PILLAR LEGAL

California Privacy Protection Agency Moves Forward With New Draft Privacy Regulations

U.S. TECH LAW UPDATE[1]

August 29, 2022

By: Greg Pilarowski | Alexandra Ashbrook

I. Introduction

On August 24 and 25, 2022, the California Privacy Protection Agency (the "Agency") held a public hearing on proposed regulations affecting the California Consumer Privacy Act of 2018 (the "2018 Act"), as amended by the Consumer Privacy Rights Act of 2020 (the "2020 Act", and collectively with the 2018 Act, the "CA Privacy Acts"). Amongst its various changes to the 2018 Act, the 2020 Act established the Agency to implement and enforce the CA Privacy Acts.[2] The CA Privacy Acts directed the Agency to update existing regulations to account for the 2020 Act, operationalize new rights and concepts introduced by the 2020 Act, and reorganize and consolidate requirements under the CA Privacy Acts.

The 2018 Act was enacted in late 2018 and became operative on January 1, 2020. Under the 2018 Act, Californians obtained new privacy rights and privacy obligations were imposed upon businesses operating in California. Thereafter, in November 2020, Californian voters approved the 2020 Act,[3] which granted consumers in California new privacy rights including:

- The right to delete personal information that a business collects from them.[4]
- The right to correct inaccurate personal information the business maintains about them.[5]
- The right to know what personal information a business has collected about them, and how the business uses, sells, and shares that information.[6]
- The right to opt out of the sale or sharing of their personal information.[7]
- The right to limit a business' use and disclosure of sensitive personal information about them to certain business purposes.[8]

---

[1] This U.S. Tech Law Update is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This U.S. Tech Law Update may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-474-3258 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: greg@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] Cal. Civ. Code § 1798.199.10.

[3] More information on the 2020 Act's updates to the 2018 Act is available in the Firm's U.S. Tech Law Update "The California Privacy Protection Agency Talks Rulemaking—Are Businesses Ready for New California Data Privacy Rules?"

[4] Cal. Civ. Code § 1798.105.

[5] Cal. Civ. Code § 1798.106.

[6] Cal. Civ. Code §§ 1798.110, 1798.115, 1798.140, subds. (ad), (ah).

[7] Cal. Civ. Code § 1798.120.

[8] Cal. Civ. Code § 1798.125.

In the fall of 2021, the Agency solicited preliminary written comments from the public regarding implementation of the 2020 Act's amendments to the 2018 Act. On June 8, 2022, the Agency approved a set of proposed regulations (the "Draft Regulations") implementing the 2020 Act. Then, on July 8, 2022, the Agency published a notice of proposed action in the California Regulatory Notice Register, beginning the formal rulemaking process. Both the 2018 Act and the 2020 Act include a list of additional regulations for formulation and eventual adoption to further the purposes of the CA Privacy Acts. The 2020 Act directs the Agency to implement such regulations by July 1, 2022, and enforcement of the 2020 Act is set to take place beginning July 1, 2023.[9] Following the public comment period, the Agency may make changes (initiating a new public comment period) or choose to move ahead with the Draft Regulations by issuing the final version of the regulations, releasing a final statement of reasons for the changes, and submitting the regulations to the Office of Administrative Law.[10]

Note that as the Agency moves forward with implementation of the Draft Regulations, the United States does not currently have comprehensive federal data protection legislation. As a result, many states continue to implement state-level privacy legislation:

- *Virginia*. The Virginia Consumer Data Protection Act becomes effective on January 1, 2023.
- *Colorado*. The Colorado Privacy Act becomes effective on July 1, 2023.
- *Connecticut*. The Connecticut Act Concerning Personal Data Privacy and Online Monitoring becomes effective on July 1, 2023.
- *Utah*. The Utah Consumer Privacy Act becomes effective on December 31, 2023.

