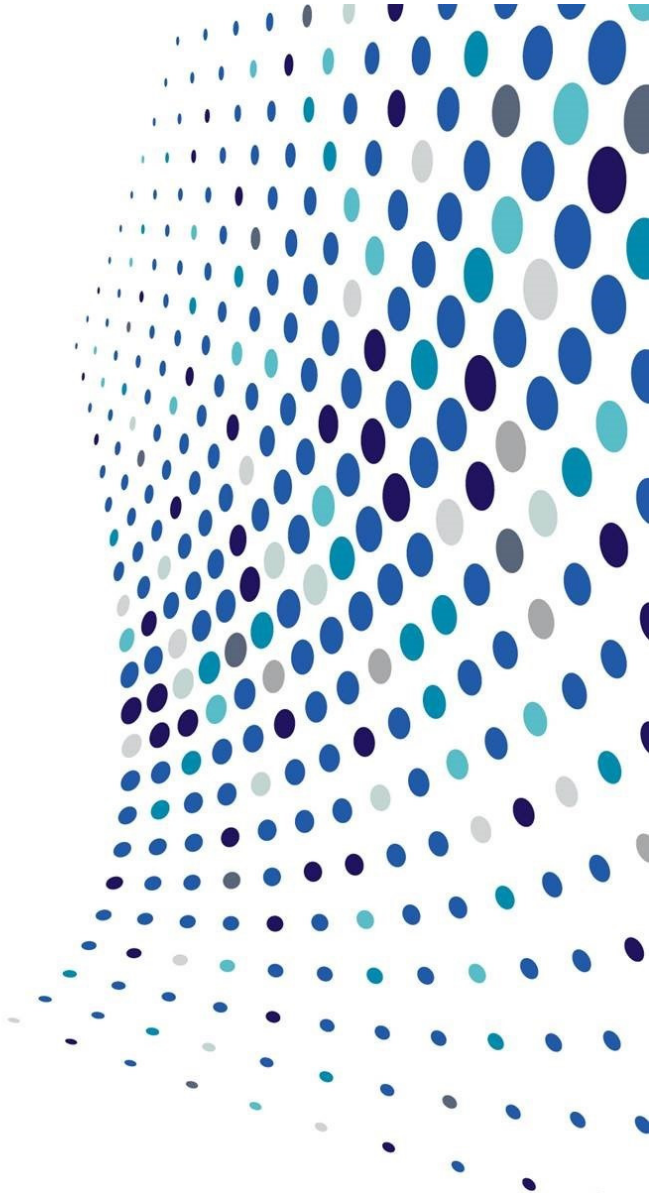
O'Melveny

# Privacy Deep Dive Session 2: Implementing Data Subject Rights

Scott Pink and John Dermody

March 10, 2022



## Overview

- Right to Correct
- Right to Access & Data Portability
- Right to Delete
- Right to Restrict
- Opt-out Rights
- Methods for Submission of Requests
- Verification and Responses
- Practical Considerations

# Right To Correct

# Right to Correct

**Right to Correct included in Virginia and Colorado; added to California by CPRA:**

- A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.
- "Commercially reasonable" efforts to correct the inaccurate personal information.
- The CPPA has sought comments on procedures for correction requests, as well as whether businesses should be exempt if compliance would be "impossible, or involve a disproportionate effort."

# Right of Access & Data Portability

# Right of Access

**Right of Access included in Virginia, Colorado, and California (amended by CPRA):**

- **1798.110:** Consumers have the right to confirm whether a controller is processing their personal data and to access that data.
- Business must provide the categories of:
  - personal information it has collected about the consumer
  - sources of that information
  - business and commercial purpose for collecting, selling and sharing
  - third parties to whom the information is disclosed
- As well as “specific pieces of personal information it has collected about that consumer.”

## Right of Access

**1798.115:** The right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

- The categories of personal information that the business collected about the consumer.
- The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.
- The categories of personal information that the business disclosed about the consumer for a business purpose.

## Data Portability

**CO**: “A consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. A consumer may exercise this right no more than two times per calendar year.” *Does not appear to be limited to data company collected from requester.*

**VA**: “To obtain a copy of his personal data that he previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.” *Twice per year.*

**CA**: “A business that receives a verifiable consumer request pursuant to sections 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer.” *Twice per year. Does not appear to be limited to data company collected from requester.*

# California – Portability Requirements

**Current CCPA Regulations (which may change):**

- Business should not provide sensitive data: 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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics.
- For sensitive data, the business should inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects “unique biometric data including a fingerprint scan” without disclosing the actual fingerprint scan data.

