2020 Privacy Law Update: The Impact of the California Consumer Privacy Act (CCPA)

PRESENTED BY:
Amanda L. Gratchner, Principal, IdeaLegal
Andrew Migliore, VP of Engineering & Security Officer, RadarFirst
Xavier Clark, Technology Attorney, Schwabe, Williamson & Wyatt
Alex Wall, Wall Law

Disclaimer

- Information is for educational purposes only
- **Not legal advice**

Agenda

- Security Fundamentals
- CCPA Overview
- Compliance Considerations

Privacy is *not* Security

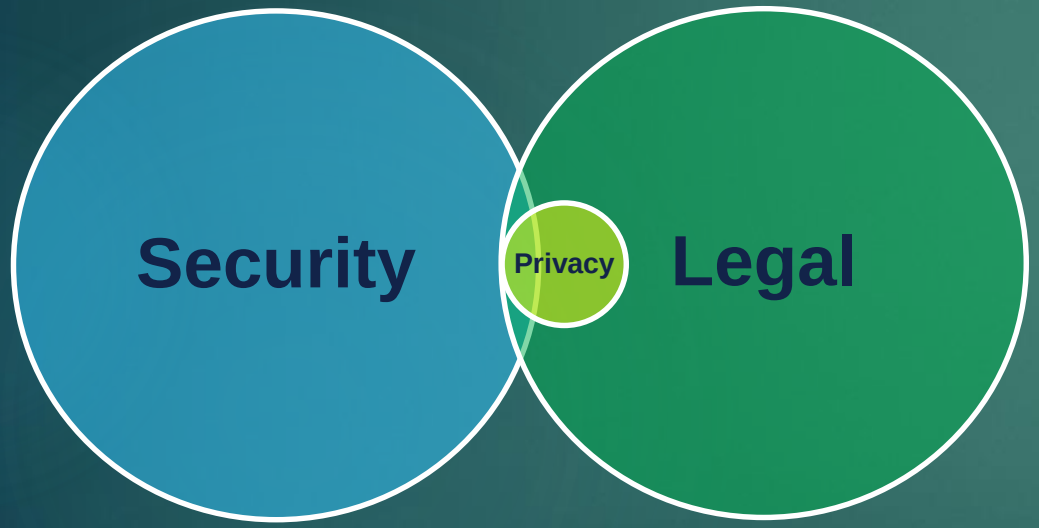
Sharing a common goal to protect personal information

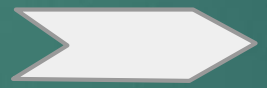
Privacy	Security
Focused on how personal information is collected, used, and disclosed.	Focused on safeguarding data from unauthorized use or disclosure.

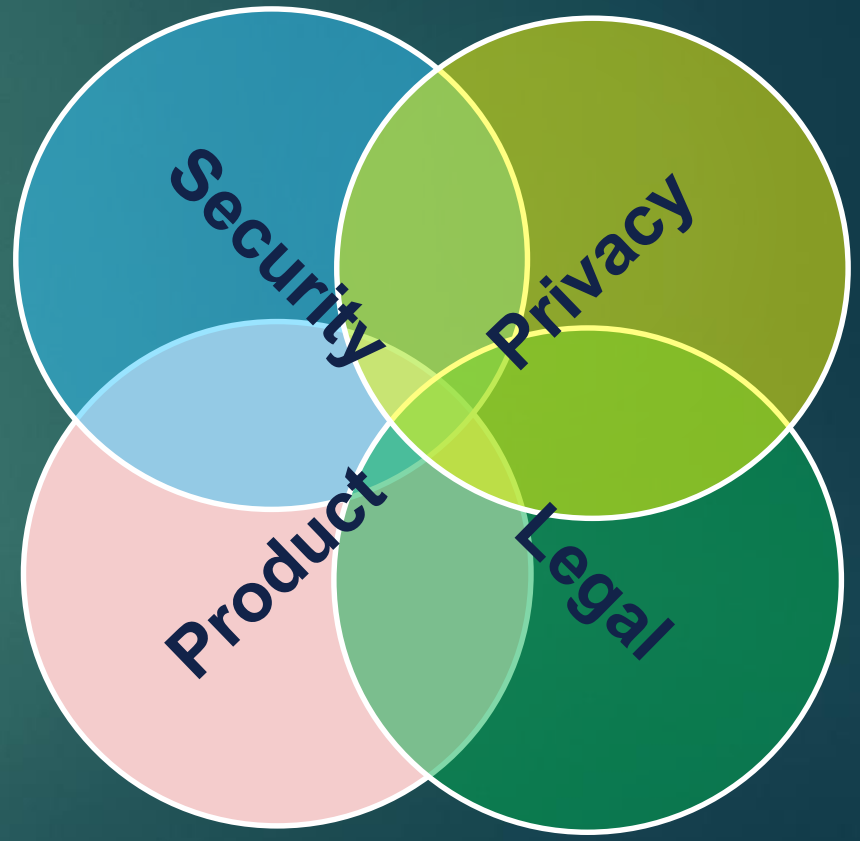
Why security needs to care about privacy:

