The following is a summary of the proposed regulations published by the Office of the Attorney General on October 10, 2019 (the "Regulations"). They are intended to provide guidance to consumers and businesses subject to the California Consumer Privacy Act ("CCPA").

Notices to Consumers

Notice of Collection: It is obvious from the Regulations that something more than a link to the privacy policy is required but exactly what that means is still unclear. We do know from the Regulations that in addition to the requirements for notice of collection set forth in CCPA[1], businesses that directly collect personal information from consumer must provide in the notice (i) a link to the business' comprehensive privacy policy, and (ii) if selling personal information, the "Do Not Sell My Personal Information" link (if an offline notice a link to the webpage for the link). If the business collects personal information online, instead of providing the "notice of collection" requirements directly in the notice the business can put a link in the notice that directs the consumer to the "notice of collection" provision(s) of the business's privacy policy.

For businesses that don't directly collect information from consumers (e.g., data brokers) but then sell that personal information, they are obligated to confirm that the consumers whose personal information they collect were given the explicit notice of the sale and the opportunity to opt-out. This can be confirmed either by (i) contacting the consumer directly; or (ii) contacting the source of collection. If contacting the source, a signed document from the source stating that notice and opportunity to opt-out were given is required. An example of the notice provided to the consumer must be attached to the signed document.

Notice of the Right to Opt-Out of the Sale of Personal Information: In addition to the CCPA § 1798.135, subdivision (a) requirements, a business that does not have a website or substantially interacts with consumers offline must establish a method that informs consumers of the right to opt-out of the sale. Examples in the Regulations include a paper notice or signage that directs the consumer to a website where the notice can be found.

Businesses that provide the "Do Not Sell My Personal Information" link on the webpage can link to the section of their privacy policy that contains the opt-out information rather than creating a separate opt-out webpage. The notice or privacy policy must include information on using an authorized agent (including any proof necessary to verify the agency), and other methods for submitting opt-out requests. Other methods for providing opt-out submissions include a toll-free number, designated email, a form submitted in person, and a form submitted by mail.

While under the CCPA a business that does not and will not sell personal information is not required to post opt-out notices, the Regulations require the business to include in their privacy policy that they do not and will not sell personal information.

The Office of the Attorney General points out in the Regulations that it is working on a uniform "Do Not Sell My Personal Information" button or logo that it hopes to present for public comment at a later, unspecified date.

[1] C. C. §1798.100(b)

Notice of Financial Incentive: The CCPA requires certain information to be provided in the notice of financial incentive (provide notice of incentive, material terms, and right to withdraw).[2] The Regulations obligate the business to also provide a summary of the financial incentive or price of service difference that is being offered, how the consumer can opt-in to the incentive, why the financial incentive or price of service difference is permitted under the CCPA, a good-faith estimate of the value of the incentive, and the method used to determine the value.

Privacy Policy Requirements: The CCPA specifically talks to online privacy policies[3] and the Regulations clarify that the privacy policy must also include its offline practices in the policy as well[4]. A link to a privacy policy must include the word "privacy" on the business homepage, and if applicable, the download or landing page of the mobile app. The CCPA also lists certain provisions that need to be included in the privacy policy:

- the CCPA's consumer privacy rights (right to know, right to request deletion, right to opt-out of a sale, right to non-discrimination for exercising consumer privacy rights under the CCPA),
- the procedures for consumers to make requests based on their CCPA rights,
- the business's practices of collecting and maintaining consumer personal information,
- how a consumer can designate an authorized agent,
- a designated business contact to answer consumer privacy policy questions,
- the date it was last updated (to ensure compliance with the 12-month privacy policy update requirement of the CCPA, § 1798.130, subdivision (a)(5)), and
- a description of the processes used for parents and guardians of minors to affirmatively authorize the sale of a child's personal information, if the business has actual knowledge that it collects or maintains personal information of a minor (additional requirements when dealing with minors discussed in more detail below).

Handling Consumer Requests

Methods for Submitting Requests to Know, Requests to Delete, and Requests to Opt-In After Opting Out: The Regulations provides examples of additional methods through which consumers can submit requests to know and requests to delete: a designated email, a form submitted in person, and a form submitted by mail. Businesses should provide the same methods for requests to know pursuant to Sections 1798.100, 1798.110, and 1798.115. The Regulations do not require a particular method for requests to delete (which is in contrast to the toll-free number requirement for requests to know). From a risk point of view, it is advisable to have a toll-free number for requests to know and requests to delete, unless you are an exclusively online business, since the statute itself requires that. When determining which methods to use the business should look to the ways in which it interacts with consumers. At least one method **must** reflect how the business primarily interacts with consumers, even if the business is then required to provide three methods of submission. If the business does not **interact with consumers directly** in the ordinary course of the business, at least one method through which consumer can submit requests to know and delete must be provided.