The United States does, however, continue with its attempts to adopt comprehensive data privacy legislation at the federal level. The latest iteration—the American Data Privacy and Protection Act (the "ADPPA")—is a bipartisan, bicameral data privacy bill. The ADPPA is the first federal data privacy legislation to pass committee, fueling expectations that the bill will ultimately become law and pre-empt many state-level data privacy laws.[11]

II. Collecting and Using Personal Information

The Draft Regulations introduce a new restriction on the collection and use of personal information. In particular, a business's collection, use, retention, and/or sharing of a consumer's personal information must be "reasonably necessary and proportionate" to achieve the purpose(s) for which the personal information was collected—meaning that a reasonable consumer must expect the particular use, retention, or sharing of the personal information.[12] In addition, the Draft Regulations require a business obtain explicit, affirmative consent if it intends to use a consumer's personal information for a purpose that is "unrelated or incompatible with the purpose(s) for which the personal information is collected or processed."[13] For example, a business that provides a mobile flashlight application cannot collect consumer geolocation

[9] Cal. Civ. Code § 1798.185(d).
[10] Regular Rulemaking, OFFICE OF ADMINISTRATIVE LAW (accessed Aug. 26, 2022), https://www.oal.ca.gov/wp-content/uploads/sites/166/2017/05/Regular-Rulemaking-Flowchart_FINAL_June-2014-2.pdf.
[11] Find a summary of H.R. 8152 – 117th Congress (2021-2022) here.
[12] Draft Regulations § 7002(a).
[13] Draft Regulations § 7002(a).

information through its application without the consumer's explicit consent, as the collection of geolocation is not within the reasonable expectations of an average consumer nor reasonably necessary and proportionate to achieve the purpose of providing a flashlight function.[14]

III. Transparency of Communications to Consumers

a. *Format, Design and Implementation*

The new Draft Regulations promulgate new formatting requirements for disclosures and communications with consumers. Such disclosures and communications must be easy to read and understandable (i.e., in straightforward language that avoids technical and legal jargon).[15] Moreover, disclosures must use a format that is readable on smaller screens, be available in languages in which a company conducts its business and be reasonably accessible to consumers with disabilities.[16]

In addition, the Draft Regulations set forth new design principles regarding receipt of 2018 Act requests and consumer consent.[17] In particular:

- The methods of receipt must use language that is easy to understand.
- The path for a consumer to exercise a more privacy-protective option must be easier or symmetrical to the path to exercise a less privacy-protective option.
- The method of receipt must avoid language or interactive elements that may be confusing to a consumer (e.g., double negatives, toggle buttons that do not clearly indicate a choice, unintuitive placement of buttons, et cetera).
- The method of receipt must avoid manipulative language or choice architecture (e.g., wording that guilts or shames a consumer or bundles consent).
- The method of receipt must be easy to execute and not add unnecessary burden or friction to the process by which a consumer submits a request.

b. *Privacy Policy*

Under the Draft Regulations and in line with the 2020 Act, businesses must make new disclosures within their privacy policies, including:[18]

- Identification of the categories of personal information the business has sold or shared to third parties in the preceding 12 months (or a statement that the business has not done so).
- Identification of the specific business or commercial purpose for selling or sharing consumer's personal information.
- A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.

[14] Draft Regulations § 7002(b)(1).
[15] Draft Regulations § 7003(a).
[16] Draft Regulations § 7003(b)(1)-(3).
[17] Draft Regulations § 7004((a)(1)-(5).
[18] Draft Regulations § 7011(e)(1)(A)-(K).

- Identification of the categories of personal information that the business has disclosed for a business purpose to third parties in the preceding 12 months (or a statement that the business has not done so), the categories of third parties to whom the information was disclosed, and the specific business or commercial purpose for disclosing the personal information.
- A statement regarding whether or not the business uses or discloses sensitive personal information, unless exempted under the CA Privacy Acts (see below).

IV. Handling Consumer Requests

a. *"Disproportionate Effort"*

The Agency added a new exclusion from compliance with consumer requests—situations which require "disproportionate effort."[19] Under the Draft Regulations, "disproportionate effort" within the context of a business responding to a consumer request means the time and/or resources expended by the business to respond to the request significantly outweigh the benefit provided to the consumer by responding to the request. Responding to a consumer request may require disproportionate effort when:

- The personal information is not in a searchable or readily accessible format.
- The personal information is only maintained for legal or compliance purposes, is not sold or used for any commercial purpose, and would not materially impact the consumer.

