State Privacy Law Workshop

Tanya Madison, Olga Medina, Libbie Canter, and Jayne Ponder

November 8, 2023

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

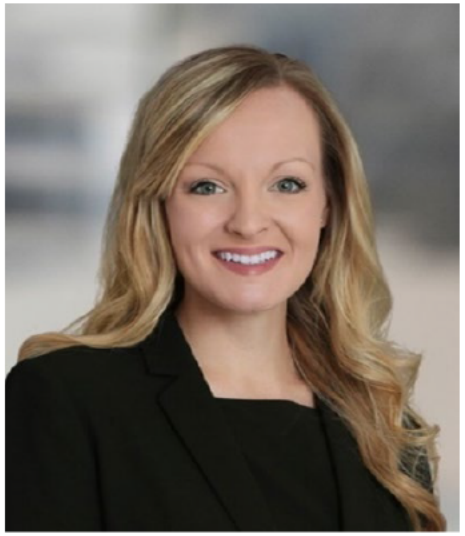
www.cov.com

Presenters

Libbie Canter
Covington & Burling LLP

Tanya Madison
Aristocrat Technologies

Olga Medina
BSA | The Software Alliance



Jayne Ponder
Covington & Burling LLP

Agenda

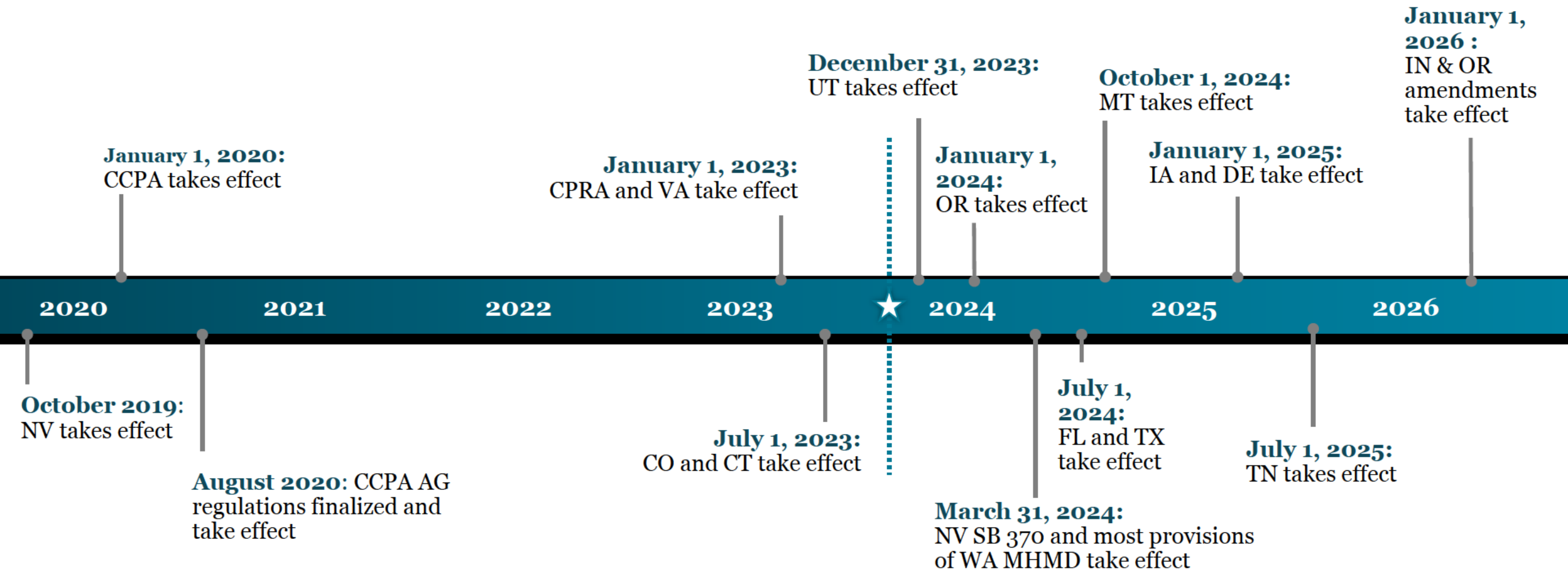
State Comprehensive Privacy Laws

State Privacy and Data Security Hot Topics

Part I

Comprehensive Privacy Laws

Timeline of State Privacy Activity



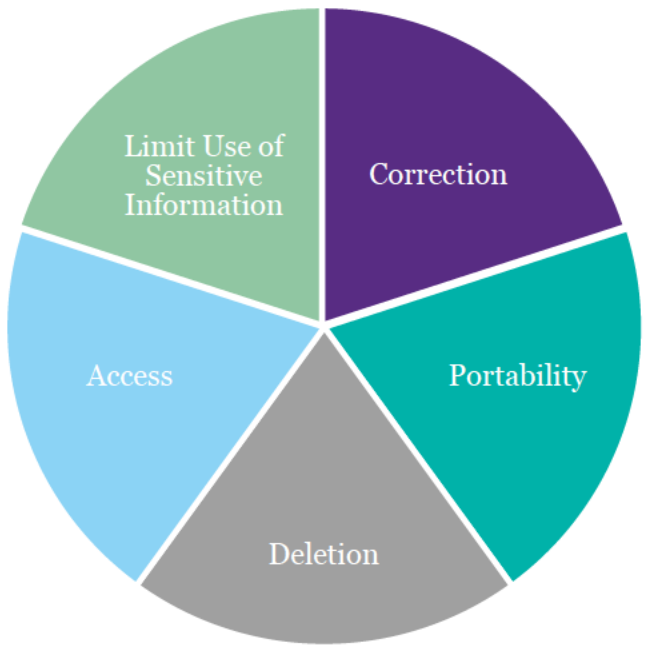
California

CCPA and CPRA

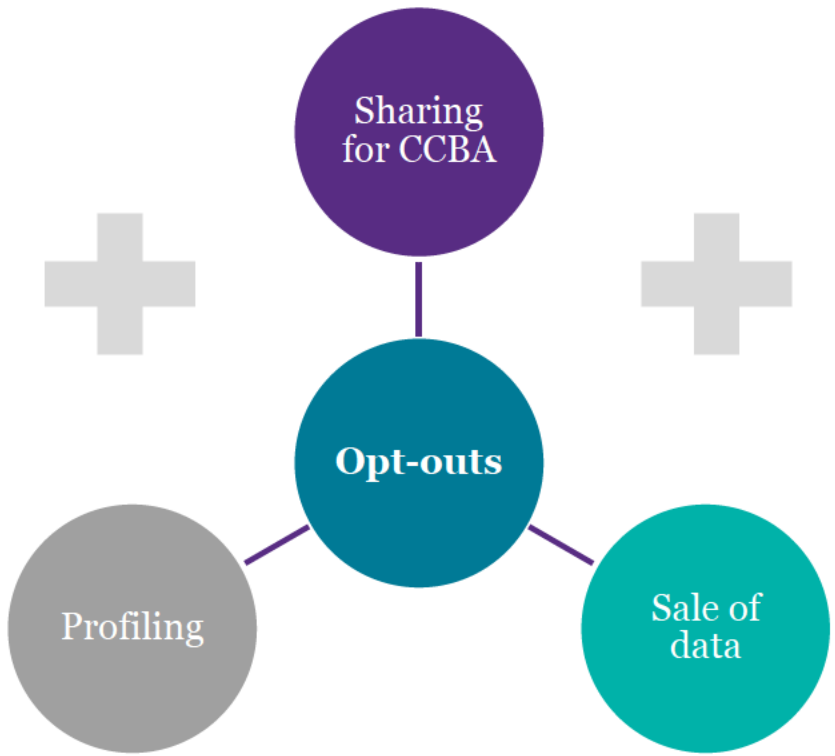
COVINGTON

CPRA Strengthens and Amends CCPA

Consumer Rights



New Opt Out Rights



Other Obligations

- Privacy Notices
- Discrimination/ Retaliation
- Minimization and Retention
- Service Providers and Contractor Terms
- Terms For Third Parties for Sale or Sharing
- Reasonable Security Procedures and Practices
- Data Protection Assessments
- Cyber Audits

What's Next for the CCPA?

Rulemaking:

- Dark patterns
- Correction requests
- Opt-out preference signals
- Rights to limit
- Privacy notice requirements