# Verification and Responding to CA Right to Know Request

- Generally, validate through an existing password-protected user account. If no account, then there are specific requirements to validate the request:
  - Right to know categories of information: Reasonable degree of certainty (match at least two data points)
  - Right to know specific pieces of information: Reasonably **high** degree of certainty (match at least three data points, plus acquire a signed declaration under penalty of perjury)

- If cannot validate at level required for specific personal information, consider request to be for categories of information.

- Unless otherwise specified by requestor, must provide personal information for the 12 months preceding the receipt of request. A consumer may request that the business disclose the required information beyond the 12-month period (but for information collected after Jan. 1, 2022), and the business shall be required to provide that information unless doing so proves **impossible** or would involve a **disproportionate effort**.

# Right to Delete

## Right to Delete

- CO, VA, and CA
- CPRA extended Right to Delete: businesses must now notify any service providers or contractors to delete the consumer's personal information from their records and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.
  - Deletion request flows down to subcontractors and entities providing services to service providers
  - Deletion right somewhat limited in CA: A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.
- Virginia/Colorado – contracts with sub processors must contain flow-down deletion requirement

# Right to Delete – CA Specific Requirements

**Shall comply 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;
- Aggregating the consumer information
- If storing information in archives or backups, may delay compliance until that data is restored to an active system of used for sale, disclosure, or commercial purpose.
- If complying, must communicate to requestor that it will maintain a record of the request as required by CCPA.

**If denying request:**

- Explain why and delete personal information that is not subject to exception.
- If business sells personal information, ask consumer if they would like to opt out of the sale of personal information (referencing right to opt out).

## Right to Delete – Exceptions

**CA**:

If personal information is “reasonably necessary” to:

- Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business’ ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business and compatible with the context in which the consumer provided the information.
- Comply with a legal obligation.
- Help to ensure security and integrity to the extent the use of the consumer’s personal information is reasonably necessary and proportionate for those purposes.

## Right to Delete – Exceptions

**CO**: No definition of “deletion.” The deletion obligations do not restrict ability to:

- Comply with federal, state, or local laws, rules, or regulations;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
- Investigate, exercise, prepare for, or defend actual or anticipated legal claims;
- Conduct internal research to improve, repair, or develop products, services, or technology;
- Perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller;
- Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action

## Right to Delete – Exceptions

**VA § 59.1-578:** No definition of "deletion." The deletion obligations do not restrict ability to:

- Comply with federal, state, or local laws, rules, or regulations;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;
- Conduct internal research to improve or repair products, services, or technology;
- Perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party

## Right to Delete – Practicalities

- Scope of search for data
  - What are back up systems?
  - Local drives
  - Key is to put data beyond use
- Consider California option for double opt-in to deletion
- Does not generally apply to de-identified and aggregate data or publicly available information
- New Apple Requirements (6/30/22) – account creation must also allow users to initiate deletion of their account from within the app (might require capability to delete personal information as well).

# Opt-out Rights

| California | Virginia | Colorado |
|---|---|---|
| Sale = providing PI to third party for monetary or other valuable consideration | Sale = exchange of personal data for monetary consideration to a third party. | Sale = exchange of personal data for monetary or other valuable consideration to a third party |
| Sharing = providing PI to third party for cross-context behavioral advertising | Targeted advertising = displaying advertisements based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. | Targeted Advertising = similar to Virginia |
| Profiling = evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements – subject to regulations | Profiling = similar to California | Profiling = similar to California |

# Opt-Out Procedures

## California:

- Clear and conspicuous link on home page/mobile app titled “Do Not Sell My Personal Information”
  - need one more method (email address, toll free number, form, user enable privacy controls)
- Must be easy to execute
- CCPA regulations: treat user-enabled privacy controls as opt-out
- CPRA does not address opt-out signals – business has the option to respond to them
- CPPA will issue regulations governing opt-out signals
- CPRA allows businesses to obtain consent through a consent page
  - might require notice of financial incentive

## Colorado:

- no separate requirements

## Virginia:

- July 1, 2023: may allow opt-out through user selected universal opt-out mechanism
- July1, 2024: must allow opt-out through such mechanism
- Attorney General to issue regulations