However, a business may not simply avoid putting adequate processes and procedures in place to comply with consumer requests. The business must demonstrate that the time and/or resources needed to comply with the request would be significantly higher than the material impact on the consumer.

b. *Requests to Delete*

The Draft Regulations operationalize the new privacy rights granted by the 2020 Act: the right to deletion and the right to correction of inaccurate personal information (see below). Naturally, pursuant to a request to delete, a business must permanently and completely erase personal information from existing systems (with the exception of archived or back-up systems), deidentify, or aggregate the consumer information.[20] However, the Agency imposes further responsibilities. Pursuant to the Draft Regulations, when a consumer exercises his or her right to delete, a business must notify the business' service providers, contractors, and third parties with whom the business has sold or shared information to delete the consumer's personal information from their records.

However, businesses may refuse a request to delete when complying with such a request involves disproportionate effort or when the business cannot verify the identity of the requestor.[21] When refusing to comply with a request to delete, in whole or in part, a business must provide the consumer with a detailed explanation of the basis for the denial, including any

[19] Draft Regulations § 7001(h).
[20] Draft Regulations § 7022(b).
[21] Draft Regulations § 7022(a), (b)(3), (c)(4), and (f)(1).

conflict with federal or state law, exception to the CA Privacy Acts, or factual basis for contending that compliance would be impossible or involve disproportionate effort.[22] In its Draft Regulation explanation (the "Initial Statement of Reasons"), the Agency states that requiring an explanation is necessary to prevent businesses from abusing the impossibility or disproportionate effort explanation, and allows the consumer and the Agency to hold businesses accountable with relatively little cost to the business.[23]

c. ***Requests to Correct***

As with requests to delete, the Agency operationalizes the right to correct by setting forth the rules and procedures businesses must follow for the submission and handling of requests to correct. In complying with a request to correct, a business must not only correct personal information on existing systems and implement measures to ensure that it remains corrected, but also instruct all service providers, contractors, and third parties that maintain copies of relevant personal information to similarly make such corrections in their respective systems.[24] In addition, the Draft Regulations require the business to inform the consumer that, upon the consumer's request, it will note both internally and to any entity or person with whom it discloses, shares, or sells personal information that the accuracy of the personal information is contested by the consumer.[25]

A business may also deny a request to correct under several circumstances, including:

- If the business determines that the contested personal information is more likely than not accurate based on a "totality of the circumstances," such as the nature of the personal information (i.e., whether it is objective, subjective, unstructured, or sensitive), how the business obtained such information, and any documentation relating to the personal information's accuracy.[26]
- If the business instead deletes the contested personal information, where deletion does not negatively impact the consumer or the consumer consents to deletion.[27]
- Where the business cannot verify the identity of the consumer requesting correction.[28]
- Where there is a conflict with federal or state law, an exception to the CA Privacy Acts applies, the consumer cannot provide accurate documentation to demonstrate inaccuracy of the personal information, or contention that compliance proves impossible or involves disproportionate effort.[29]
- If the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months of receiving the request (unless the consumer provides additional documentation to prove that the information is inaccurate).[30]

[22] Draft Regulations § 7022(f)(1).
[23] Initial Statement of Reasons, § 7022, Subsection (b)(3).
[24] Draft Regulations § 7023(c).
[25] Draft Regulations § 7023(f)(3).
[26] Draft Regulations § 7023(b)(1).
[27] Draft Regulations § 7023(e).
[28] Draft Regulations § 7023(a).
[29] Draft Regulations § 7023 (f)(1).
[30] Draft Regulations § 7023(g).

