help operationalize the CCPA including to provide implementation guidance on "right to know" requests. *S*ee Cal. Code Regs. tit., 11, § 999.301(n) (proposed Oct. 11, 2019). The outcome of this rulemaking may affect the analysis of this section as well as the other sections of this Guidance.
[24] Cal. Civ. Code §§ 1798.100, 110, 115, 130. Proposed CCPA regulations refer to the access right as a "request to know." Cal. Code Regs. tit. 11, § 999.301(n) (proposed Oct. 11, 2019).
[25] Cal. Civ. Code §§ 1798.110(a)(1), (5).
[26] *Id*. at §§ 1798.115(a)(2), (3).
[27] *Id*. at § 1798.140(o)(1).
[28] *Id*. at § 1798.140(o)(1)(K).

information it has *collected* about that consumer" and the "specific pieces of personal information it has *collected* about a consumer."[29] The CCPA defines "collects" as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[30] This definition suggests that the CCPA requirement to give consumers access to the categories and specific pieces of personal information a business has collected about a consumer does not include the inferred data a business may have created from the personal information the business receives in its normal course of business.

A reasonable interpretation of the term "collect" is that it does not include modeled data, inferred data, or other business-generated data, because the definition implies that a business *received* data from the consumer or a third party and did not generate the data on its own. The definition of "collect" suggests that to engage in collection, the personal information must already have existed or have been generated by an entity and obtained by the covered business. The descriptive verbs that define "collect" do not appear to include the concept of generating new data from personal information that a business has already accumulated. As a result, a reasonable interpretation under the law is that business-generated, modeled, and inferred data created from the personal information the business already possesses does not constitute "collection" of personal information under the CCPA. Because such inferences were made by the business itself and were not collected, under this reading the inferences need not be returned pursuant to the CCPA obligation to provide the categories and specific pieces of personal information collected about a consumer. Additionally, there are public policy reasons that support not providing such internally-generated inferences under the access right. For example, inferences may reveal information that is subject to intellectual property protection. Also, certain kinds of inferred data could be meaningless to consumers, and providing inferred data could result in an unreadable, unwieldly, or exceedingly voluminous access disclosure.

II. Inferences Businesses Receive from another Business Are Collected. If a business receives inferred, modeled, or business-generated data from another business, such data would likely be subject to a CCPA access request served on the business because such information is now "collected" under the CCPA.[31] To "collect" personal information under the CCPA is to receive it by any means, including by receiving such personal information from other businesses. As such, any entity that "collects" inferred data from another business should return that data in response to a consumer's CCPA request pursuant to the CCPA requirement to provide the categories and specific pieces of personal information collected about a consumer.[32]

III. Inferences Businesses Sell or Disclose for a Business Purpose Are Subject to a CCPA Access Request. In addition to disclosing the categories and specific pieces of personal information the business has collected about a consumer, the CCPA requires a business also to

[29] *Id*. at §§ 1798.110(a)(1), (5) (emphasis added).
[30] *Id*. at § 1798.140(e).
[31] *Id*. at §§ 1798.100, 110, 115, 130, 140(e).
[32] *Id*. at §§ 1798.110(a)(1), 110(a)(5), 140(e).

provide a list of "[t]he categories of personal information that the business sold about the consumer…" and "[t]he categories of personal information that the business disclosed about the consumer for a business purpose" in response to a CCPA access request.[33] If a business sells the proprietary inferences, modeled, or business-generated data that it created internally to third parties or discloses such data for a business purpose, the business should disclose that it has sold or disclosed inferences for a business purpose in a CCPA access response.

Because of the CCPA requirement to provide a list of the categories of personal information sold about a consumer and the categories of personal information disclosed about the consumer for a business purpose, it is possible that businesses may need to list inferences in the sale-related sections of a CCPA access response and not the collection-related sections of the response. For example, a business that creates its own modeled, business-generated, or inferred data about consumers internally and sells that data to other parties would not have to disclose that it has collected inferred data, but would have to disclose that it sold or disclosed inferred data for a business purpose in a CCPA access response.[34]

[33] *Id*. at §§ 1798.115(a)(2), (3).
[34] *Id*. at §§ 1798.100, 110, 115, 130, 140(e).

CCPA GUIDANCE
VERIFYING A REQUEST TO OPT OUT OF THE SALE OF PERSONAL INFORMATION[35]

The California Consumer Privacy Act ("CCPA") gives consumers the right to opt out of a business's ability to sell personal information.[36] Unlike the CCPA's access and deletion rights, the law does not explicitly require a consumer to submit a "verifiable consumer request" that a business refrain from selling the consumer's personal information. While the CCPA does not require a verifiable consumer request before a business must effectuate an opt out, nothing in the law restricts a business from requesting that consumers verify their identities before acting on an opt out request.

I. The CCPA Does Not Restrict a Business From Requiring Consumers to Verify Themselves. While the CCPA's access and deletion rights are actionable on a business only when a consumer submits a verifiable consumer request,[37] there is no similar triggering mechanism for a consumer to opt out of a business's sale of his or her data.[38] The CCPA states that "[a] consumer shall have the right, at any time, to *direct* a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[39] Proposed CCPA regulations note that "[i]f a business has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request."[40] Businesses must act on an opt out request no later than 15 days after receiving it.[41]

Creating a means of verifying opt out requests will help prevent fraudulent opt outs. For example, third parties could facilitate mass consumer opt outs without ensuring that they have appropriate authority and verifying information from the consumer needed to make such opt outs. The Federal Trade Commission ("FTC") acknowledged issues surrounding mass third party opt outs on behalf of consumers by noting that such large-scale opt outs may not accurately reflect the wishes of consumers.[42] In the context of the CCPA, the potential for problems associated with mass third party opt outs could be exacerbated by the fact that the third parties facilitating such opt outs may not obtain information sufficient to verify a consumer that is requesting to opt out. It is also a concern in a more limited scale. For example, an opt out

