RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PRV-T08**

It’s All About the States: Navigating the Privacy Thicket

Behnam Dayanim

Partner, Global Chair of Privacy & Cybersecurity Practice
Paul Hastings LLP

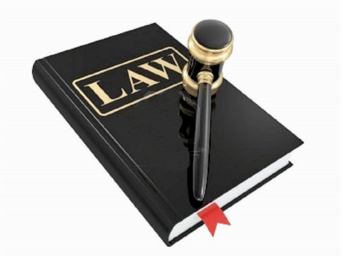
#RSAC

Agenda

- History of state legislation on privacy and security
- Background, provisions and current status of CCPA
- Other states’ new privacy efforts
- Federal enforcement and legislative responses
- What to expect next?
- What to do next?

Privacy And Security

- A promise of *privacy* is meaningless without *security.*
- *Privacy:* Deciding ownership, use and disclosure of personal information
  - A public policy question – societal, business, political
  - As a result, more "law dependent"



- *Security:* Protecting information from unauthorized or unwanted access or disclosure
  - An implementation issue – technical, administrative, "cultural"

Early efforts in privacy

- Focused on credit reporting agencies, largely (although not entirely) preempted
- CalFIPA (2004) and Vermont Financial Privacy Act (2001)
- California Confidentiality of Medical Information Act (CMIA) (2012)
- A few states enacted certain types of online privacy acts, requiring privacy notices, tracking disclosures and the like
- Sector-specific or narrowly targeted

Security Laws – first comprehensive safeguard req'ts

- **MA 201**
  - **WISP Required**. Massachusetts law (namely, 201 C.M.R. 17 et seq. ("MA 201")) requires covered organizations to maintain a comprehensive written information security program ("WISP").
    - WISP records containing personal information ("PI") about MA residents.
  - **Risk-Based Approach**. MA 201 adopts a risk-based approach to info security, meaning that the WISP can take into account the business' "size, scope and type."
  - **12 implementation specifications and 8 specific control requirements**