Organizations have to evolve to keep pace

Privacy, historically, was addressed by Security by throwing incidents over the wall to Legal...







But now Privacy needs to be an equal partner as the landscape is far more complex.

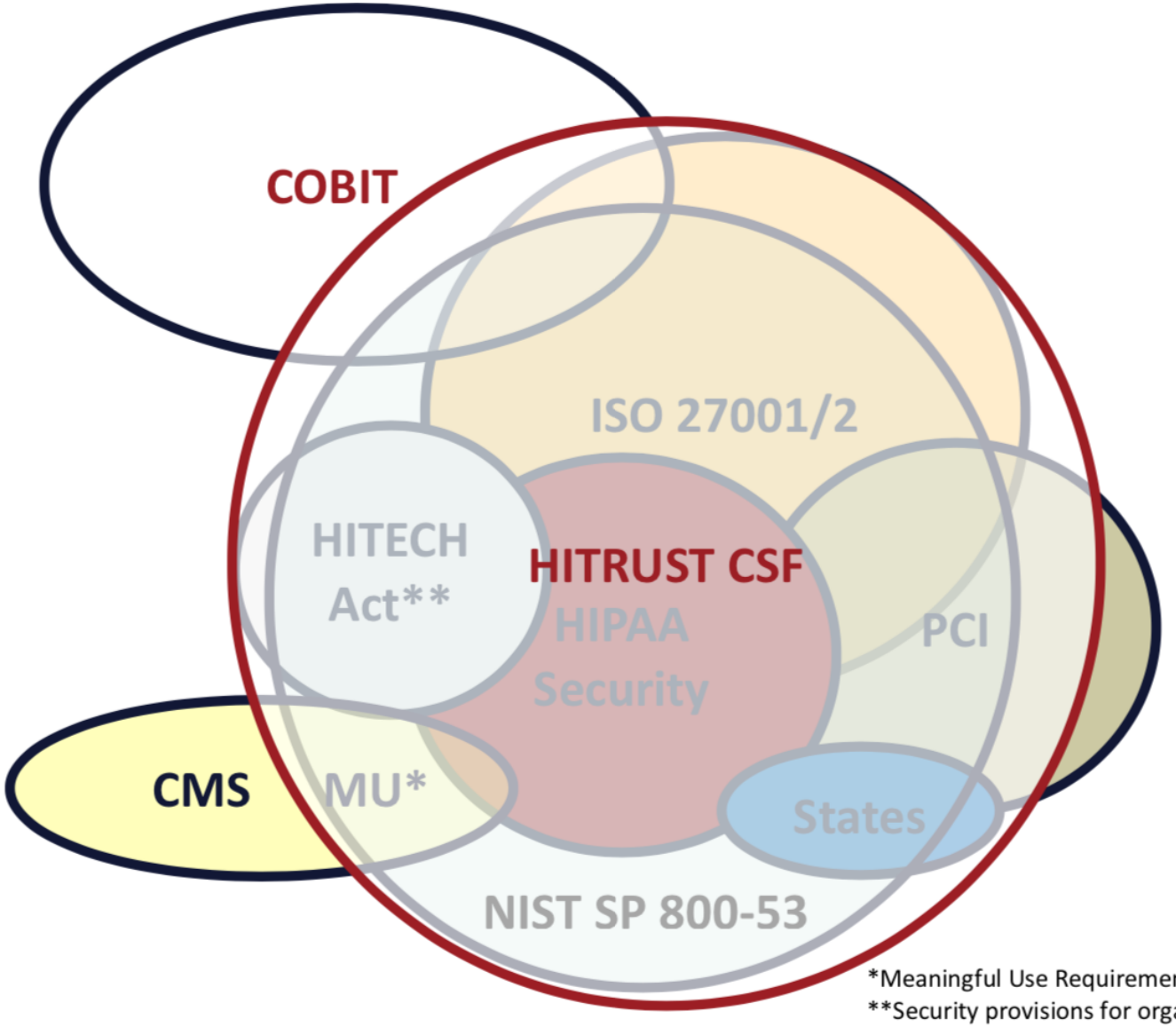
Privacy by Design (PbD):The 7 Foundational Principles