# Sensitive Information – Restrictions

## California – Right to Restrict

- Applies to sensitive personal information only.
- Consumer shall have the right, at any time, to limit use of the consumer's sensitive personal information, to the following:
  - ensure security and integrity of use of personal information
  - short term transient use (cannot be used for targeted advertising or building a profile)
  - performing services on behalf of a business
  - verify or maintain the quality or safety, or improve, upgrade or enhance a service or device that is owned, manufactured, manufactured for, or controlled by the business
- Does not apply to sensitive personal information that is collected or processed without purpose of inferring characteristics of consumer.
- Same mechanism as opt-out of sale – separate or combined link (Limit Use of My Sensitive Personal Information) – can also choose to respond to opt-out preference signals.

# Methods of Submitting Requests

## Methods of Submission

- **Virginia –** one or more secure and reliable means
- **Colorado –** means must be described in privacy policy
- **CA: Requirements vary based on nature of data collection:**
  - Exclusively online – email is sufficient
  - Otherwise, two methods, which must include a toll-free telephone number. Other methods include:
    - a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail
  - In store – printed form, email, tablet or computer portal in-store, or toll-free number
  - Authorized Agents – a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request, including requiring the consumer to verify their own identity directly with the business and directly confirm with the business that they provided the authorized agent permission to submit the request.
    - valid Power of Attorney under CA law sufficient

## Methods of Submission

**CA: Household Requests – requests to know/delete**

- Password-protected account or –
- 3 requirements met: (1) all consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information; (2) business individually verifies all the members of the household; and (3) the business verifies that each member making the request is currently a member of the household

# Verification and Responses

## Verification Requirements

**CO and VA:** Use “commercially reasonable” to validate request; may request the provision of additional information reasonably necessary to authenticate the request.

**CA:** Establish and document a “reasonable method” for verification:

- “When feasible” match identifying information to personal information already maintained.
- Avoid collection of unnecessary personal information.
- “Generally avoid” requesting additional information if you can verify identity based upon internal records.
- Delete any new personal information collected for verification as soon as practical (except for record retention requirements).
- Implement verification procedures that align with the sensitivity of data and risk of harm.

# Verification Requirements

**CA:**

**Verification for Account Holders**

- If maintain password-protected account, verify through existing authentication practices.
- If disclosing or deleting data, re-authentication is required.

**Verification for Non-Account Holders**

- Right to Know Categories of Information: Reasonable degree of certainty (match at least two data points).
- Right to Know Specific Pieces of Information: Reasonably high degree of certainty (match at least three data points, plus acquire a signed declaration under penalty of perjury).
- Request to Delete: Reasonable to reasonably high degree of certainty depending upon the sensitivity of the data.

## Response Requirements – Timing

**CA:**

- Confirm receipt within 10 days and provide information about how the request will be processed, including verification process and potential timing
- Respond substantively within 45 calendar days
  - 45 clock runs regardless of verification
  - May deny request without verification
  - Can take additional 45 days to respond with notice and explanation to requestor
- Respond within 15 business days to opt-out request

**VA and CO:**

- Respond substantively within 45 days, may be extended additional 45 days with notice

*NOTE: GDPR requirement is a response within 30 days, and can be extended for up to two months with notice

## Response Requirements – Substance

Must explain reason for denying request:

- **CA** notes that the response must explain if it is because any conflicts with federal or state law, or exception to CCPA/CPRA (unless prohibited from doing so).
- In **CO and VA**, must also provide instructions on how to appeal.

Generally cannot require user to create an account to make requests

## Response Requirements – Record Keeping

**1798.105**: The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this title.

**Current CCPA Regs**: CA § 999.317: Maintain record of response for at least **24 months.**

- Record must contain: date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.
- Record-keeping information shall not be used for any other purpose except as reasonably necessary to improve compliance.
- Businesses processing personal information of 10 million or more consumers in a calendar year must compile metrics on the data subject rights requests, including the median or mean day to respond to requests.
  - Publicly disclose this information by July 1 every year.