[2] C. C. § 1798.130 (b) (3)
[3] C. C. § 1798.130 (a)(5)

For requests for deletion and requests to opt back in, businesses must provide a two-step verification process. The consumer must first submit a request for deletion or to opt back in and then separately confirm that the request should be processed as requested.

Finally, the Regulations impose a "do not ignore" obligation on businesses who receive requests not properly submitted in accordance with the CCPA or Regulations. The request cannot be simply ignored and the business must either (i) treat the request as if it was properly submitted; or (ii) provide the consumer with the correct method and/or explain any deficiencies that need to be corrected before the request can be processed.

Responding to Request to Know, Requests to Delete, Requests to Opt-In After Opting Out, and Household Data

Requests to Know and Requests to Delete: The Regulations added a new deadline for businesses who receive requests to know and requests to delete. Within ten (10) days of receiving such a request, the business must confirm receipt of the request and explain to the requesting consumer (i) how requests are processed, (ii) the identification verification process, and (iii) when the consumer can expect a substantive response to the request. If the business substantively responds to the request before the 10-day window expires then the business does not need to send the above confirmation. According to the Office of the Attorney General Initial Statement of Reasons, this confirmation of receipt may be prepared in advance and automatically sent in response to a request.

In response to potentially confusing and conflicting timeframes within CCPA for responding to requests to know and delete, the total maximum number of days a business can take to substantively respond is 90 days from the day the request is received by the business (an initial 45 days and a one-time, 45-day extension in certain circumstances).

When a business cannot verify the identity of the consumer who makes the request, the business **must not disclose specific pieces of information**. Instead the business should inform the consumer of the inability to verify, and evaluate the request as if requesting disclosure of categories of personal information. If the business is evaluating a request to **disclose categories of personal information**, and denies the requests in whole or in part based on the inability to verify the identity of the consumer, the business (i) **may** disclose the categories of personal information, and (ii) **must** inform the consumer of the inability to identify, and (iii) **must** direct the consumer to the section of the privacy policy that discusses the collection, maintenance, and sale of personal information.

The Regulations also require the business to weigh the risk to the security of the requested information when evaluating the validity of a request.

In addition, the Regulations helpfully clarify that businesses should **not at any time disclose**: a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers.

If a business must deny a request to know **specific pieces of personal information**, in whole or in part, because of a conflict with federal or state law or a CCPA exception the business should:

- inform the consumer of the denial,

- provide an explanation, and
- if denied in part, disclose the information not denied.

Reasonable security measures must be used when transmitting information to the consumer. If the business has a password-protected account for the consumer, a secure self-service portal may be used.

Responding to Requests to Know: With respect to the substance of responses to requests to know, the disclosure should cover the 12-month period that precedes the date the request to know was received. Individualized responses to requests to know categories of personal information, categories of sources, and categories of third parties are required. It is not acceptable to refer to the privacy policy generally, unless the response is the same for all customers and the privacy policy includes all the information that would be required in an individualized response. For each category of personal information requested the business must provide: (i) the categories of sources, (ii) the business or commercial purpose for the collection; (iii) the categories of third parties the information was sold or disclosed to for a business purpose; and (iv) what the business purposes was in reference to (iii). In addition, the categories must be disclosed in a way that is understandable to the consumer.

Responding to Requests to Delete: We get a lot of questions about this one. The Regulations helpfully provide the following appropriate ways to respond to a request to delete: (i) permanently and completely erase on existing system; (ii) de-identify the personal information; or (iii) aggregate the personal information. With respect to deleting personal information on existing systems, the deletion of the personal information on archived or backup systems may be delayed until the next time the system is accessed or used. The business must provide the requesting consumer with the method that was used to delete the information and disclose that it will keep record of the request pursuant to CCCPA § 1798.105, subdivision (d).

If denying a request to delete personal information, the business **must** inform the consumer of the denial and the basis of the denial. If the basis includes statutory and/or regulatory exceptions, those must be disclosed too. If only some of the personal information is covered by an exception, the information that is not covered should be deleted. In addition, a business can provide a requesting consumer with the option to have only some of the personal information deleted; however, the business must still provide a global option to delete and the global option must be more prevalent than the option to select what information be deleted.