Although PbD is not new, GDPR made it a legal requirement. Even if your company is not subject to the GDPR it is good practice for what is to come.

The following are the 7 foundational principles.

1. Privacy as the Default
2. Privacy Embedded into Design
3. Full Functionality — Positive-Sum, not Zero-Sum
4. End-to-End Security — Lifecycle Protection
5. Visibility and Transparency
6. Respect for User Privacy
7. Proactive not Reactive / Preventative not Remedial

How different Security Frameworks overlap



*Meaningful Use Requirements
**Security provisions for organizations

What is an ISO 27001 audit

ISO 27001 is the internationally-accepted standard for governing an organization's information security management system (ISMS). The ISMS preserves the confidentiality, integrity, and availability of information by applying a risk management process. Certification gives confidence to interested parties that risks are managed. ISO 27001 standard regulates an ISMS through policies and procedures and associated legal, physical, and technical controls.

What is a SOC 2 audit

A Service Organization Control (SOC) report comes in three varieties and can be used to review potential third-party service providers or shared with prospects and customers to demonstrate your company's information security controls.

SOC 1 reports are traditionally used to prove controls over financial reporting.

SOC 2 incorporates Trust Services Criteria (TSC) for general IT controls.

SOC 3 is an abstract of a SOC 2 report without any sensitive information so that it can be public facing and suitable for marketing purposes.

SOC 2 Type I and Type II

Point in time vs. a period of time

A **Type I** report focuses on management's **description** of the company's controls and effectiveness at *a point in time*. The auditor then prepares the report, interpreting this description in their professional opinion.

A **Type II** report, involves the American Institute of Certified Public Accountants (AICPA) attestation requirements. Type II focuses on more than a single snapshot and instead reviews *a period of time*. Management must provide documentation proving the **effectiveness** of its controls throughout the audit period.

SOC 2 Type II vs ISO 27001: the end result

Report (SOC) vs. Certificate (ISO)

- A SOC attestation report contains an auditor opinion letter, an assertion letter from the service organization's management, a system description containing a narrative on the five key components concerning the system under review (infrastructure, software, people, procedures, and data), and the applicable trust services criteria, related control, and the testing results.
- An ISO 27001 engagement results in a certificate which is a 1-2 page document which contains information such as the ISMS scope, in-scope locations, standard certified against, effective dates of the certificate (date issued, date of expiration, etc.).

CCPA

- Effective: January 1, 2020
- California AG enforcement: July 1, 2020
- AG regulations not yet finalized
- Amendments to CCPA pushed some obligations to January 1, 2021 (related to employee and business-to-business personal information)
- Expands the rights of consumers and requires businesses to disclose how personal information is collected, used and disclosed

Who does CCPA apply to?

Consumers:

- California residents;
- Excludes personal information of employees (used for employment purposes) and individuals in business-to-business communications until January 1, 2021

Businesses:

- Annual gross revenue exceeds $25 million; or
- 50% or more of annual revenue from sharing personal information of consumers; or
- Annually buys, sells, receives or shares personal information of 50,000 consumers or devices

What does CCPA apply to?