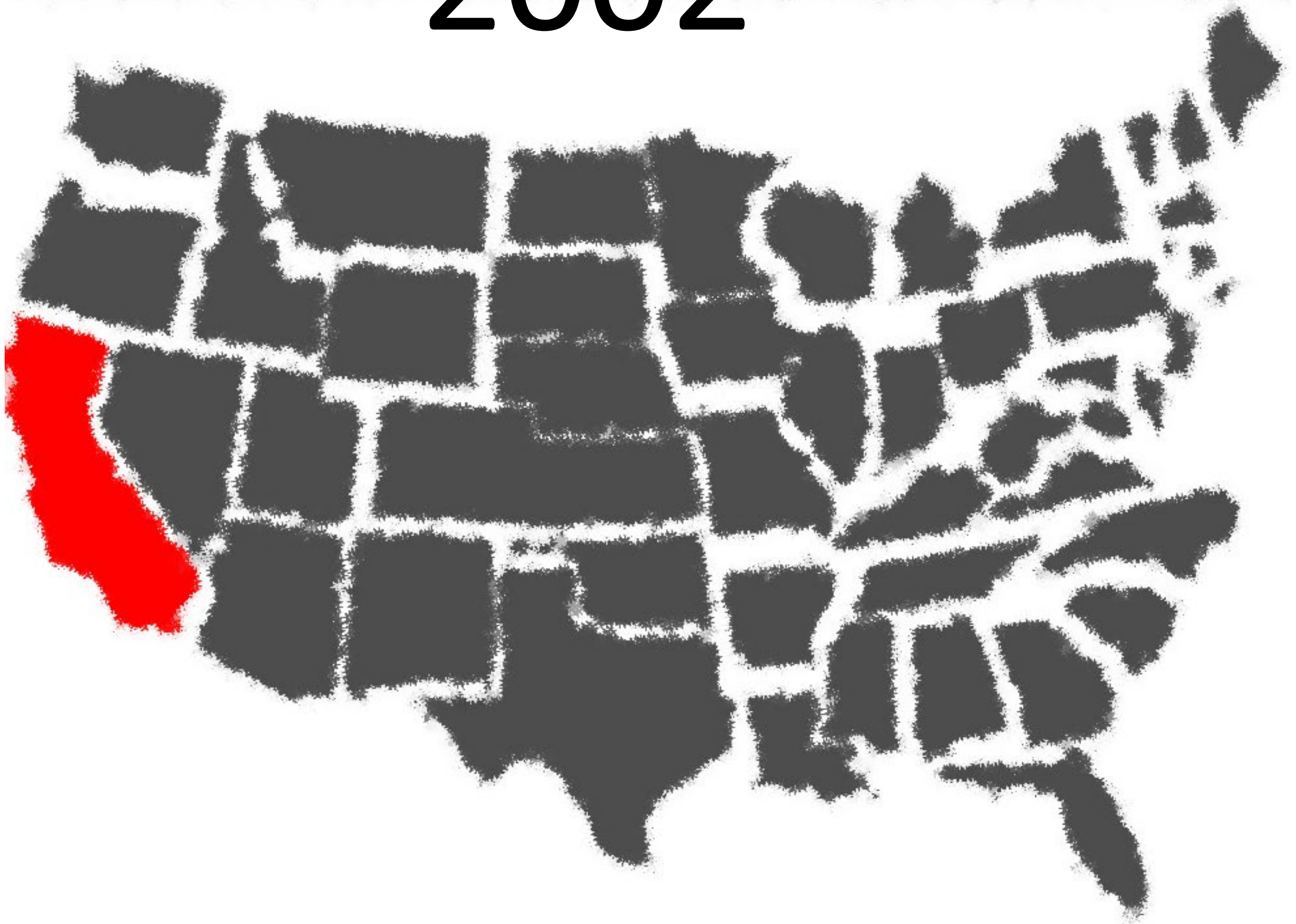
New York DFS Cybersecurity Rule

- **Scope**. Applies to banks, insurers and other financial services institutions (MTLs) subject to its jurisdiction.
- **Cybersecurity Program**. Establish a program designed to ensure confidentiality, integrity and availability of information systems.
- **Written Policies**. Adopt written policies and procedures to protect information systems and nonpublic information.
  - Board of Directors must review; senior officer must sign off.
- **CISO**. Designate a qualified individual to serve as Chief Information Security Officer (CISO).
  - Must submit report to board, at least biannually, on policies' effectiveness.
- **Pen Testing/Vulnerability Assessments**. Continuous monitoring or annual testing/assessments.
- **Vendors**. Design policies and procedures to ensure security of systems and non-public information accessible to third-party service providers.
  - Requires (i) vendors meet "minimum cybersecurity practices" and (ii) periodic assessment, at least annually.

