

Consumer Requests Under the California Consumer Privacy Act

Nancy L. Perkins
Arnold & Porter

Christi Perri
Jim Simatacolos
Toyota Motor North America

Jill Whitby
First Republic Bank

May 8, 2020

- **Verifying a Consumer's Identity**
- **Requests to Know**
- **Requests to Delete**
- **Timing and Service Providers**
- **Household Requests**

Verifying A Consumer's Identity

- *“Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business”*
 - *“If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer.”*
1. **When is it helpful or necessary to seek additional information?**
 2. **What additional information is most helpful to obtain?**
 3. **Does this provision encourage excessive collection of personal information?**

- *“The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer’s request, except as required to comply with [the CCPA’s record-keeping requirements].”*
 - 1. What personal information should be retained to show that sufficient verification was made?**
 - 2. What personal information should be retained to defend a claim that insufficient verification was the cause of unauthorized disclosure?**

Need for “Sensitive Information” to Verify

- *“Avoid collecting . . . [sensitive] personal information, unless necessary for the purpose of verifying the consumer.”*
 - *“Consider the type . . . of personal information . . . maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process.”*
 - **“Sensitive” personal information includes full name, Social Security number, driver’s license number, biometric information.**
- 1. When is obtaining sensitive personal information necessary for verification?**
 - 2. If you already maintain sensitive personal information, should you seek more in order to do a “more stringent verification”?**

- *“A business shall not require a consumer . . . to pay a fee for the verification of their request.”*
- *To avoid collecting new personal information, “use a third-party identity verification service that complies with [the CCPA].”*

1. How much should be invested in third-party verification services?

2. Do the costs of paying for such services outweigh the benefits?

- *To avoid collecting new personal information, “a business may . . . require the consumer to provide a notarized affidavit to verify their identity”*
- **But not** *“unless the business compensates the consumer for the cost of notarization.”*
 1. **Do the costs of engaging notaries to notarize consumers’ affidavits of identity outweigh the benefits?**
 2. **How practical is it to get a notary in the current COVID-19 emergency environment?**
 - **California does not permit in-state notaries to do remote online notarizations**

Requests to Know

- *“A business shall deny a request to know specific pieces of personal information if . . . there is no reasonable method by which [the] business can verify the consumer to the degree of certainty required by [the CCPA regulations].”*
- **Which alternative below is more likely/risky?**
 - 1. Business denies request based on insufficient verification; consumer files complaint; CA Attorney General finds business liable for failure to respond**
 - 2. Business grants request for specific pieces of information; request was fraudulent; true consumer sues for breach of security**

- To grant a request to know *categories* of personal information, a business must verify the identity of the requestor “to a *reasonable degree of certainty*.”
- To grant a request to know *specific pieces of personal information*, a business must verify the identity of the requestor “to a *reasonably high degree of certainty*.”
 1. What is a “reasonable degree of certainty”? What doubts are acceptable?
 2. What is a “reasonably high degree of certainty”? Can there be any doubt?

- *If a business cannot verify the identity of the person making a request for specific pieces of personal information to a “reasonably high degree of certainty,” the business may not disclose any specific pieces of personal information to the requestor and must “evaluate the consumer’s request as if it is seeking the disclosure of categories of personal information.”*
 1. **What type of verification would justify disclosing categories when there is insufficient verification to disclose specific pieces of personal information?**
 2. **Does the requirement to disclose categories without a reasonably high degree of certainty as to the identity of the recipient present phishing/spear phishing risk for consumers and businesses?**

- *In responding to a request to know the categories of personal information collected, “a business shall identify the categories of personal information, categories of sources . . . , and categories of third parties to whom the business sold or disclosed [the] information, in a manner that provides consumers a meaningful understanding of the categories listed.”*
 1. **What information is needed to provide “a meaningful understanding” of listed categories?**
 2. **Must there be examples within generically-referenced categories?**
 3. **Must the purposes for the disclosures be provided?**

- *In responding to a request to know, a business is not required to search for personal information that:*
 - *is not in a searchable or reasonably accessible format,*
 - *is kept solely for legal or compliance purposes, AND*
 - *is not sold or used for commercial purposes.”*
1. **When is personal information not “reasonably accessible”?**
 2. **If personal information is maintained pursuant to a business’s self-created document retention policies, is the information kept for “compliance purposes”?**

Requests to Delete

- *“A business shall comply with a consumer’s request to delete their personal information by:*
 - *Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;*
 - *Deidentifying the personal information; or*
 - *Aggregating the consumer information.”*
-
- 1. Do all of these alternatives serve a consumer’s purpose in requesting deletion?**
 - 2. Should a business tell the consumer which option was chosen?**

The Deidentification Option

- **“Deidentification”** requires de-linking and disassociating information from any particular consumer, *and*:
 - implementing procedures and technical safeguards that prohibit reidentification;
 - making no attempt to reidentify the information; and
 - preventing inadvertent release of deidentified information
1. **Why should the CCPA be concerned with the release of deidentified information?**
 2. **Do consumers have privacy rights in deidentified information?**

“[W]ith respect to data stored on the archived or backup system,” a business “may delay compliance with the consumer’s request to delete, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.”