- **Personal Information**: information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household.
  - Examples: name, postal/email address, unique personal identifier, IP address, account name, government identifier number (SS, driver's license, passport); records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; biometric information; Internet activity including browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement; geolocation data; audio, electronic, visual, thermal, olfactory, or similar information; employment-related information; education information; inferences drawn from any of the information identified to create a profile about a consumer

What rights does CCPA grant?

Notice & Transparency

At or before collection: categories of information collected and the purpose

Typically disclosed through a privacy policy

Notice requirement applies to employee information now

Right to Know

What is collected

Categories of third parties it is shared with

Categories of sources of information and

The purpose

*Same rights apply where a business sells the information + opt-out of selling

Right to Deletion

Not an absolute right

Exemptions

- Transactional data
- Security
- Errors
- Free Speech
- CECPA Compliance
- Public Interest Research
- Expected Internal uses
- Legal Compliance
- Other Internal Uses

CCPA Compliance Considerations

Policies/Procedures

Privacy Notice (public)

Employee Privacy Notice

Data Sharing

Individual Rights Requests

Security

Encryption

Contracts

Vendor contract provisions

Data sharing agreements

Enforcement and Damages

"We will look kindly, given that we are an agency with limited resources, and we will look kindly on those that … demonstrate an effort to comply…[but], if they are not (operating properly) … ***I will descend on them and make an example of them***, to show that if you don't do it the right way, this is what is going to happen to you."

- California Attorney General Xavier Becerra on CCPA Enforcement, *Reuters, December 10, 2019*

Enforcement and Damages

AG enforcement begins July 1, 2020

Attorney General

1798.155. Attorney General can bring a civil action to enjoin violating activities and assess and recover penaltie$

- 30 day notice and cure period;
- $2500 per violation
- $7500 per *intentional* violation
- Violation not a defined term (what if a single process violation impacts multiple consumers?)

Private Right of Action

1798.150. Breach involving non-encrypted and non-redacted "personal information" (narrower definition) as a result of a business' violation of duty re reasonable security procedures and practices

- Consumers can bring individual or class action after 30 day notice and cure period;
- Greater of actual or statutory damages;
- Statutory: $100-$750 per consumer, per violation

Other Harm

Reputational

"I will descend on them and *make an example of them*"

- Consumer trust, loyalty
- Competitive disadvantage

Business / Commercial

- Sales / Tarnished Brand
- Partnerships / alliances
- Marketing / PR costs
- Insurance costs
- Regulatory scrutiny
- M & A challenges

Noteworthy Terms - 1798.140. Definitions

(a) "**Aggregate consumer information**" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been de-identified;

(h) "**Deidentified**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:
(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
(2) Has implemented business processes that specifically prohibit reidentification of the information.
(3) Has implemented business processes to prevent inadvertent release of deidentified information.
(4) Makes no attempt to reidentify the information.

(o)(3) "**Personal Information**" *does not include* consumer information that is *deidentified* or *aggregate consumer information*.

Noteworthy Terms - 1798.140. Definitions

(c) "**Business**" means:
(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which thatsuch information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185;
(B) Alone or in combination, annually buys, receives *for the business' commercial purposes*, sells, or shares *for commercial purposes*, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

Noteworthy Terms - 1798.140. Definitions

(d) "**Business purpose**" means the use of personal information for the business' or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.
(The statute lists seven categories of uses of PI for "business purposes" such as certain auditing, detecting security incidents or illegal activity, debugging, non-commercial transient use, service provider use, internal R&D, and quality control.)

(f) "**Commercial purposes**" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

Noteworthy Terms - 1798.140. Definitions

(t)(1) "**Sell**," "**selling**," "**sale**," or "**sold**," means 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*.

(t)(2)(c) For purposes of this title, a *business does not sell* personal information when:
The business uses or shares *with a service provider* personal information of a consumer that is necessary to perform a *business purposes* if both of the following conditions are met:
- (i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.
- (ii) The service provider does not further collect, sell, or use the *personal information* of the consumer except as necessary to perform the business purpose.

Questions

Resources

- CCPA: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100.
- Office of the Attorney General (CA): https://oag.ca.gov/privacy/ccpa
- California AG *Proposed* Regulations: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf