

Tackling CPRA & Unique State Privacy Regulation Challenges

Brad Kelso – Managing Partner, Privageo

Usama Kahf – Partner, Fisher Phillips

Alyssa Coon – Privacy & Cyber Counsel, Axiom

Overview of Consumer Privacy Laws

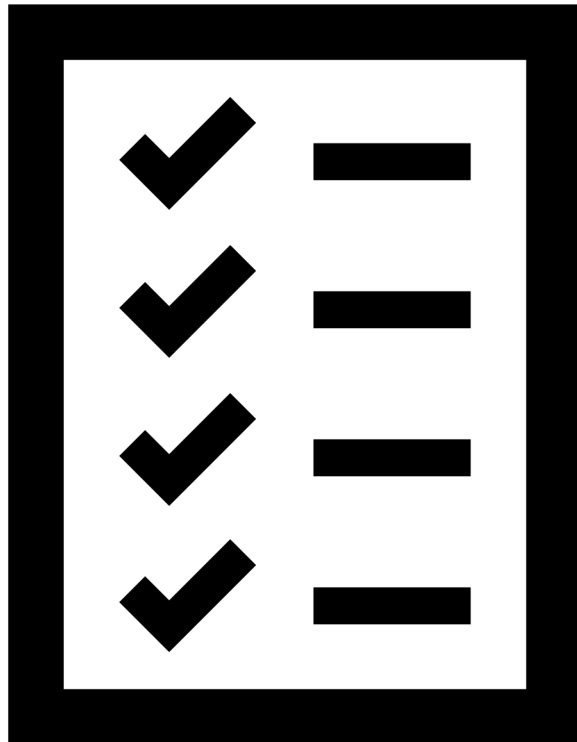


Usama Kahf

Partner, Fisher Phillips



Agenda



- Overview of consumer privacy laws
- Who are “consumers” under the law
- Challenges and complexities of HR data
- Compliance & data breach risks
- Current Requirements of California Consumer Rights Act (“CCPA”)
- New Obligations Under the California Privacy Rights Act (“CPRA”)

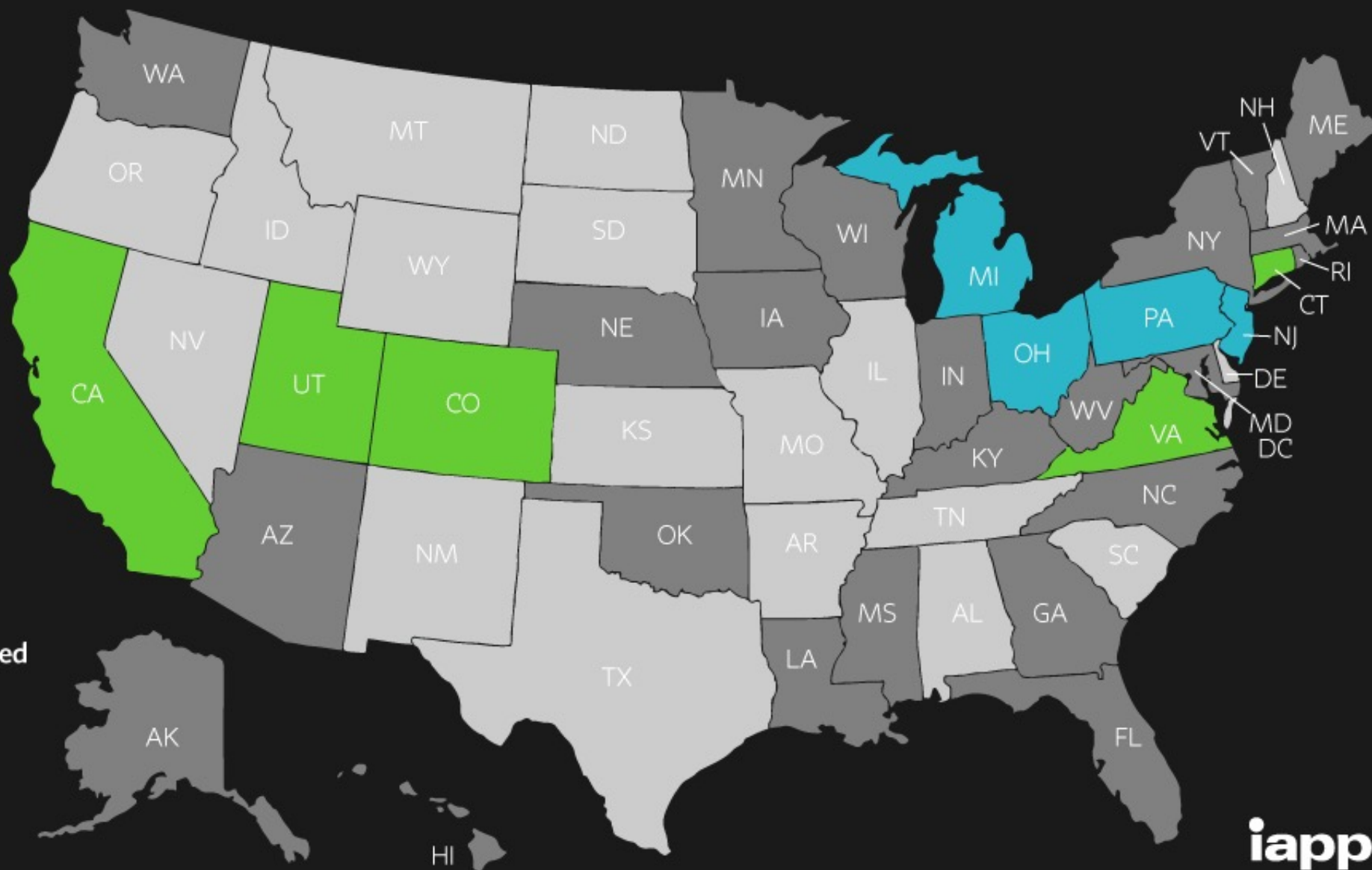
Overview of Consumer Privacy Law

1. Notice & Transparency – telling consumers what data is collected and how it will be used
2. Giving consumers some control over use, disclosure, and retention of their personal data
3. Imposing limits on collection, disclosure, use, sale, sharing, and retention of personal data

US State Privacy Legislation Tracker 2022

STATUTE/BILL IN LEGISLATIVE PROCESS

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



Last updated: 10/7/2022

New State Consumer Privacy Laws



Law	Date Effective
California Consumer Privacy Act of 2018 (CCPA)	January 1, 2020
California Privacy Rights Act of 2020 (CPRA or Prop 24) (Amends the CCPA)	January 1, 2023 (**some provisions already in effect)
Virginia Consumer Data Protection Act (VCDPA)	January 1, 2023
Colorado Privacy Act (CPA)	July 1, 2023
Connecticut Data Privacy Act (CDPA)	July 1, 2023
Utah Consumer Privacy Act (UCPA)	December 31, 2023

Important Dates for CCPA/CPRA

1/1/22

- CPRA has lookback that applies to PI collected by businesses on or after January 1, 2022

1/1/23

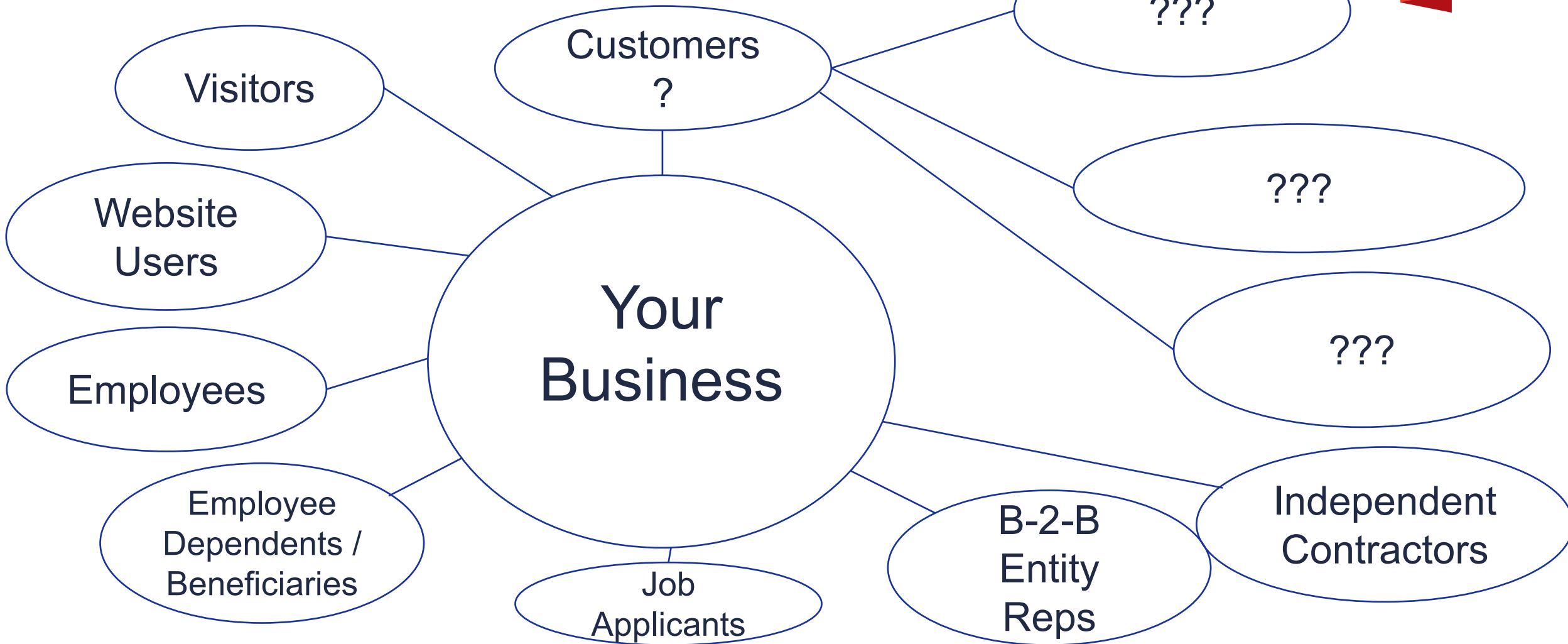
- CPRA amendments to CCPA become operative
- Employee/Applicant and B-2-B exemptions expire
- Data collected from employees and representatives of businesses are subject to all CCPA requirements

Who are “Consumers”?

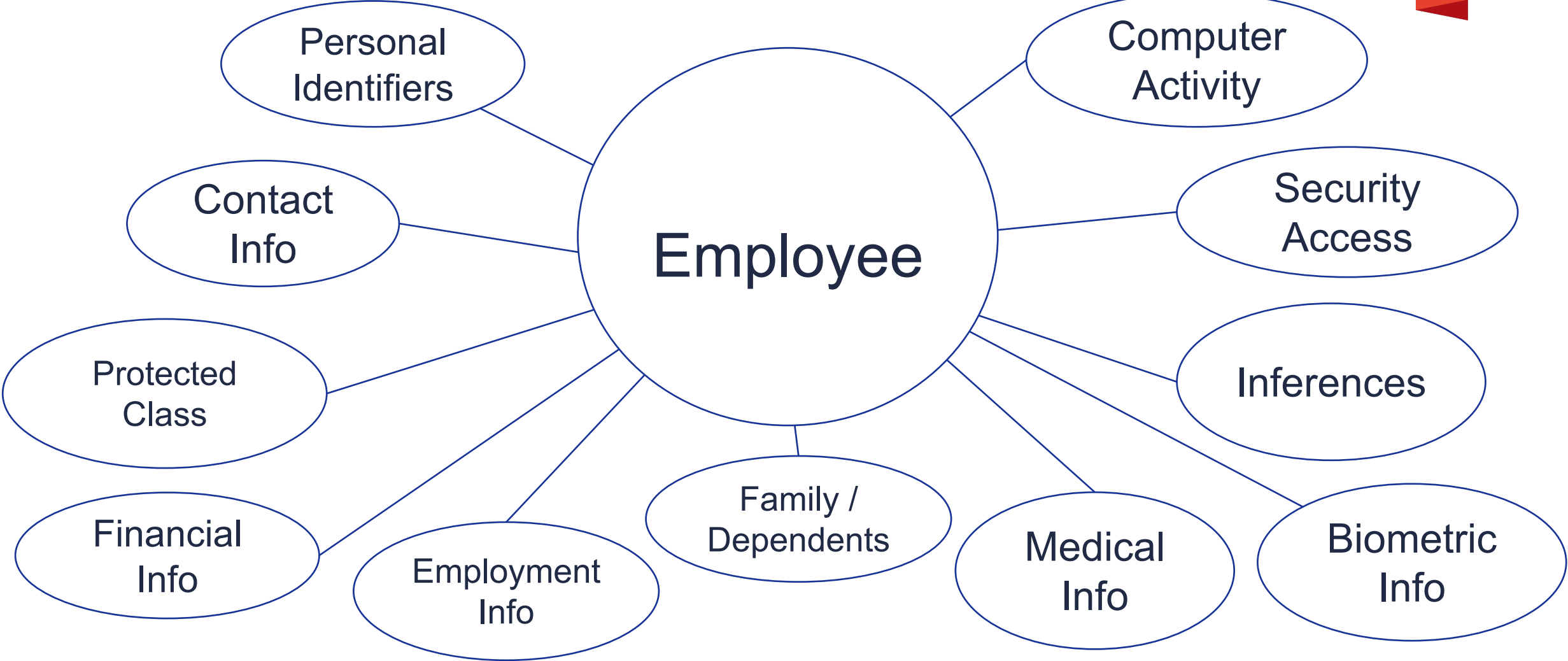


State	Definition	Includes EEs and Job Applicants?	Includes B2B?
California	Natural person who is a California resident	Yes	Yes
Colorado	Individual who is a Colorado resident	No	No
Connecticut	Individual who is a Connecticut resident	No	No
Virginia	Natural person who is a Virginia resident	No	No
Utah	Individual who is a Utah resident	No	No

Who Are Your Consumers?



Categories of Employee Data



CA – Consequence of Non-Compliance

- Consumers can file individual and class action lawsuits for data breaches under CCPA ➔ **\$100-750 per person per incident or actual damages, whichever is greater**
- Effective 1/1/23, CCPA prohibits retaliation against employees for exercising their rights under the CCPA.
- Starting 7/1/23, Cal. Privacy Protection Agency (CPPA) will begin enforcement (compliance deadline still 1/1/23) ➔ **penalties of \$2,500 per violation, or \$7,500 per intentional violation**
 - Authority to audit businesses to ensure compliance and investigate potential violations
 - Agency would have 5 years to bring an enforcement action

CCPA/CPRA Requirements 1/1/2023

1. Provide “**Notice at Collection**” to all California “Consumers” at or before point of collection
2. Online **Privacy Policy** and separate privacy policy for employees
3. Consumer request management process:
 - ✓ 2 methods for consumers to submit requests (toll-free number and electronic method)
 - ✓ 10 business days to acknowledge / 45 calendar days to respond (other deadlines may apply - 15 business days for deletion requests)

Consumer Request Rights as of 1/1/2023

1. Right to Know
2. Right to Access
3. Right of Deletion
4. Right to Opt-Out of Sale / Sharing of Personal Information
5. Right to Correct
6. Right to Limit Use or Disclosure of Sensitive Personal Information

CCPA/CPRA Requirements 1/1/2023

4. Implement **reasonable security measures** to protect personal data, including due diligence over vendors
5. New terms in contracts with all “**service providers**” and “**contractors**” as defined by CPRA
6. Data minimization
7. Training of employees who play any role in compliance with any of the CCPA requirements

Muscle Beach?

California Privacy Laws: **Executing to Meet Employment Requirements**



Brad Kelso
Co-Founder, Privageo



Employment Data is Different

1. Broad Uses of Employment-Related Data
2. Large Number of Data Sources
3. Employment Data is Often “Unstructured”
4. Frequent Data Sharing with or Collection By Service Providers
5. Employment Data is NOT Transactional
6. Unique Retention Obligations for Employee Data



The Value of a Complete Privacy Framework

1. Consumer Trust and Consent
2. Legal and Risk Management
3. Third Parties
4. Data Management
5. Data Protection
6. Leadership and Control
7. Communication and Training

Employees through a Privacy Lens?



“Reckless Rebels”
26%
Data Rich



“Savvy Digitals”
21%
Loyal Tech Adopters



“Conditional Consumerists”
19%
Fastest Growing



“Skeptical Protectionists”
23%
Skews ‘Boomer’



“Nervous Unawares”
13%
Low Smart Phone use

Forrester Technographics Study, 2021

Employees Themselves Are Different

- **CPRA is likely to usher in Privacy as a weapon**
 - Biggest Threat? (ask Europe)
- **Speaks to the CORE of your relationship**
 - Value
 - Security
 - Confidentiality - Access control
 - Health Sensitivity
- **Value to a privacy culture**
 - PS: They don't care that you use SaaS (should they?)

Is HR in the Security Business?

“In California... Yes”

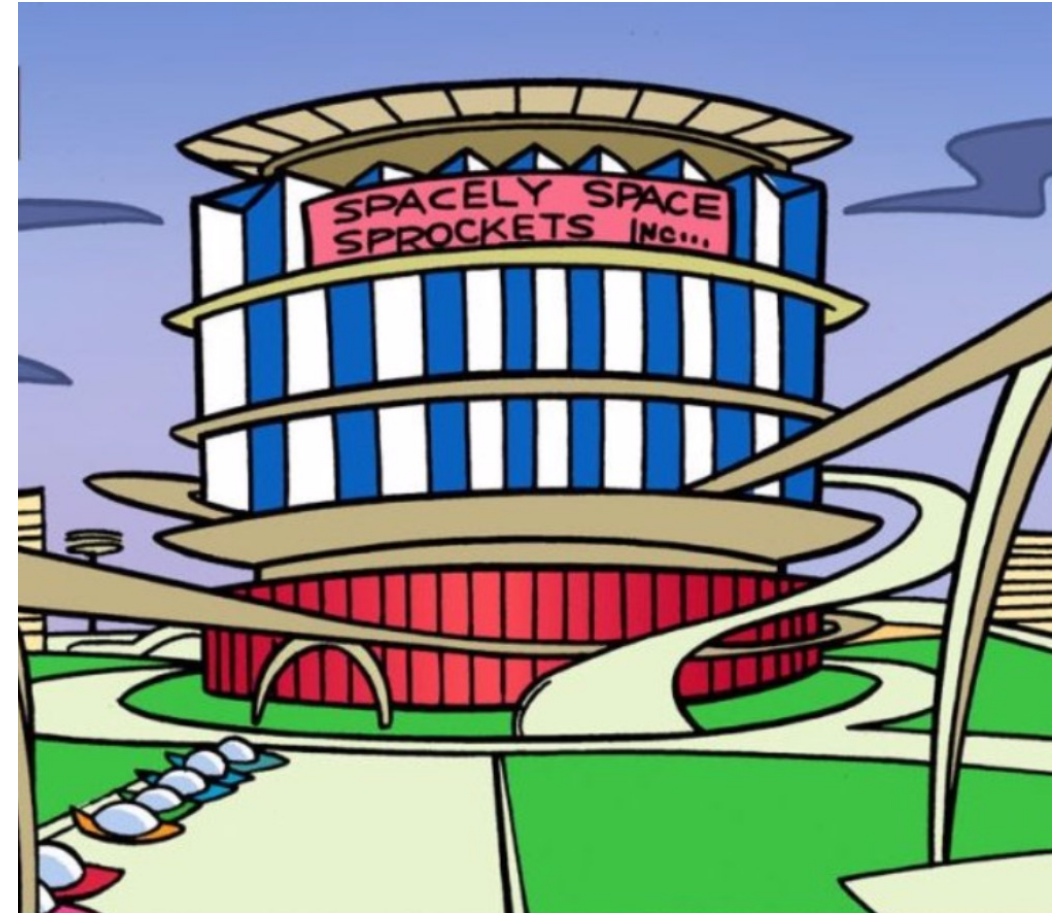
- Annual security assessment
- Data Retention P and P's

Scope:

- All employment systems:
 - Inventory Assets (hardware and endpoints)
 - Software (SaaS)
 - Data Stores
- Security Protections
- Data Governance
- Restoration

“Reasonable” Security Safeguards

- Matched to business
- CIS 18...Three Levels



From the Practitioner



Alyssa Coon
Privacy & Cyber Counsel
Axiom



Hiding from CCPA

Exemptions

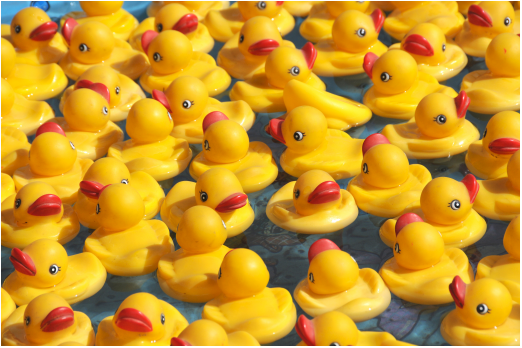
- Employees
- B2B
- GLBA
- HIPAA

Wait and see...

- Guidance from AG
- Guidance from CPPA
- Enforcement Activity
- Legislative action



Dancing the Data Map Mambo



Deploy various groups to identify the source, systems, third parties, and business purposes for the data

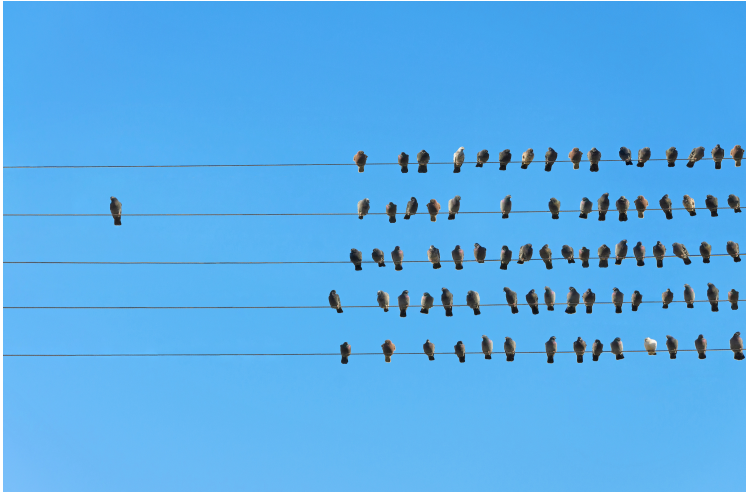


Create a response approach

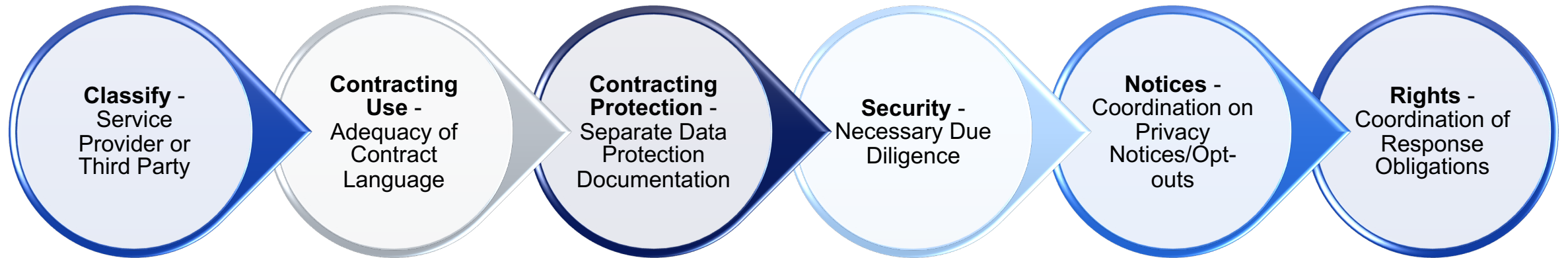
Find the data elements in the data



Organize information



Whoops... Third Parties?!



Communications 101

- Different notices for unique audiences
 - e.g., Employees, B2B, Customers
- Type/Timing of notices
 - e.g., layered, just in time
- Different response processes for unique audiences
 - e.g., Right to delete for all or some
- Communicating exemptions
 - e.g., GLBA, HIPAA
- Specifying rights based on different states
 - e.g., California, Colorado
- Determining the right level of detail for notices
 - e.g., Retention periods, categories of Third Parties



Final Thoughts



Managing Privacy in Uncertainty

- Issues still “Open”
- Closed Issues
- CPPA providing Latitude for Good Faith
 - What does “Good Faith” look like?