



# The California Consumer Privacy Act: Part 2

Business Obligations  
and Responsibilities (So Far As We  
Know Them—They Will Change)



# Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

# Speakers

---



Richard Lutkus

*Partner & Member Global  
Privacy and Security Team  
San Francisco Office*  
[rlutkus@seyfarth.com](mailto:rlutkus@seyfarth.com)



Jason Priebe

*Partner & Member Global  
Privacy and Security Team  
Chicago Office*  
[jpriebe@seyfarth.com](mailto:jpriebe@seyfarth.com)



John Tomaszewski

*Partner & Co-Chair Global  
Privacy and Security Team  
Houston Office*  
[jptomaszewski@seyfarth.com](mailto:jptomaszewski@seyfarth.com)



Edward "Ted" Murphree

*Counsel & Member Privacy  
and Security Team  
Houston Office*  
[emurphree@seyfarth.com](mailto:emurphree@seyfarth.com)



# **Business Obligations The Exercise of a Consumer's Rights**

# The Exercise of a Consumer's Rights

---

- The Rights a Consumer exercises under the Act determines a business's obligations
- Consumer Rights
  - Notice (both collection & onward transfer)
  - Access
  - Deletion
  - Opt-Out
- **In General**, Section 1798.130 of the Act determines Business Obligations for **every** exercise of Consumer Rights under the Act
- **Opt-Out**, Section 1798.135 of the Act determines Business Obligations for exercise of Opt-Out (or Opt-In) under the Act

# General Obligations

## General Rule

- Provide **notice** of business practice on-line (including consumer rights description and method to submit request) **and** list of categories collected, sold, or disclosed
- Provide **two** methods for consumers to submit requests (toll free # required)
- Receive **verifiable** request and confirm prior to responding.
- Business has 45 days to respond (extended to 90 total days upon reasonable notice to consumer during 1<sup>st</sup> 45 days)

# Duty to Disclose Information Collected

In addition to General Obligations above, Business must:

- ID Consumer by associating information in the verifiable consumer request with PI previously collected and ID the PI by categories collected in the **prior 12 months**
- Provide **prior** notice to Consumer of PI of categories to be collected and intended purpose. Use outside this purpose is **prohibited**
- Provide a list of categories of PI online that business has collected about consumers for the previous 12 months

## Duty to Disclose Sale or Disclosure for Business Purpose

In addition to General Obligations above, Business **must**

- ID consumer by associating with any information previously collected.
- ID the PI by categories sold or disclosed in prior 12 months
- Disclosure shall be made be separate lists.
- Notice shall be provided in online page (usually the privacy policy) – notice shall be made to each by separate list.
- If no sale or disclosure, state this in privacy policy
- The 3rd party sale or disclosure prohibition provision.



# Duty to Delete

In addition to the General Obligations above, Business must:

- delete PI pursuant to the request AND direct Service Providers to delete as well
- Exceptions to Business Obligation based on business necessity:
  - Completion of transaction involving PI
  - Security Breach
  - Debug to ID and repair error
  - Free speech
  - Compliance with CECP
  - Scientific, historical or statistical research in public interest subject to conditions
  - Solely internal uses reasonably aligned with consumers expectations.
  - Legal obligation
  - Catch all—otherwise use PI internally in lawfully compatible with context in which consumer provided it.
- deletion obligation **only** applies to PI collected from Consumers

# Duties Associated with Opt-Out

- Business must provide notice that Consumer has the right to Opt-Out of “sale” of Personal Information
- Once right is exercised, Business shall respect decision for minimum 12 months  
(You can't chase them down for an opt-in for 12 months)
- Notice must be provided Consumers regarding use of financial incentives
- Business is prohibited from entering Consumer into financial incentives program **absent** Opt-In

# Duty to NOT Discriminate

- If a Consumer exercises rights under this Act, Business shall not discriminate against them
- **Exception**—A business may charge different prices or rates for goods or services or provide different level or quality of goods or services **if reasonably related to the value** provided the consumer by the consumer's data

## Business Obligation under both Sections: To Train Staff

- Business must ensure individuals handling consumer inquiries **or** compliance with the Act know: consumer rights provisions, business obligation provisions, **and** how to direct consumers in exercising their rights



# Data Security

# Business Duty to Secure PI

- Business has an **affirmative duty** to implement and maintain reasonable security procedures and practices appropriate to the nature of the information with the charge to protect the information.
- Breach creates a private cause of action (not new law)
- CoA must be based on unauthorized access **and** exfiltration, theft or disclosure.
- Action may include suit:
  - To recover damages (the greater of \$100-\$750 per consumer per incident **or** actual damages)
  - Injunctive or declaratory relief
  - Any other relief Court deems proper

# De-Identified PI as Security

Business must implement:

- technical safeguards to prohibit re-identification;
- business processes to prohibit re-identification
- business processes to prevent inadvertent release of de-identified information; **and**
- There must not be any attempt to re-identify the information.

# Third Party & Vendor Considerations

The key is to ask the following questions:



## Is a Service Provider Used?

- If Yes, Business must 1) provide notice in its Terms and Conditions **and** 2) Service Provider must not further collect, sell or use PI except as necessary for business purpose
- Business must use a contract with specific terms
- Failure to comply with specific contractual terms will result in classification as 3rd party sale

# Is Business Selling PI to a 3<sup>rd</sup> Party?

If yes, the business must provide:

- **online** Opt-Out
- Consumer rights notice and description
- Note, if the business has **actual** knowledge that Consumer is **less than 16**, it must have **affirmative** authorization to sell PI (Opt-In)
- Businesses that willfully disregard Consumer's age are **deemed to know**

# Is there Merger or Acquisition Activity?

- This involves transferal of PI as asset to 3rd party in merger, acquisition or other transaction where 3rd party assumes control of business

This is fine

- if information is used or shared inconsistently with original use, then it is a sale **and** 3rd Party must provide prior notice of new or changed practice to consumer



# Enforcement

# Enforcement Obligations

---

- **Enforcement Authority vested in the CA Attorney General**
  - Any business or 3<sup>rd</sup> Party may seek the AG's opinion regarding compliance with the Act
  - 'Go Live' date of 1/20/20, **but** AG must adopt regs and cannot bring action until 7/1/20
  - AG has authority to adopt rules and procedures as necessary to further the law's purposes
  - Enforcement tools include injunction and civil penalty not more than \$2500 per violation or not more than \$7500 per intentional violation but must give 30 day notice and opportunity to cure
  - Private CoA exists for failure to provide adequate security for PI
  - District, City & County Attorneys may also have authorization to enforce



**Questions?**