State Data Breach Notification Laws

2002

Eighteen years ago…



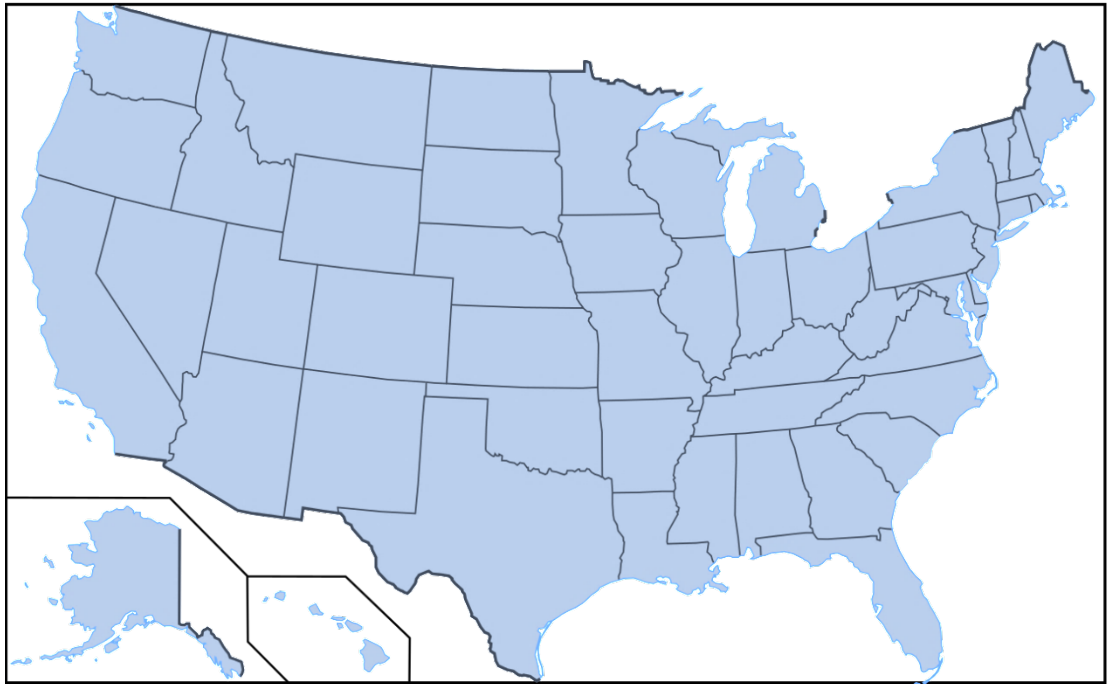
No Legislation Enacted

Legislation Enacted

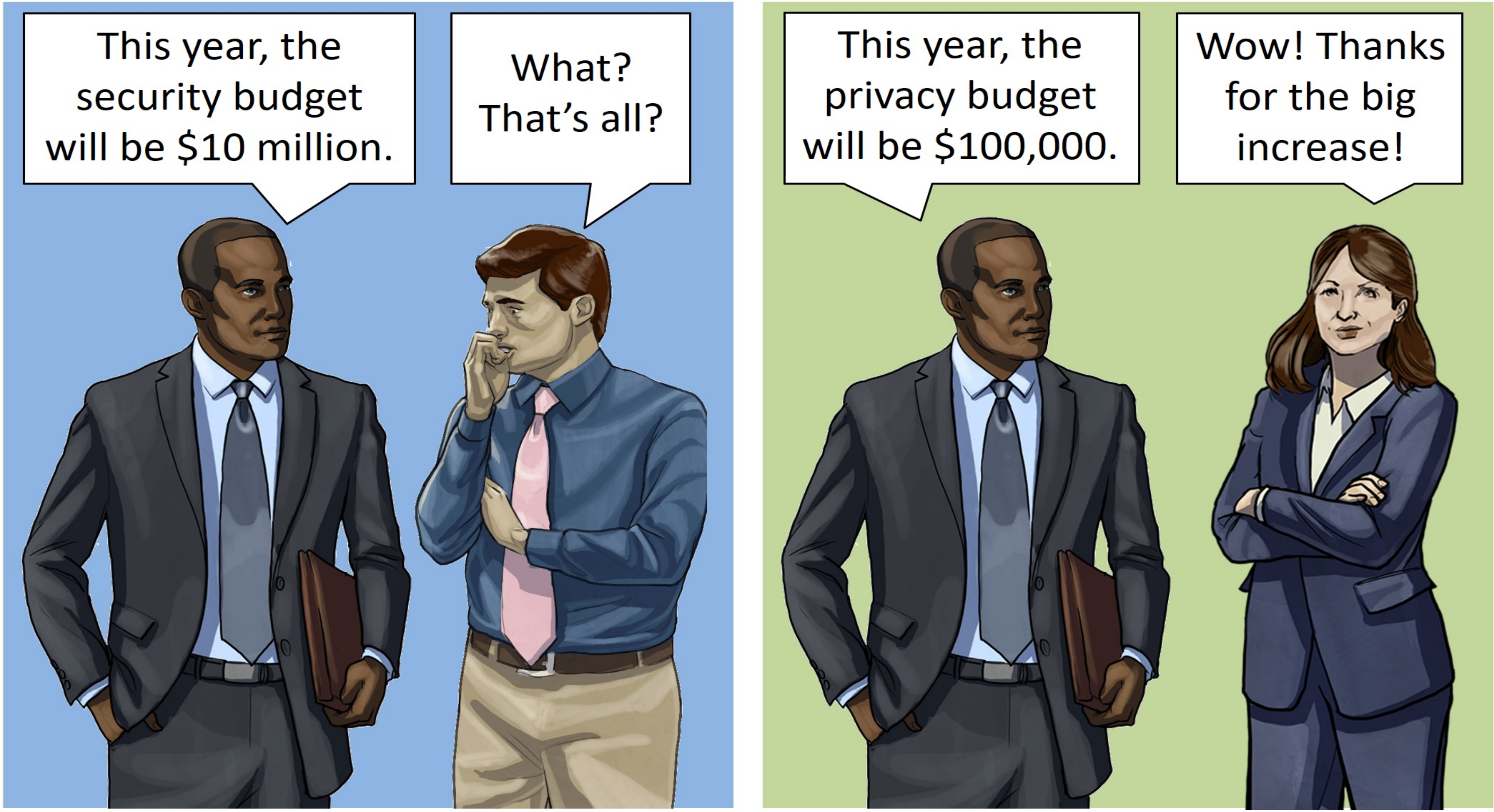
State Data Breach Notification Laws

2020

Today…



Legislation Enacted

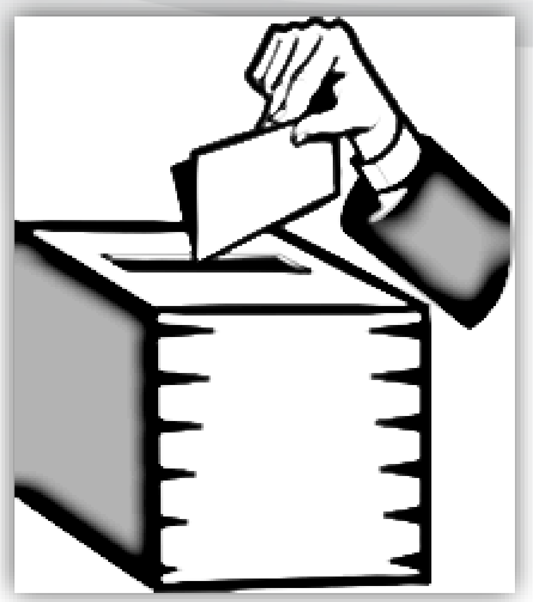

This year, the security budget will be $10 million.
What? That's all?
This year, the privacy budget will be $100,000.
Wow! Thanks for the big increase!

Written by Daniel J. Solove

www.teachprivacy.com

Illustrated by Ryan Beckwith

CCPA, A History: Introduction



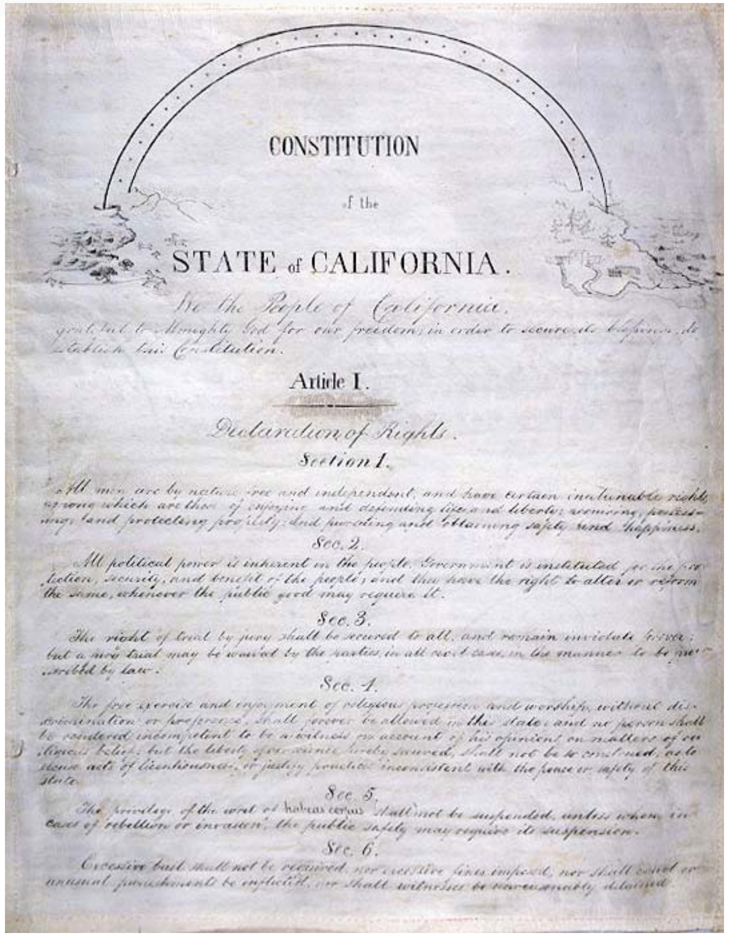
- The CCPA exists largely due to the efforts of one man—Alastair Mactaggart, a wealthy California real estate investor who started worrying about data privacy after talking with an engineer from Google.

- Mactaggart spent nearly $3.5 million to place an initiative on California's November 2018 ballot to enhance privacy rights in California.

CCPA, A History: CCPA Adopted

- In California, a ballot initiative cannot be amended by the legislature.

- This brought industry to the table to fast-track a legislative alternative to the ballot initiative. After only a few weeks of negotiations, the CCPA was adopted.



CONSTITUTION

of the

STATE of CALIFORNIA.

We the People of California, grateful to Almighty God for our freedom, in order to secure its blessings, do establish this Constitution.

Article I.

Declaration of Rights.

Section 1.

All men are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing and protecting property; and pursuing and obtaining safety and happiness.

Sec. 2.

All political power is inherent in the people. Government is instituted for the protection, security, and benefit of the people; and they have the right to alter or reform the same, whenever the public good may require it.

Sec. 3.

The right of trial by jury shall be secured to all, and remain inviolate forever; but a jury trial may be waived by the parties in all civil cases, in the manner to be prescribed by law.

Sec. 4.

The free exercise and enjoyment of religious profession and worship, without discrimination or preference, shall forever be allowed in this state; and no person shall be rendered incompetent to be a witness on account of his opinions on matters of religious belief; but the liberty of conscience hereby secured, shall not be so construed, as to excuse acts of licentiousness, or justify practices inconsistent with the peace or safety of this State.

Sec. 5.

