SecureTheVillage™

How Simple Changes to Your Contracts Can Mitigate Risk Under the CCPA

March, 2020

This SecureTheVillage Webinar brought to you by our NEW Platinum Investor

MILLER KAPLAN

How Simple Changes to Your Contracts Can Mitigate Risk Under the CCPA

- Guide: Stan Stahl, PhD
  - Founder, SecureTheVillage
  - President, Citadel Information Group

- Guests:
  - Matt Seror, Buchalter
  - Weiss Hamid, Buchalter

Contracts: Outline

- Outline
- CCPA Overview
- Liability impacts of CA Attorney General Guidance
- Private rights of action to CCPA
- Contract language related to opting out
- Statutory damages for data breaches except where reasonable practices and policies are in place. What does this mean?
- Relation to other CA laws that require business to have security plans. See Cal. Civ. Code 1798.81.

CCPA Overview

The goal of the CCPA is to provide California consumers transparency and options regarding the collection, retention and use of their person information. Key provisions include:

- Providing consumers the right to find out what information businesses have, the source of the information and to whom it is being shared.
- Providing consumers the right to "opt-out" from the sale of personal data.
- Prohibiting businesses from discriminating against a consumer for opting out.
- Creating a private right of action for consumers in connection with certain data breaches.
- Allowing the California Attorney General to institute civil actions stemming from CCPA violations, which could carry hefty statutory fines.

Guidance from California Attorney General

- Timeframe for compliance with consumer requests
  - A business receiving a consumer request must respond within 45 days (with one possible 45 day extension)
  - All consumer requests (and the responses thereto) must be kept for 24 months.
- Notices provided under the CCPA must use straightforward language that is easy for the average consumer to understand. Notices must be accessible to consumers with disabilities.
- Any business receiving a consumer request must take steps to verify the identity of the consumer prior to responding.
- Proposed regulations provide specific examples of non-discriminatory actions.

Do I want my vendor to be a "service provider?"

- The CCPA states "A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to "*opt-out*."
- The CCPA defines "sale" broadly: selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
- There are, however, instances where the "opt-out" would make aspects of your business more difficult:
  - Web-hosting providers
  - Data analytics provider
  - Cloud storage providers
- There is an exception that a business is not "selling personal information" if it shares personal information with a **service provider** if two conditions are met:
  - The business provided notice that the information is being used in its privacy policy;
  - The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

Service Providers Requirements

- What is a **service provider**?
  - The CCPA defines a service provider as a company "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title . . . ."
- What is a **business purpose?**
  - short term use provided it is not disclosed to a third-party or used to build a profile of the consumer
  - performing services such as customer service, order fulfillment, payment processing, advertising or marketing, analytics and similar services
- Steps you'd want to take to get your vender classified as a service provider
  - *Have a contract with the business to process personal information for a specific purpose*
  - *Make sure the contract prohibits the service provider from processing/using the data in ways not outlined in the contract*

Private Right of Action Under the CCPA

- The CCPA provides for a limited private right of action to California consumers when their "nonencrypted and nonredacted personal information" is "subject to an authorized access, exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures.
  - Not all violations of the CCPA trigger this private right of action.
- Statutory damages available. Not less that $100, not greater than $750 (per consumer/per incident).
- Business have a 30 day written notice and cure period.
- Maintenance of reasonable security procedures and practices can serve as a defense to a private right of action.
- Efforts to expand private of action have failed (so far).

What is a Reasonable Security Procedure and Practice?

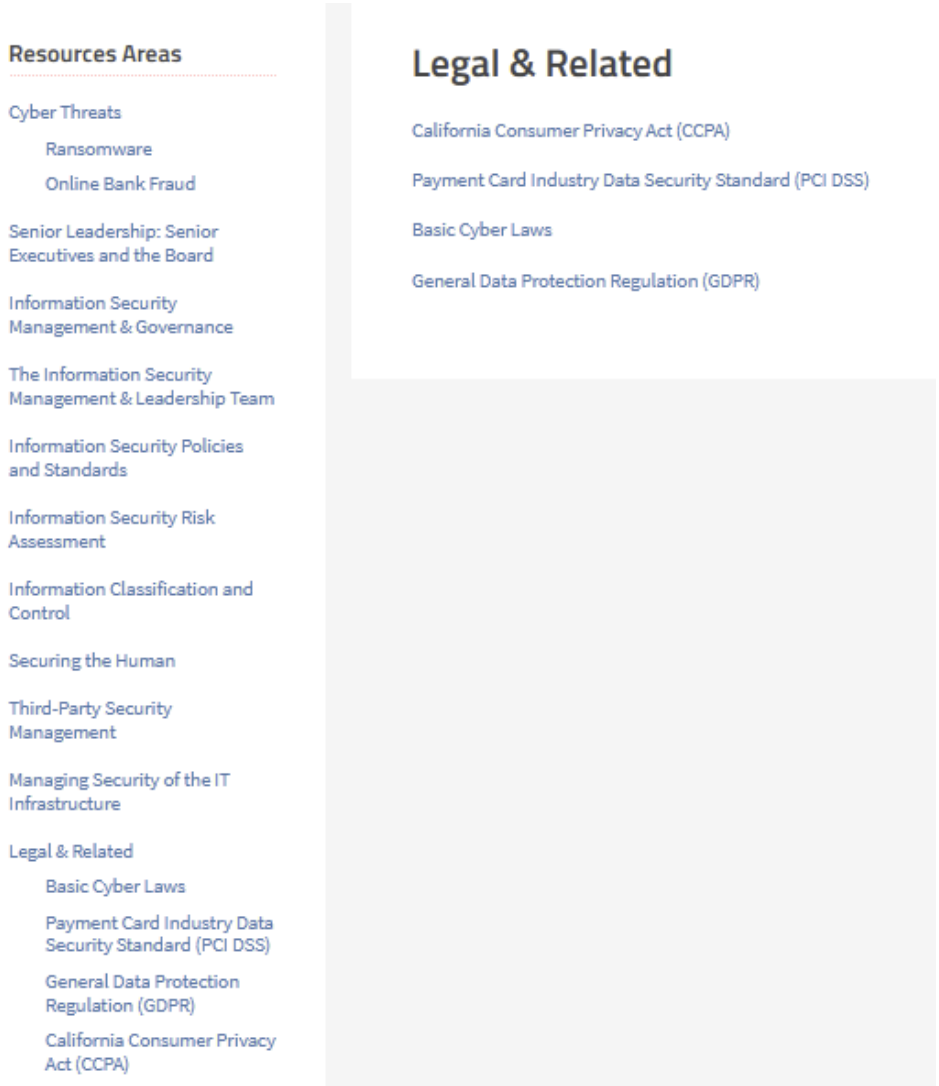
- The statute is as vague as it reads when it comes to what is “reasonable”
- California has other statutes regarding maintenance of customer records; Cal. Civ. Code 1798.81
  - A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.
  - A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.
- At a minimum, failure to comply with prior existing California statutes is likely to be unreasonable.
- Having periodic risk assessments and internal/external penetration tests will also support an argument that your security procedure and practice are reasonable.

Minimum Reasonable Information Security Practices by SecureTheVillage

- Information Security Management
- Information Security Subject Matter Expertise
- Security Management of Sensitive & Private Information
- SecureTheHuman
- Security Management of the IT Interface
- Security Management of the IT Infrastructure
- Third-Party Security Assurance
- Information Resilience
- Information Security Governance

SecureTheVillage: https://mrsp.securethevillage.org/summary-for-it-service-providers/

ResourceKit: Legal & Related



https://resourcekit.securethevillage.org/resources/legal-related/

Next Webinar: April 9

Under Development

Stay Tuned

SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable
- SecureTheVillage ResourceKit
- Second Thursday of month, 10AM Pacific

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives understand how to turn their organization into Cyber Guardians and create a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Minimum Reasonable Security Practices: A set of information security management practices so basic as to be necessary for a claim that one's information security practices and procedures are reasonable. *Developed in support of CCPA.*

Community-Based Programs: Train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: *SecureTheVillage.org*

For More Information …

Stan Stahl, SecureTheVillage & Miller Kaplan
Stan@SecureTheVillage.org
@stanstahl
323-428-0441

Matt Seror, Shareholder, Buchalter
mseror@buchalter.com
213-891-5731

Weiss Hamid, Associate, Buchalter
whamid@buchalter.com
(213) 891-5087

FREE *Cybersecurity News of the Week & Weekend Vulnerability and Patch Report*
https://SecureTheVillage.org

Interested in Cybersecurity? Please Get Involved!!!

Follow SecureTheVillage on LinkedIn
https://www.linkedin.com/company/secure-the-village

Get Our Free *Cybersecurity News of the Week & Weekend Vulnerability & Patch Report*
https://securethevillage.org/

Attend an Event
https://securethevillage.org/events/

Join the SecureTheVillage Leadership Council
https://securethevillage.org/about/leadership-council/
https://securethevillage.org/about/leadership-council-faq/

For Marketing / Sponsorship Opportunities
Email us at info@securethevillage.org. Put *Sponsor Opportunity* in Subject
Visit us at https://securethevillage.org/sponsorship-opportunities/

SecureTheVillage™

How Simple Changes to Your Contracts Can Mitigate Risk Under the CCPA

Thank You!