O'Melveny

# Privacy Deep Dive Session 1: Data Controller Obligations

Scott Pink and John Dermody

*February 22, 2022*

# Overview

- Do the New Laws Apply to you
- Determining Exemptions
- Data Minimization, Retention, and Purpose Limitations
- Data Impact Assessments
- Data Security

# Overview

## Existing Laws

- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)

## New Laws

- California Privacy Rights Act (CPRA) – January 1, 2023
- Virginia Consumer Data Protection Act (VCDPA) – January 1, 2023
- Colorado Privacy Act (CPA) – July 1, 2023

## Getting Ready

- Start Early
- Engage all Stakeholders
- Planning and Implementation – Create a Schedule and Stick to It
- Make an Ongoing Process – New Products/Developments

# Do the New Laws Apply to You?

# Determining Whether You Are Subject to the Laws - California

## Doing Business in California and meets one of three thresholds:

- As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year.
- Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of [50,000 – until 12/21/22][100,000 -starting 1/1/23] or more consumers or, households, or devices.
- Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

- **Control and common branding**

- **Joint Ventures**

# Determining Whether You Are Subject to the Laws – CO and VA

## Colorado

- Conducts business in Colorado or sells product or services intentionally targeted to residents of Colorado, and meet either of the following thresholds:
  - Controls or processes personal data of 100,000 or more consumers during a calendar year; or
  - Derived revenue or received discounts from the sale of personal data and control or process data of at least 25,000 consumers.

## Virginia

- Conducts business in Virginia or produce products or services targeted to Virginia residents and meets the following threshold:
  - Control or process the personal data of at least 100,000 Virginia consumers.
  - Lowered to 25,000 consumers if over 50% of the business's gross revenue derives from selling personal data.

- **No Revenue Thresholds**

## Determining Whether You Are Subject to the Laws – GDPR

- Entity is established in the European Union
- Offering goods or services to residents in the European Union
- Monitoring behavior of residents in the European Union
- Pursuant to an international treaty

# Determining Exemptions

# Determining Exemptions – Entity Level

| California | Colorado | Virginia |
|---|---|---|
| Non-Profits | N/A | Non-Profits |
| Covered entities/BAAs subject to HIPAA | Covered entities/BAAs subject to HIPAA | Covered entities/BAAs subject to HIPAA |
| N/A | Financial Institutions subject to GLBA | Financial Institutions subject to GLBA |
| Institutions of higher education (if non-profit) | Institutions of higher education (if non-profit) | Institutions of higher education (whether or not non-profit) |
| Government entities | Government Entities<br>Air Carriers<br>National Securities Association | Government Entities |

# Data Inventory and Mapping

# Data Inventory and Mapping

- Critical First Step, and a Continuing Obligation
- Create Internal Process that Tracks
  - New data creation or acquisition
  - Transition of data sets (cloud migration, alternative systems, archives)
  - Development or use of new data analytics

- Data inventory and mapping allows you to meet other obligations

# Data Inventory and Mapping

## Understanding what data is covered

- Consumer = resident of state
- Personal Information/Data - definition varies by state

| State | Definition | Categories |
|---|---|---|
| California | Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. | Yes (e.g., identifiers, protected classification, commercial information, biometric data, geolocation data, etc.) |
| Colorado | Information that is linked or reasonably linkable to an identified or identifiable individual<br><br>Identified or identifiable individual means an individual who can be readily identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier. | No |
| Virginia | Any information that is linked or reasonably linkable to an identified or identifiable natural person (a person *who can be readily identified, directly or indirectly)* | No |

# Data Inventory and Mapping

- Differentiating Sensitive Information
- Additional Rights/Consent Requirements

| State | Definition |
| --- | --- |
| California | Social security, driver's license, state identification card, or passport number; consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; genetic data; biometric information for the purpose of uniquely identifying a consumer; health data; sex life or sexual orientation. |
| Colorado | Racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; genetic or biometric data or personal data from a known child (under 13) |
| Virginia | Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data for the purpose of uniquely identifying a natural person; personal data collected from a known child (under 13); or precise geolocation data. |

# Data Inventory and Mapping – What is not Covered

- Publicly Available Information
- Employment Information
- Business to Business Information
- Aggregate and De-Identified Information
- PHI under HIPAA or medical records under state medical privacy laws
- Clinical research data
- Personal Information subject to Gramm Leach Bliley (and in California the Financial Information Privacy Act)
- Education records under FERPA (Colorado)
- Credit Reports under FCRA
- Driver Privacy Protection Ac
- COPPA
- Miscellaneous Additional Exemptions

# Data Inventory and Mapping – Elements of Data Inventory

- **Names or titles of data owners (e.g. "Human resources")**
- **Types of data (e.g. "Job applicant data")**
  - Sensitive?
- **Sources of the data**
- **Where to find the data within your system (e.g. "HR Intranet")**
- **Data subjects (e.g. "New job applicants")**
- **How the data was collected (e.g. "Online employment submissions")**
- **How the data is used (e.g. "Demographic research")**
- **Is data shared or disclosed**
- **How long the data will be stored**
- **Who has access to this data**
- **Data security measures applied**
- **Policies for deleting or preserving the data**
- **Do any exemptions apply?**

# Data Inventory and Mapping

- Where to start?
  - Provide Questionnaire to Data Owners
  - Meet with IT and Business owners

- Organize types of data by lines of business, functions, or other criteria
  - This can be very complicated depending upon the size of the business and use of data

# Data Inventory and Mapping – The Process

- Conduct internally v. outsource
- Information gathering: written questionnaire v. interviews
- Identify units that have data
- Identify representative of each unit
- Data at rest and dynamic information
- Identify third parties involved in data processing
- Is inventory designed to show compliance (e.g., data minimization, security and permissible purpose for processing)?

- **Identify methods of data collection, processing and storage**
  - Systems
  - Devices and applications
  - Products
  - Websites
  - Mobile Applications
  - On Site (Retail)
  - Automated tools

# Data Minimization, Retention, and Purpose Limitation

# Data Minimization

- **Laws impose data minimization requirements:**
  - A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.
  - Data Inventory/Mapping should implement data minimization principles
  - Adopt Privacy by Design Principles for all Products/Services/Operations that incorporates these principles
- **Data retention policies should align with data minimization and data purpose principles**
- **Privacy policy retention language needs to align with practices**

# Data Retention

- **Relatively New Consideration in Records Management**
  - Typically Records Management is about what data am I obligated to keep (litigation holds, OSHA records, etc.)
- **Data is an Asset and a Liability**
  - Delete when no longer necessary for the purposes for which the data are collected or processed.
- **Articulate retention period in notice**
  - For XX period of time
  - For as long as necessary for the purposes identified in privacy policy
  - Until the end of the Public Health Emergency

# Purpose Limitation

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- **Without an internal data governance process, it is very difficult to live up to this obligation**

- **May be easier to identify for certain categories of data (health or financial data)**

# Data Impact Assessments

# Data Protection Assessments

*Risk Assessment; Data Protection Impact Assessment*

- **California**: If processing presents **significant risk** (forthcoming CPRA rulemaking)
- **Colorado**: Heightened risk of harm (targeted advertising with profiling risk, selling personal data, processing sensitive data)
- **Virginia**: Targeted advertising, sale of personal data, profiling in certain circumstances, sensitive data, that otherwise present a **heightened risk** to consumers
- **GDPR**: Likely to result in **high risk to individuals** (systematic automated processing with legal effect, large scale processing of sensitive data, systematic monitoring of a publicly accessible area on a large scale)

# Data Protection Assessments

## CA*, CO, VA,

- Data protection assessments shall identify and weigh the **benefits** that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public **against the potential risks to the rights of the consumer associated with such processing**, as mitigated by safeguards that can be employed by the controller to reduce such risks.
- The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into the assessment

## GDPR

- describe the nature, scope, context and purposes of the processing;
- lawfulness of processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

# Data Protection Assessments

**DPAs may need to be provided to regulators.**

- **California**: "Submit to the California Privacy Protection Agency on a regular basis"; not required to divulge trade secrets; regulations forthcoming
- **Colorado**: Available to the AG on request; does not constitute a waiver or attorney-client privilege or work-product protection; exempted from state FOIA
- **Virginia**: Must disclose to AG in connection with an investigation; does not constitute a waiver or attorney-client privilege or work-product protection; exempted from state FOIA
- **GDPR**: If determine that processing is high risk, must consult with Data Protection Authority; must disclose DPIA and other documentation to Data Protection Authority upon request

# Data Security

# Data Security

Whether in the law itself, or by reference to other requirements, the state privacy laws generally impose an obligation to implement and maintain **reasonable security measures** to prevent unauthorized access to personal information.

**Virginia Adds Greater Detail**: requires controllers to establish and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.

## 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

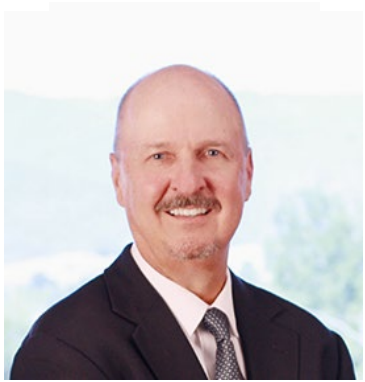
**Telephone**
+1 202 383 5306

**Email**
jdermody@omm.com

# CLE Code: 921246

# QUESTIONS?

# Scott Pink



**Special Counsel**
Data Security & Privacy

**Resident Office**
Silicon Valley

**Telephone**
+1 650 473 2629

**Email**
spink@omm.com

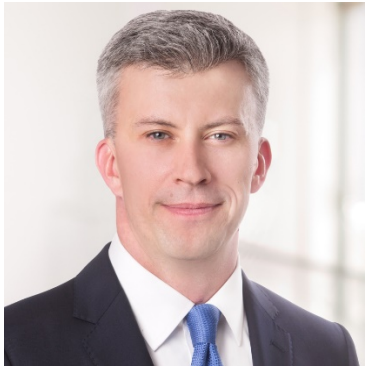
A former general counsel for a major media company, Scott Pink brings an insider's perspective to his broad-based practice. It's what's made him the lead outside advertising and marketing counsel to several well-known brands, and a sought-after resource on intellectual property, privacy and cybersecurity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