The privilege of the writ of habeas corpus shall not be suspended, unless when in cases of rebellion or invasion, the public safety may require its suspension.

Sec. 6.

Excessive bail shall not be required, nor excessive fines imposed, nor shall cruel or unusual punishments be inflicted, nor shall witnesses be unreasonably detained.

CCPA History

Ballot Measure Proposed
Oct. 12, 2017

CCPA Adopted
June 28, 2018

CCPA Amended
Sept. 23, 2018

CCPA Effective Date
Jan. 1, 2020

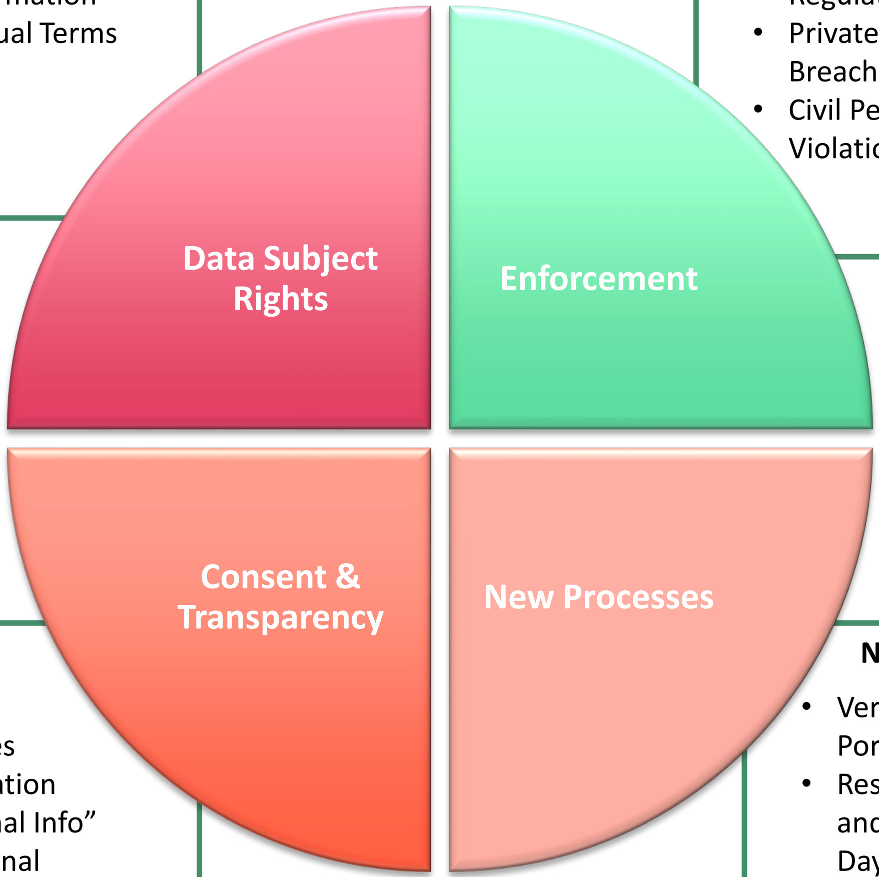
CCPA Overview

Data Subject Rights

- Notice to Data Subjects
- Opt-Out of Sale of Information
- Receive Services on Equal Terms
- Breach Notification
- Data Portability
- Deletion
- Access

Enforcement

- Attorney General to Adopt Final Regulations by July 1, 2020
- Private Right of Action for Data Breach
- Civil Penalties: $2,500-$7,500 Per Violation



Consent/Transparency

- Opt-Out Regime
- Updated Privacy Policies
- 12 Month Opt-In Limitation
- “Do Not Sell My Personal Info”
- Opt-In for Sale of Personal Information Under Age 16

New Processes

- Verification for Access, Deletion, or Portability Requests
- Response to Data Access, Deletion, and Portability Requests within 45 Days
- Determine age of CA Resident
- Reasonable Security

What are the potential fines?

- California AG
  - California AG can bring civil penalties of $2,500-$7,500 depending on nature of violation (e.g., intentional or not) and can also bring injunctive relief (i.e., can order entities to stop certain practices).
  - Not until **July 2020**.
- Individual Lawsuits
  - However, **private right of action (e.g., lawsuits brought by, or on behalf of, individuals) for data breaches began on January 1, 2020.**
  - The potential liability can be extraordinary—companies liable for damages between $100–$750 per consumer per incident or actual damages, whichever is greater. Consumers don’t need to show actual harm!

A US GDPR?

- Some similarities, but important differences.
- No express consent requirement and opt-out from “sale” (disclosure) only.
- Narrower rights of access and deletion.
- Much narrower range of potential penalties.

CCPA Core Requirements

<table>
<tr><th></th><th>GDPR Core Requirements</th><th>California Consumer Privacy Act Core Requirements</th></tr>
<tr><td rowspan="2"><b>Security</b></td><td colspan="2"><b>Appropriate Data Security to Safeguard Information</b>
Articles 5(1)(f), 32; CCPA Sec. 1798.150(a)(1)</td></tr>
<tr><td colspan="2"><b>Breach Notification</b>
GDPR Articles 33, 34; CCPA Sec. 1798.112 (no new notification requirements, but allows statutory damages for breach violations)</td></tr>
<tr><td><b>Data Transfers</b></td><td><b>Adequacy measures required for transfers outside EEA</b>
Articles 44-50</td><td></td></tr>
<tr><td><b>Service Providers</b></td><td><b>Contractual Requirements in Service Provider Agreements</b>
Articles 23, 28</td><td></td></tr>
<tr><td><b>Personal Data</b></td><td><b>Information Relating to an Identified or Identifiable Person</b>
Articles 1, 4</td><td><b>Expanded Definition of Personal Information</b>
CCPA Sec. 1798.140(o)</td></tr>
<tr><td><b>Compliance Timing</b></td><td><b>24 months (after 4 years of legislative negotiations)</b></td><td><b>18 months (after 7 days of legislative activity)</b></td></tr>
<tr><td><b>Request Channel</b></td><td></td><td><b>Toll-Free Number Required</b>
CCPA Sec. 1798.130(a)(1)</td></tr>
<tr><td><b>Disclosures</b></td><td><b>Appropriate Disclosures to Data Subjects</b>
Articles 12-14</td><td><b>Mandated Specific Disclosures</b>
CCPA Sec. 1798.130</td></tr>
</table>

INCREASED BURDENS UNDER CCPA

- While GDPR and CCPA have many similarities and both laws require companies to adopt comprehensive data protection programs, the CCPA will impose additional burdens on companies beyond what may have been done for GDPR compliance.

	GDPR	CCPA
CCPA is broader in scope	The GDPR regulates data that is traditionally thought of as "personal data"	The CCPA regulates more information, including data related to households and devices, which will, in turn, impact systems and data sets unaffected by GDPR
CCPA is Still a Moving Target	GDPR was negotiated for several years and went through multiple public iterations	CCPA was drafted and passed quickly, which may require amendments and shifting requirements
CCPA is Unprecedented in the US	The General Data Protection Directive (GDPR's predecessor) was in place for over 22 years	No comprehensive rights-based data protection framework has previously been implemented in the United States

INCREASED BURDENS UNDER CCPA

- While GDPR and CCPA have many similarities and both laws require companies to adopt comprehensive data protection programs, the CCPA will impose additional burdens on companies beyond what may have been done for GDPR compliance.

	GDPR	CCPA
CCPA has Increased Litigation Risk	GDPR provides a private right of action and the right to enter into group litigation; however, these are not common in the EU	Litigation risk under the CCPA's private right of action is high, particularly given the highly developed class action system present in the United States
CCPA has Less Flexible Requirements	Under GDPR, companies have some flexibility in how companies must provide notice and communications with customers	The CCPA requires companies to use certain communications channels (e.g. toll free numbers), as well as very specific disclosure requirements
CCPA Has Additional Consumer Rights and Requirements	GDPR establishes numerous rights (access, correction, deletion, portability, restriction of processing) with broad exceptions	The CCPA establishes a right for consumers to request deletion of any personal information about the consumer, also with broad exceptions, but with a specific mechanism to opt out of the sale of personal data

Important Exemptions and Limitations

- **Retention**. Adds the following language in italics: "This title shall not be construed to require a business to *collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or* reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."
- **B2B Communications (One-Year Moratorium)**. Added a one-year moratorium on CCPA obligations for businesses that process personal information of individuals acting in their capacity as an employee (or owner, director, officer, or contractor) of another entity, provided such processing is related to (i) providing or receiving a product or service to/from such entity or (ii) due diligence of such entity. However, the private right of action for data breaches, right to opt-out of "sales," and right against non-discrimination still apply. **This exemption will expire on January 1, 2021.**

Important Exemptions and Limitations, cont’d

- Exemption for three categories of employment-related “personal information” until **January 1, 2021:**
  - information that is collected from individuals in the course of a job application or from employees in the course of employment;
  - information that is collected and used solely within the context of having an emergency contact on file; and
  - information that is collected and used solely within the context of administering employment-related benefits.
- However, the notice provision and the private right of action for breach provision still apply.

Areas of Tension or Uncertainty

- **Scope of "Sale"**
- "**Publicly available information**" (which is not considered "personal information") – "information that is lawfully made available from federal, state, or local government records"
- **Non-discrimination**. A business may charge a consumer a different amount or provide a different level or quality of goods or services "if that difference is reasonably related to the value provided to the business by the consumer's data" (rather than the value provided to the *consumer*)
- ***How to treat non-Californians?***

US State and Federal Efforts to Strengthen Privacy Rules

State

Legislation has been introduced or enacted in at least 15 US states :

Hawaii
Illinois
Maine
Maryland
Massachusetts
Nebraska
New Hampshire
New Mexico
New Jersey
New York
Nevada
North Dakota
Rhode Island
Texas
Virginia
Washington

Federal

Dec. 18, 2019

House Energy & Commerce Committee staff circulate a draft bipartisan privacy bill.

Nov. 26, 2019

Consumer Online Privacy Rights Act introduced in Senate

April 10, 2019

BROWSER Act introduced in Senate

Jan. 15-16, 2019

Apple CEO Tim Cook and GAO both recommend "comprehensive federal privacy legislation."

But first . . .

Again?

CCPA 2.0

- If enough signatures are received, the **California Privacy Rights Act of 2020** (the "**CPRA**") will appear on the Nov. 2020 ballot initiative.
- Would go into effect **January 1, 2023**
- New **right to opt-out of "sharing"**
  - "Sharing" is a disclosure even without consideration, and expressly including for behavioral advertising.
  - Limited exception for targeting using only first-party data of website with which the consumer is "intentionally interacting."
- Establishment of "**California Privacy Protection Agency**": Tasked with implementing and enforcing the CPRA

CCPA 2.0 cont'd

- New or modified links on homepage:
  - "**Do Not Sell or Share My Personal Information**": Allows opt-out of both (i) "sales" and (ii) any "sharing" of personal information.
  - "**Limit the Use of My Sensitive Information**": Allows opt-out of use of "sensitive personal information" except for defined business purposes.
- One "clearly labeled" link allowed if it allows same opt-out functionality (unknown what it needs to be called)

Nevada ("mini-CCPA")

- In May 2019, law amended to require online services to post privacy notices with right of opt-out from "sale"
  - "Sale" means transfer for money of covered information to a person **for resale/re-transfer** (narrower than CCPA)
  - "Covered information" also is narrower than CCPA
- Applies to anyone targeting NV consumers (in traditional sense)
- Excludes entities covered by GLBA or HIPAA
- No rights of access, deletion, portability, non-discrimination
- No private right of action

Maine

- Act to Protect Consumer Online Personal Information
- Reaction to congressional reversal of Obama-era FCC rule
- Broadband service provider cannot use or disclose customer PI absent express consent
  - Standard exceptions (advertise own products, payment, fraud, etc.)
  - Covers “information from a customer's use of broadband Internet access service, including but not limited to. . .” browsing and app usage, precise geolocation, financial, health, children, device ID, etc.
- Must implement “reasonable” security measures
- Cannot condition or disadvantage service based on refusal to consent
- Only applies to BSPs operating within the state
- In some respects broader than longstanding MN and NV laws governing ISPs
- ISPs have filed suit, attacking constitutionality of the statute

New York

- Back to security paradigm with SHIELD Act
- Takes effect March 2020
- Mandates certain security measures (similar to MA)
- Expands definition of “private information” (consistent with some other states)
- Expands notice obligation to include “access” (not just “acquisition”)

CCPA/GDPR "Copycat" Bills

- "**Washington Privacy Act**" (SB 6281):
  - Right to opt-out of sales, profiling and targeted advertising
  - Imports "controller" and "processor" definitions from the GDPR
  - Enforcement by attorney general only
- **New Jersey** (SB 269)
  - Requires disclosure of legal basis for each processing activity
    - Doesn't define or otherwise elaborate on what a "legal basis" is
  - Requires data retention period
  - Information security program must meet standard imposed by (i) applicable federal law or (ii) industry standards.