- 1. What internal connectivity are businesses implementing to comply with the requirement to delete from archives or back-up systems?**
- 2. Is it OK if some archived personal data is never deleted?**

Records of Requests for Deletion

- *Business must maintain records of requests to delete, including those that were granted.*
- *“A business may retain a record of [a request to delete that was granted] for the purpose of ensuring that the consumer’s personal information remains deleted from the business’s records.”*
 - 1. Can personal information be included in a record of a request to delete where the request was granted?**
 - 2. If so, what personal information and why?**
 - 3. If not, how can the business “ensure that the consumer’s personal information remains deleted”?**

- *When a business denies a request to delete personal information based on an exception to the CCPA, the business must, inter alia:*
 - *“Delete the consumer’s personal information that is not subject to the exception; and*
 - *“Not use the consumer’s personal information retained for any other purposes than provided for by that exception.”*
- 1. If the denial is because the personal information is exempt from the CCPA (e.g., the information is “nonpublic personal financial information” under the GLBA or “protected health information” under HIPAA), what is the “purpose” for which the retained information may be used?**
- 2. How will the CA Attorney General determine which pieces of personal information are subject to exemptions defined by reference to federal laws?**

- *If a business that denies a request to delete sells personal information and the requesting consumer did not opt out of such sale:*
 - *“the business shall ask the consumer if they would like to opt out of the sale of their personal information” and provide the business’s “Do-Not-Sell” option to the consumer again.*
1. What is the statutory basis for this requirement?
 2. Is there a solid policy basis for this requirement?

Timing and Service Providers

- *Businesses have 45 calendar days to respond to requests to know or to delete, “regardless of the time required to verify the request.”*
- *If necessary and if it provides notice to the consumer, a business may take up to an additional 45 calendar days to respond.*

1. **Are these time limits realistic?**
2. **Should they be more nuanced, e.g., more time for vastly broad requests?**
3. **If verification is incomplete at 90-day deadline, is it more risky to grant or to deny a request to know or delete?**

- *A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.”*

1. **How feasible is it to comply with an opt-out request in 15 days?**
2. **What complications arise in implementing compliance with opt-out requests?**

- *If a consumer requests **specific pieces** of personal information from a business and **the information is held by a service provider**:*
 1. **How can the business best ensure that it will be able to provide the consumer with the requested information within 45 days?**
 2. **Should the business require the service provider to respond directly to the consumer's request?**

- *If a consumer requests **deletion** of personal information by a business and **the information is held by a service provider**:*
 1. **How much discretion should the business give the service provider in determining whether to grant or deny the consumer's request?**
 2. **Should the business require the service provider to provide an attestation of deletion and if so, how detailed should that be?**

- *“If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either:*
 - *act on behalf of the business in responding to the request or*
 - *inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.”*
- 1. **When will it be appropriate for a service provider to act on behalf of the business?**
- 2. **If the service provider chooses to act on behalf of the business, is the business liable for the service provider’s decisions on verification and granting or denying specific requests?**

Household Requests

“Household” Definition

- A person or group of people who:
 - reside at the same address,
 - share a common device or the same service provided by a business, *and*
 - are identified by the business as sharing the same group account or unique identifier occupying a single dwelling.
1. **Do businesses typically know how many persons are in a household?**
 2. **Do businesses usually know the ages or names of household members?**

Requests to Know Household Information

- A business **must deny** a request to know specific pieces of personal information, or to delete personal information, about a household unless:
 - The household has a password protected account, or
 - The business:
 - receives the request from all consumers of the household jointly
 - individually verifies the identity of each member of the household, and
 - verifies that each requestor is currently a member of the household.
1. **Should businesses require that parents verify the identity of children under 13?**
 2. **What evidence should businesses require to verify who is currently a member of a household?**

Providing Household Information Based on a Single Consumer's Request

- *Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information as it would other consumer requests.*
 - 1. What are the perils for a business that grants a single household member's request for specific pieces of the household's information?**
 - 2. What recourse would a household member have against alleged over-disclosure of personal information to another household member?**

Speaker Contact Information



Nancy L. Perkins

Arnold & Porter
(202) 942-5065
nancy.perkins@arnoldporter.com

Christi N. Perri

Toyota Motor North America
(859) 409-8012
christi.perri@toyota.com

Jill Whitby

First Republic Bank
(415) 364-4916
jwhitby@firstrepublic.com

Jim Simatacolos

Toyota Legal One c/o Toyota Motor
North America, Inc.
(469) 292-7329
jim.simatacolos@toyota.com