- Where the business has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive.[31]

Similar to requests to delete, when denying a request to correct, the business must provide the consumer with a detailed explanation of its reasoning for the denial that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request.[32]

d. ***Requests to Opt-Out of Sale/Sharing***

The 2020 Act's amendments to the 2018 Act require the Agency to establish rules and procedures to facilitate and govern the submission of a request to opt-out of the sale or sharing of personal information and govern business compliance with such request.[33] Pursuant to the Draft Regulations, businesses must comply with requests to opt-out of sale and sharing by ceasing to sell and/or share with third parties the consumer's personal information, notify third parties to whom the business has sold or shared the consumer's personal information that the consumer has opted-out, and direct such parties to comply with the opt-out request and forward the request to any other applicable third parties.[34] The business must also provide a mechanism by which the consumer can confirm that his or her request to opt-out was processed by the business.[35] *However, the Draft Regulations further clarify that providing information to service providers or contractors does not constitute a sale or sharing of personal information, and thus the consumer does not have the right to opt-out of this type of sharing*.[36] As discussed below, service providers and contractors receive personal information from consumers from or on behalf of the business pursuant to a contract complaint with the CA Privacy Acts. On the other hand, consumers maintain the right to opt-out of the sale or sharing of personal information with other types of third parties (see below).

e. ***Requests Regarding Sensitive Personal Information***

When the 2020 Act goes into effect, consumers will have the right to limit business' use and disclosure of their sensitive personal information. "Sensitive personal information" under the CA Privacy Acts includes, amongst other things, personal information that reveals a consumer's social security number, driver's license number, state identification number, passport number, precise geolocation, racial or ethnic origin, or religious or philosophical beliefs.[37] The Agency implements this right to limit in the Draft Amendments, setting forth rules and procedures businesses must follow regarding the submission and handling of these requests. In particular, a business that uses or discloses sensitive personal information must provide two methods for submitting requests to limit this use and disclosure, both of which must be easy for consumers to use.[38] Moreover, a consumer request to limit does not need to be "verified" like other types of

[31] Draft Regulations § 7023(h).
[32] Draft Regulations § 7023(f)(2).
[33] Cal. Civ. Code § 1798.185(a)(4).
[34] Draft Regulations § 7026(f)(1)-(3).
[35] Draft Regulations § 7026(f)(4).
[36] Draft Regulations § 7026(f)(1).
[37] Cal. Civ. Code § 1798.140(ae).
[38] Draft Regulations § 7027(b), (c).

requests under the CA Privacy Acts—a business may only ask the consumer for additional information if necessary to complete the request.[39]

Furthermore, the Draft Regulations describe the situations in which a business may use or disclose sensitive personal information *without* offering consumers an ability to limit such use or disclosure:[40]

- To perform services or provide goods reasonably expected by an average consumer (e.g., a consumer's precise geolocation may be used by a mobile application providing the consumer with directions).
- To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
- To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for such actions.
- To ensure the physical safety of natural persons.
- For short-term, transient use (e.g., non-personalized advertising shown as a part of a consumer's current interaction with the business).
- To perform services on behalf of the business, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financings, providing analytic services, providing storage, or other similar services.
- To verify or maintain the quality or safety of a service or device that is owned, manufactured by or for, or controlled by the business, and to improve, upgrade, or enhance such services or devices.

V. Consumer Opt-Outs

a. *New "Alternative" Opt-Out Link*

In the Draft Regulations and in line with the CA Privacy Acts,[41] the Agency provides an option for a single, alternative opt-out link in lieu of posting the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links.[42] The alternative opt-out link must be titled "Your Privacy Choices" or "Your California Privacy Choices" and must include a particular icon promulgated within the Draft Regulations.[43] In addition, the alternative out-opt link must direct a consumer to a webpage that includes a description of the consumer's rights to opt-out of sale/sharing and right to limit, and an interactive form or mechanism by which the consumer can submit their request.[44]

b. *New Opt-Out Preference Signal Rules*

The CA Privacy Acts require that the California Attorney General promulgate regulations to facilitate the submission of a request to opt-out of the sale of personal information, and

[39] Draft Regulations § 7027(e).
[40] Draft Regulations § 7027(l)(1)-(7).
[41] Cal. Civ Code § 1798.135(a)(3).
[42] Draft Regulations § 7015.
[43] Draft Regulations § 7015(b).
[44] Draft Regulations § 7015(c).

furthermore require a business to treat user-enabled global privacy controls (e.g., a browser plug-in, privacy setting, device setting, or other mechanism) as a valid opt-out request to promote innovation and ease of use for consumers making requests.[45] Accordingly, in the Draft Regulations, the Agency introduces the concept of "opt-out preference signals," which provide consumers with an easy-to-use method by which consumers interacting with a business online can automatically exercise their right to opt-out of the sale or sharing of personal information. An opt-out preference signal allows a consumer to opt out of the sale and sharing of their personal information with all businesses they interact with online without having to submit individualized requests to each business.[46]

Businesses must process any opt-out preference signals that are in a commonly recognized format (e.g., a HTTP header field).[47] When a business receives or detects an opt-out preference signal, the business must treat that signal as a valid request to opt-out and not require the consumer to provide any additional information.[48] However, if an opt-out preference signal conflicts with a consumer's business-specific privacy settings, the business may notify the consumer of the conflict and provide the consumer with an opportunity to opt-in.[49]

When processing opt-out preference signals, businesses must display whether or not they processed the consumer's signal, for example through a pop-up stating "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the business' website.[50] *Notably, if a business processes opt-out preference signals in a "frictionless" manner, the business is not required to post the otherwise required "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links*.[51] To process opt-out preference signals in a "frictionless" manner, a business:

- Shall not charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.
- Shall not change the consumer's experience with the product or service offered by the business.
- Shall not display a notification, pop-up text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal (except for the notification that the business has processed such signal).[52]
- Must include in its privacy policy a description of the consumer's right to opt-out, a statement that the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner, and instructions for any other method by which the consumer may submit a request to opt-out.[53]

[45] Cal. Civ. Code § 1798.185.
[46] Draft Regulations § 7025(a).
[47] Draft Regulations § 7025(b)(1).
[48] Draft Regulations § 7025(c)(1), (2).
[49] Draft Regulations § 7025(c)(3).
[50] Draft Regulations § 7025(c)(6).
[51] Draft Regulations § 7025(e).
[52] Draft Regulations § 7025(f)(1)-(3).
[53] Draft Regulations § 7025(g)(2).

- Must allow the opt-out preference signal to fully effectuate the consumer's request to opt-out.[54]

VI. Business Engagements

a. *Contractors, Service Providers, and Third Parties*

The CA Privacy Acts impose different obligations upon the different outside parties with which a business shares, discloses or processes personal information, consisting of contractors, service providers, and other third parties. The differences between each type of entity are subtle and outlined in the table below:

	Contractor[55]	**Service Provider**[56]	**Third Party**[57]
Receipt of Personal Information	From the business	From or on behalf of the business (i.e., from the consumer directly)	As part of the sharing or sale of personal information
Purpose of Receipt of Personal Information	A "business purpose" (e.g, providing marketing or advertising)[58]	To process such personal information, as directed by the business	For the third party's own purposes via the sharing or sale of personal information
Right to Opt-Out Applicable	No	No	Yes

b. *Contract Requirements*

The CA Privacy Acts mandate certain contractual provisions for contractors and service providers. Whereas the 2018 Act (as amended by the 2020 Act) listed such requirements in different parts of the law's text, the Agency opted to consolidate the contractual requirements for both contractors and service providers. In particular, a contract complaint with the CA Privacy Acts between a business and contractor or service provider must:[59]

- Prohibit the service provider or contractor from selling or sharing personal information it receives from or on behalf of the business.
- Identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information on behalf of the business and specify that the business is disclosing personal information only for the limited and specific business purpose(s) set forth within the contract.
- Prohibit the service provider or contractor from retaining, using, or disclosing the personal information for any purposes other than those specified in the contract, for any commercial purpose other than the business purpose specified in the contract, outside the direct business relationship between the service provider/contractor and the business, or otherwise permitted by the CA Privacy Acts.

[54] Draft Regulations § 7025(g)(3).
[55] Cal. Civ. Code § 1798.140(j).
[56] Cal. Civ. Code § 1798.140(ag).
[57] Cal. Civ. Code § 1798.140(ai).
[58] Cal. Civ. Code § 1798.140(e), (j)(1).
[59] Draft Regulations § 7051(a).

- Require the service provider or contractor to comply with applicable sections of the CA Privacy Acts, including providing the same level of privacy protection as required of businesses by, for example, cooperating with the business in responding to and complying with consumers' requests, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business.
- Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information in a manner consistent with the business' obligations under the CA Privacy Acts, such as by conducting ongoing manual reviews and automated scans of the service provider or contractor's systems, regular assessments, audits, or other technical and operational testing at least once every 12 months.
- Require the service provider or contractor to notify the business no later than five business days after it decides that it can no longer meet its obligations under the CA Privacy Acts.
- Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's or contractor's unauthorized use of personal information, for example by requiring the service provider or contractor to provide documentation that verifies it no longer retains or uses the personal information of consumers that have made a valid request to delete with the business.
- Require the business to inform the service provider or contractor of any consumer request made pursuant to the CA Privacy Acts they must comply with, and provide information necessary to the service provider or contractor for compliance with the request.

The Draft Regulations also impose slightly different contractual requirements on third parties. In particular, a business that sells or shares a consumer's personal information with a third party must enter into an agreement with that third party that:[60]

- Identifies the limited and specified purpose(s) for which the personal information is sold or disclosed.
- Specifies that the business is disclosing the personal information to the third party only for the limited and specified purposes set forth within the contract and requires the third party to only use the personal information for those limited and specified purposes.
- Requires the third party to comply with the CA Privacy Acts.
- Grants the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information in a manner consistent with the business' obligations under the CA Privacy Acts.
- Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

[60] Draft Regulations § 7053(a).

- Requires the third party to notify the business no later than five business days after it decides it can no longer meet its obligations under the CA Privacy Acts.

c. ***Third Party Obligations***

The 2020 Act amendments to the 2018 Act add requirements on third parties who are forwarded consumer requests from a business who sold or shared personal information with them. As such, the Draft Regulations outline such obligations, which include:

- A requirement that the third party comply with a consumer's request to delete, correct, opt-out of the sale/sharing of personal information, or limit the use and disclosure of sensitive personal information forwarded to them by a business that provided, made available, or authorized the collection of the consumer's personal information.[61]
- A requirement that a third party that collects personal information online (e.g., through a first party's website) and receives an opt-out preference signal recognize such signal as a valid request to opt-out of the sale/sharing of personal information.[62]

VII. Audit and Enforcement

a. ***Investigations***

Whereas the CA Privacy Acts as drafted did not outline the procedure surrounding investigations and enforcement of the CA Privacy Acts, the Draft Regulations lay out the process for filing sworn complaints with the Agency as well as enforcement proceedings. Complaints may be filed on the Agency's website against a business in violation of the CA Privacy Acts.[63] Subsequently, the Agency will notify the business in writing of the actions it plans to take against the business.[64] Similarly, the Draft Regulations vest the Agency with the power to initiate investigations on its own initiative, instead of requiring a sworn complaint from a consumer.[65]

b. ***Agency Audits***

To ensure compliance with the CA Privacy Acts, the Draft Regulations provide the Agency with the ability to audit a business.[66] A business may be subject to an audit if the Agency suspects possible violations of the CA Privacy Acts, if the business' collection or processing of personal information presents a significant risk to consumer privacy or security, or if the business has a history of noncompliance with privacy law.[67] Audits may be announced or unannounced, and failure to cooperate with an audit may result in issuance of a subpoena or warrant against the business.[68]

[61] Draft Regulations § 7052(a), (b)
[62] Draft Regulations § 7052(c).
[63] Draft Regulations § 7300(a).
[64] Draft Regulations § 7300(b).
[65] Draft Regulations § 7301.
[66] Draft Regulations § 7304(a).
[67] Draft Regulations § 7304(b).
[68] Draft Regulations § 7304(c).