New York

- New York Privacy Act (SB 5642)
  - Similar to CCPA but more far-reaching in some respects
  - Creates "data fiduciary" obligations that supersede duties to owners or shareholders
  - No processing of personal data without opt-in consent
    - "Consent" definition imported from GDPR
  - Imports "controller" and "processor" definitions from GDPR
  - Private right of action
  - No location, size or revenue exceptions for those covered

Illinois (a mini-CCPA)

- Data Transparency and Privacy Act – not yet enacted
- Similar to CCPA, although somewhat narrower
- Excludes employment context
- Applies only to a "private entity" that owns a website or application that either buys, receives sells or shares for a commercial purpose the information of more than 50,000 consumers or derives 50% or more of its annual revenues from selling personal information
- More limited transparency/disclosure obligation
- Narrower definition of sale: "*selling, renting, or licensing of a consumer's personal information by an operator to a third party in direct exchange for monetary consideration, whereby, as a result of such transaction, the third party may use the personal information for its own commercial purposes*."
- Blanket carve-out for entities regulated by GLBA and HIPAA (but not FCRA)

CCPA/GDPR "Copycat" Bills

- Other "copycat" bills:
  - Nebraska (LB 746)
  - New Hampshire (HB 1680-FN)
  - Virginia (HB 473)
- Other bills more limited in scope also introduced to state legislatures
- All bills are relatively early in committee process
  - Washington Privacy Act likely furthest along

Federal Debate and Action

- BROWSER Act, introduced in Senate with bipartisan sponsorship
  - Applies to “broadband internet access services” and “edge services”
  - Requires “clear and conspicuous” notice of privacy policy (prescribes requirements)
  - Opt-in for use or disclosure of “sensitive” information
    - includes financial, health, children under 13, SSN, precise geolocation, browsing history/app usage and content of communications
  - Opt-out for other information
  - No forced waiver
  - FTC enforces; **preempts state law**

Federal Debate and Action

- Consumer Online Privacy Act
  - Democratic sponsors
  - Broad definition of PI
  - Preemption of conflicting state laws but **not** those with greater protection
  - Rights of opt-out for transfer, access, deletion, correction and portability; may not waive those rights
  - Obligation of data minimization and express consent for “sensitive” data (including intimate images and geolocation information)
  - Requires appointment of privacy officer and privacy/risk assessments
  - Non-discrimination limitations on use of data

Federal Debate and Action

- COPRA, cont'd
  - "reasonable" security practices, including vulnerability assessments, secure data retention and disposal, and employee training
  - "Large" data collectors require CEO certification
    - 5M data subjects/100K "sensitive" data
  - New privacy/security-focused bureau within FTC
  - FTC and state attorneys general can enforce
  - Private right of action (damages from $100 to $1K per violation per day)
  - Prohibits pre-dispute arbitration agreements
  - Excludes "small" businesses from its scope
    - Annual revenue of $25M or less
    - Process PI of fewer than 100K data subjects **and**
    - Derives less than 50% of revenue from transferring PI to others

Federal Debate and Action

- Republican alternative (Sen. Wicker (R-MS))
  - Similar to COPRA *but* narrower
  - No explicit non-discrimination provisions.
  - Privacy impact assessments only required of “large” data holders
  - Preempts state laws “related to the data privacy or security and associated activities of covered entities.”
  - Does not preclude arbitration and silent on private right of action.
  - Includes an interesting “constitutional avoidance” provision.
  - Affirmative consent for transfer of minor’s data; if under 16, parental consent required.

NIST Privacy Framework

- Attempt to systematize how companies think about privacy
  - Similar approach to Cybersecurity Framework
- **Core**
  - Activities and outcomes that enable dialogue about managing privacy risk
- **Profiles**
  - Specific functions, categories and specifications that manage risk
- **Implementation Tiers**
  - Support communication regarding whether sufficient mechanisms in place
- Not binding; faces significant challenges

In The Meantime, How to Comply?

- Federal deliverance is not coming (soon).
- CCPA, CCPA, CCPA
- Risk-based approach to advertising and other forms of “sale”
- Decide whether and to what extent to extend CCPA rights to others
  - Full rights
  - No rights
  - “Directionally similar” rights

Steps to Compliance

Know Your Data

- Inventory your data – know what personal information you collect and why
- Map your data – know how information is collected, where it is stored, who has access to it, where (and to whom) it is transferred and how long you keep it

Know Your 3rd Parties

- Know what 3rd parties have access to your data – create an inventory of all 3rd parties to which you may transfer data and why
- Execute contracts – make sure all of your 3rd party contracts include data protection language and are clear about how 3rd parties must assist with compliance

Processes and Communication

- Review your existing compliance measures – are GDPR processes adaptable? How deal with rights to access and deletion? Opt out from "sale"?
- Communicate clearly – make sure your privacy notices are up-to-date and you provide at least 2 methods for consumers to contact you with requests or questions
- Review Data Retention Schedules
- Raise Internal Awareness

Be Aware of Shifting Landscape

- Watch for regulatory and legislative development– this is a moving target
- Watch for industry interpretations – many industries are creating guidelines for CCPA compliance; watch for those to understand how others in your industry are interpreting the law and future laws

RSAConference2020

Thank you!

Behnam Dayanim

bdayanim@paulhastings.com

1.202.551.1737

@bdayanim