---

[35] This guidance is not legal advice. Compliance with the CCPA is a novel area. Companies should follow all developments, including ongoing rulemaking efforts by the California Attorney General, and should consult with their own counsel.
[36] Cal. Civ. Code § 1798.120(a).
[37] *Id*. at §§ 1798.100, 105, 110, 115, 130.
[38] Cal. Code Regs. tit. 11, § 999.315(h) (proposed Oct. 11, 2019).
[39] Cal. Civ. Code § 1798.120(a) (emphasis added).
[40] Cal. Code Regs. tit. 11, § 999.315(h) (proposed Oct. 11, 2019).
[41] *Id*. at § 999.315(e).
[42] Telemarketing Sales Rule, Notice of Proposed Rulemaking, 67 Fed. Reg. 4519 (Jan. 30, 2002); Telemarketing Sales Rule, Final Amended Rule, 68 Fed. Reg. 4638-4639 (Jan. 29, 2003); *see also* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 52-53 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

applied by one household member too broadly could conflict with the preferences and wishes of other members in the household.

In line with the concerns espoused by the FTC and to address issues surrounding verifying consumers submitting CCPA access requests, businesses may want to ensure that they act on an opt out request only for the consumer making the request and do not mistakenly act on the request for a different consumer who may share a name, address, or other identifying details with the requesting consumer.

II. Businesses Can Reasonably Require Verification before Acting on Opt Outs.

Although the CCPA opt out right is not explicitly tied to a business's receipt of a verifiable consumer request, there is nothing in the law or the proposed regulations that restricts a business from requesting information from the consumer to effectuate an opt out request. The proposed regulations note that a request to opt out "need not be a verifiable consumer request," but they do not proscribe a business from taking actions to verify an opt out request.[43] Because the proposed regulations state that a business must "act on" an opt out request no later than 15 days after receiving it, if a business chooses to take steps to verify a consumer's opt out request, such steps should be taken within 15 days of receiving the request to ensure the businesses are opting out the right consumer from information sale. Businesses should take care to use the information they collect to verify consumer identities only for verification purposes, as the CCPA notes that "a business shall… [u]se any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification."[44]

[43] Cal. Code Regs. tit. 11, § 999.315(h) (proposed Oct. 11, 2019).
[44] Cal. Civ. Code § 1798.130(a)(7).

APPENDIX A

SPECIFIC PIECES OF PERSONAL INFORMATION COLLECTED ABOUT YOU

In the past twelve (12) months, [Company] has collected the following specific pieces of personal information about you:

- **[**Insert specific pieces of personal information collected about the consumer.]

APPENDIX B[45]

Category	Description	Collected	Categories of Sources from which Personal Information was Collected[46]	Business / Commercial Purposes for Personal Information Collection, Sale, and Disclosure for a Business Purpose[47]	Categories of Third Parties to Whom Personal Information was Sold or Disclosed for a Business Purpose[48]
Identifiers	*E.g.*, name; alias; postal address; online identifiers; IP address; email address; account name; Social Security number; driver's license number; passport number; state identification card number; or similar identifiers.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Categories of personal information described in Cal. Civ. Code § 1798.80(e).	*E.g.*, signature; physical characteristics or description; telephone number; insurance policy number; financial information, including financial or payment card account numbers; or medical or health insurance information. Information included in this category may be duplicative of information identified in other categories in this Appendix B.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Characteristics of protected classifications under California or federal law	*E.g.*, race; color; religion; sex/gender (includes pregnancy, childbirth, breastfeeding and/or related medical conditions); gender identity, gender expression; sexual orientation; marital status; medical condition; military or veteran status; national origin; ancestry; disability (mental or	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]

[45] Include the categories listed in this **Appendix B** as applicable to the business.
[46] See pages 5 and 6 for examples of categories of sources from which personal information was collected.
[47] See pages 3 through 8 for examples of business or commercial purposes for personal information collection, sale, and disclosure for a business purpose.
[48] See pages 6 through 8 for examples of categories of third parties to whom personal information was sold or disclosed for a business purpose.

	physical including HIV/AIDS, cancer, and genetic characteristics); genetic information; request for family care leave; request for leave for an employee's own serious health condition; request for Pregnancy Disability Leave; retaliation for reporting patient abuse in tax-supported institutions; age (over 40); etc.[49]				
Commercial or transactions information	*E.g.*, records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Biometric information	*E.g.*, physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can 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.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Internet or other electronic network activity information	*E.g.*, browsing history; search history; online interests, such as information about categories of consumer interests derived from online usage; and information on a consumer's interaction with a website, application, or advertisement.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]

[49] *Protected Classes*, CALIFORNIA STATE SENATE, https://www.senate.ca.gov/content/protected-classes.

Geolocation data		YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Sensory information	*E.g.*, audio, electronic, visual, thermal, olfactory, or similar information.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Professional or employment-related information	*E.g.*, current or past job history or performance evaluations.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Education information	*E.g.*, information that is not publicly available personal information, such as those records, files, documents, and other materials which contain information directly related to a student and are maintained by an educational agency or institution or by a person acting for such agency or institution.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Inferences about your predicted characteristics and preferences	*E.g.*, inferences drawn to create a profile about you reflecting your preferences, characteristics, behavior, attitudes; and median age, wealth rating and median income.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]
Other information about you that is linked to personal information above	*E.g.*, any personal information not captured by one of the CCPA-enumerated categories of personal information listed above that may be linked to the personal information above.	YES/NO	[Insert categories of sources as applicable.]	[Insert business / commercial purposes as applicable.]	[Insert categories of third parties as applicable.]