## Appeals Process

- CO and VA (but **not** CA) require an internal appeal process for denials.
- Appeal process initiated by request from consumer "within a reasonable period" after receipt of denial notice.

| **CO:** | **VA:** |
| --- | --- |
| • 45 days after receipt of appeal to address;<br>• Must provide written reasons.<br>• May extend an additional 45 days with notice to requestor<br>• Must inform consumer of ability to contact the AG | • 60 days after receipt of appeal to address;<br>• Must provide written reasons.<br>• May extend an additional 45 days with notice to requestor<br>• Must inform consumer of ability to contact the AG |

## Practical Considerations

- Create an internal procedure with specified roles and responsibilities
- Develop uniform approach across all three states if possible?
- Consider implementing an email address with auto-response acknowledge and informing of timelines
- Create tracker (e.g., .xml) with timelines (third-party software tracking options)
- Develop verification procedures
- Create template responses for seeking verification
- Create timeline for verification requests in advance to 45 days
- Create secure recordkeeping system
- Anticipate automated third-party services
  - Likely insufficient information to verify that eligible under the laws
  - Larger volume than “legitimate” requests

## Scott W. Pink

**Special Counsel**
Data Security & Privacy

**Resident Office**
Silicon Valley

**Telephone**
+1 650 473 2629

**Email**
spink@omm.com

## John Dermody

**Counsel**
Data Security & Privacy

**Resident Office**
Washington, DC

**Telephone**
+1 202 383 5306

**Email**
jdermody@omm.com




O'Melveny

# Questions?

# Scott Pink

**Special Counsel**
Data Security & Privacy

**Resident Office**
Silicon Valley

**Telephone**
+1 650 473 2629

**Email**
spink@omm.com

A former general counsel for a major media company, Scott Pink brings an insider's perspective to his broad-based practice. It's what's made him the lead outside advertising and marketing counsel to several well-known brands, and a sought-after resource on intellectual property, privacy and cybersecurity issues.

He advises technology, media, entertainment and a variety of consumer product and franchise companies on issues of intellectual property counseling; social media law; cybersecurity and privacy; and advertising, marketing, and promotions law.

Scott had led many privacy and security compliance initiatives worldwide for clients, including GDPR compliance, HIPAA compliance audits, compliance with financial security regulations (NYDFS) and security audits for cryptocurrency and blockchain companies. He is a thought leader on GDPR issues, having published articles in Cybersecurity Law Report and speaking at conferences hosted by the International Association of Privacy Professional.

Scott also has extensive experience in technology related transactions and other legal issues in the life science field. He has represented cutting edge life science, biotech and nutritional supplement companies on privacy and security policies and issues, product development agreements, tech transfer agreements with Universities, agreements with health care providers, collaboration agreements, patent licenses, marketing agreements, materials transfer agreements, manufacturing agreements, marketing agreements and marketing compliance.

# John Dermody

**Counsel**
White Collar Defense & Corporate Investigations

**Resident Office**
Washington, DC

**Telephone**
+1 202 383 5306

**Email**
jdermody@omm.com

John Dermody joined O'Melveny after a decade in government service, recently serving as a deputy legal advisor at the National Security Council (NSC). Previously, John served in the General Counsel's offices of the Department of Homeland Security (DHS) and the Department of Defense. Drawing on his experience in the highest levels of government, John advises clients on data security, privacy, cybersecurity, and national security issues, including economic sanctions and national security reviews of investments and technology transactions conducted by the Departments of Justice, Homeland Security, Defense, the Treasury, State, and Commerce. As a member of O'Melveny's Coronavirus Task Force, John advises clients on government emergency powers, shelter-in-place orders, and data privacy issues associated with public health measures.

While at the NSC, John advised senior officials on cybersecurity, infrastructure protection, disaster response, border and transportation security, election security, biodefense, and other matters of US national security. His work included coordinating responses to and attribution of cyber incidents, revising US cyber operations policy, and helping to develop and implement the National Cyber Strategy. He also advised on US sanctions programs and matters and policies relating to supply chain security, 5G deployment, and spectrum allocation.

John's responsibilities as a senior staff attorney in the Intelligence Law Division of DHS included advising on compliance with domestic and international privacy regimes and advising government officials on data security matters related to data analytics, data sharing, and cloud computing technology, giving him unique insight on security and privacy implications of emerging technologies. John is a Certified Information Privacy Professional for the United States (CIPP/US) and Europe (CIPP/E).



O'Melveny

## CLE to Go

O’Melveny is pleased to offer free online access to professionally recorded CLE content to our clients, alumni, and friends of the firm. Please visit www.omm.com/resources/cle for more details on, and access to, CLE to Go.



O'Melveny