Requests to Opt-Out: Whether providing a separate webpage or linking to the applicable privacy policy section, businesses need to have two methods to submit a request to opt-out. One method must be an interactive webform for consumers to use to submit requests to opt-out online. The other method must coincide with how the business interacts with consumers in the ordinary course of business, using factors such as the manner in which the personal information is sold, technological capabilities, and ease of use by consumers to determine what method is most appropriate.

Significantly, the Regulations state that, if a request is submitted via a user-enabled privacy control, it should be treated as a valid request. They also state that, if submitted through an authorized agent, the business should treat the request as if submitted directly by the consumer.

One very important, newly added deadline in the Regulations requires business to act upon the request to opt-out as soon as feasibly possible, but in any event no later than 15 days after receiving the request.

When preparing to respond to a request to opt-out, the business **must**, in addition to the requirements already set forth in the CCPA, notify any business it **sold** the personal information to in the 90 days preceding the request that they may not further sell the data and then notify the consumer that such notifications have been completed. (It will be interesting to see how IAB and other self-regulatory organizations working on proposed frameworks to address such opt-outs in the ad tech ecosystem address this new 90 day requirement.)

If there is a good-faith, reasonable, and documented belief that the request is not valid then the request may be denied and the consumer should be informed of the denial and the good-faith basis. Unlike requests to know and requests to delete, verification of the request to opt-out is not required.

Requests to Opt-In After Opting Out of the Sale of Personal Information: The Regulations provide that when a consumer has opted out of having personal information sold but then transacts with the business in a way that requires the consumer to be opted-in in order to complete the transaction, businesses may contact the consumer and explain the opt-in requirement and how the consumer can opt back in to complete the transaction.

Requests to Access or Delete Household Information: If a consumer does not have a password-protected account with the business, the business should only provide such household information in the aggregate. If the business receives a joint request for specific personal information or for the deletion on household information, and each member of the household is verified properly (verification discussed in more detail below) the business shall comply with the request.

Service Providers

The Regulations attempt to clarify who is and is not a service provider, but unfortunately they make the determination even more complicated.

First, the Regulations provide that the definition of service providers includes those who provide services to a person or organization but that are otherwise not considered to be a "business" as defined under the CCPA. This is meant to cover service providers for non-profits and government entities.

Second, a person or entity that **collects** personal information directly from consumers and meets all other requirements of a "service provider" under the CCPA will be defined as a service provider for purposes of the CCPA.

Third, the Regulations strictly prohibit a service provider's use of personal information it collected from one business for the benefit of another business, except for security and anti-fraud purposes. It is unclear how this would play out when a service provider positions itself first as a business when collecting the data and then as a service provider when they use the data for a contracted "business purpose" with another business (e.g., for advertising purposes). While the Regulations attempt to clarify this distinction it does little more than state that an entity that considers itself both a business and a service provider is to comply with the CCPA and Regulations concerning any personal information it collects, maintains, or sells outside of its role as a service provider.

Training: The Regulations make clear that all individuals who handle consumer requests pursuant to the CCPA and answer consumer questions regarding the business's privacy practices be fully informed of **all** aspects of the CCPA and Regulations. The CCPA itself only required such individuals to be familiar with certain provisions rather the entire CCPA and now Regulations.

Record Keeping: Businesses are required to (i) keep documentation of requests, (ii) keep the documentation for 24 months; and (iii) include in the documentation how the business responded to the request. If the business chooses to maintain documentation via a ticket or log format it must include: (i) the date and nature of the request, the manner in which it was requested, the date of the business's response, the nature of the response, and the basis for the denial of the request if denied in whole or in part.

One very important mandate in the Regulations not included in the CCPA is the record-keeping requirements imposed on a business that alone, or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of **4 million or more consumers**. If a business meets this definition it must compile annually the number of requests to know, requests to delete, and requests to opt-out that the business received, how many request were complied with in whole or in part, and how many requests were denied. They should also provide the median number of days it took the business to substantively respond to the requests. This information should be disclosed in the privacy policy or posted on the website.

Verification

This section of the Regulations requires businesses to establish, document, and comply with a reasonable method of verifying that the person who submitted the request to know or delete is actually the person who is making the request. This section sets forth the specific requirements for verifying. The business has the responsibility to come up with a reasonable method that is workable for the business, meaning that it can follow the method and accurately document the requests and responses.

To determine the appropriate method companies should:

- If possible, verify the requestor is the consumer based on the personal information already maintained by the business, or use a third-party verification service,
- Avoid collecting certain personal information that is not redacted or encrypted unless necessary to verify; and
- Consider factors such as the type, sensitivity, value of the personal information collected, the risk of harm if access is actually unauthorized, the likelihood the request is fraudulent or malicious, if information can be spoofed, how the business interacts with the consumer, and technology available for verification.

Moreover, businesses should generally avoid requesting additional information to assist with verification unless they cannot verify the identity of the consumer with the information already maintained by the business. If additional information is collected it can only be used for verification, security, and fraud-prevention purposes. And the additional information must be deleted as soon as practical after processing the request, unless keeping the information is necessary to comply with the record keeping requirements noted above.

In addition, whether or not a user maintains an account with the business, the business must implement reasonable security measure to detect any verification activity that may be fraudulent and protect against unauthorized requests to know or delete.

Verification of Password-Protected Accounts: To verify the requestor is the consumer linked to a password-protected account, the business may use the existing authentication methods in place to verify the identity, provided that the business uses reasonable security methods discussed above. Before disclosing and deleting the specified information, businesses must require consumers to re-authenticate themselves. If fraudulent or malicious activity is suspected, the business is prohibited from complying with the request unless through further verification the business determines the activity is not fraudulent or malicious.

Verification of Non-Accountholders: For **requests to know categories of personal information**, businesses must verify the requestor is the consumer to a **reasonable degree of certainty**. A reasonable degree of certainty, for purposes of this requirement, means matching at least two data points of the requestor with two data points maintained by the business on the consumer. And the data points used must be deemed by the business to be reliable for purposes of verification.

For requests to **know specific pieces of personal information**, verification must be to a **reasonably *high* degree of certainty**. This requires matching at least three data points. Plus, the requestor must sign, under perjury and penalty of law, that they are indeed the person they say they are. Such signed documents must be maintained by the business in compliance with the record-keeping provisions of the CCPA and Regulations.

For requests to **delete**, the business must first determine the sensitivity and risk of harm by unauthorized deletion of the personal information to be deleted and then, based on the level of sensitivity and risk of harm, apply either a reasonable degree of certainty or a reasonably high degree of certainty. The same factors that are used to implement an appropriate method of verification (listed above) should be used to determine whether a heightened standard of reasonableness is required.

If a business has no way of implementing a reasonable method of verification for a particular request, in response to such request to know or delete the business must explain there is no reasonable method to verify. And if the business determines that it cannot verify to the appropriate level of reasonable certainty the identity for any of the personal information it maintains, its privacy policy must state that and why. This should be evaluated on an annual basis and documented.

Authorized Agents: When a consumer uses an authorized agent to submit a request to know or delete, a business can require: (i) the authorized agent to submit a written permission with the request to know or delete; and (ii) the consumer to directly verify their identity with the business. If the proof is not submitted, the business may deny the request. This does not apply if the authorized agent is acting under power of attorney pursuant to Probate Code sections 4000 and 4465.

Special Rules Regarding Minors

Minors under the Age of 13: If under the CCPA a business must acquire the affirmative authorization of a parent or guardian to sell the personal information of a minor under the age of 13, the business should implement a reasonable method for determining that the person who provided the affirmative authorization was indeed the parent or guardian. The reasonable method should meet the standard set

forth in the Children's Online Privacy Protection Act. This includes method for the sale of the minor's personal information online and offline. Various methods are provided in regulations issued by the Federal Trade Commission. When the affirmative authorization is received, the business must then inform the parent or guardian of their right to opt-out at a later date and how they can opt-out.

Minors Ages 13 to 16: Business must again establish, document, and comply with a reasonable process that allows minors to opt-in to the sale of their personal information and inform of their right to opt-out at a later date and how they can opt-out.

Non-Discrimination

Financial Incentives and Price of Service Differences ("Incentives"): To prevent an Incentive that is offered only to consumers who opt-in to their personal information being sold from being discriminatory, a business must reasonably relate the value of the incentive to the value of the consumer's data.

Calculating Consumer Data Value for Incentives Purpose: The Regulations provide seven (7) different methods to assess the value of consumer data but also offers a catch-all provision so that businesses can implement a method that is most practical and reliable given their business model, provided that the method is a reasonable and good faith method. In addition, such method must be documented.

Other Non-Discriminatory Acts: The Regulations specify that neither (i) a denial of a request to know, delete, or opt-out permitted by the CCPA and regulations; nor (ii) charging a reasonable fee for complying with a request pursuant to the CCPA, is discriminatory.