- Service provider obligations
- Automated decision-making access and opt-out rights*
- Risk assessments*
- Cyber security audits*

* *Pre-rulemaking on new topics*

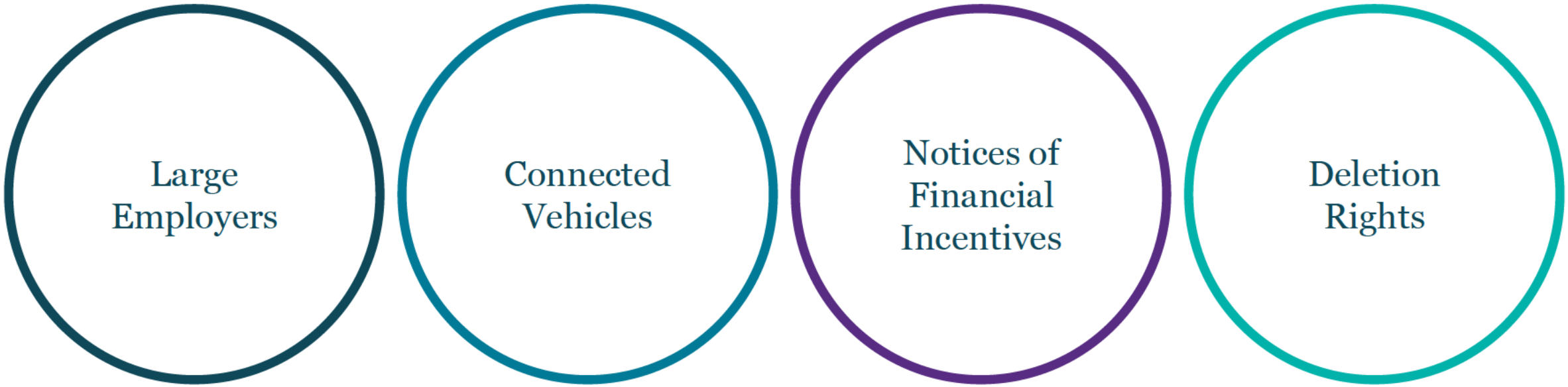
CalChamber Litigation

- California Chamber of Commerce sued to delay CCPA rules enforcement
- Court held that rules could not be enforced for a year
- CPPA and State AG appealed

Expiration of employee and B2B exemptions

- Partial exemptions had been extended until Jan. 1, 2023
- Legislative efforts to further extend failed
- Initial draft rules had one provision that specifically referenced employee data, but that was removed

Ongoing CCPA Enforcement: Areas of Priority



Sephora to pay $1.2 mln in privacy settlement with Calif. AG over data sales

CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies

News: July 31, 2023

Other State Comprehensive Privacy Approaches

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia

COVINGTON

Three Categories of State Privacy Laws

"Fewer Substantive Obligations"

- Utah
- Iowa

"Baseline Approach"

- Virginia
- Indiana
- Tennessee
- Florida
- Texas

"More Substantive Obligations"

- Colorado
- Connecticut
- Montana
- Delaware
- Oregon

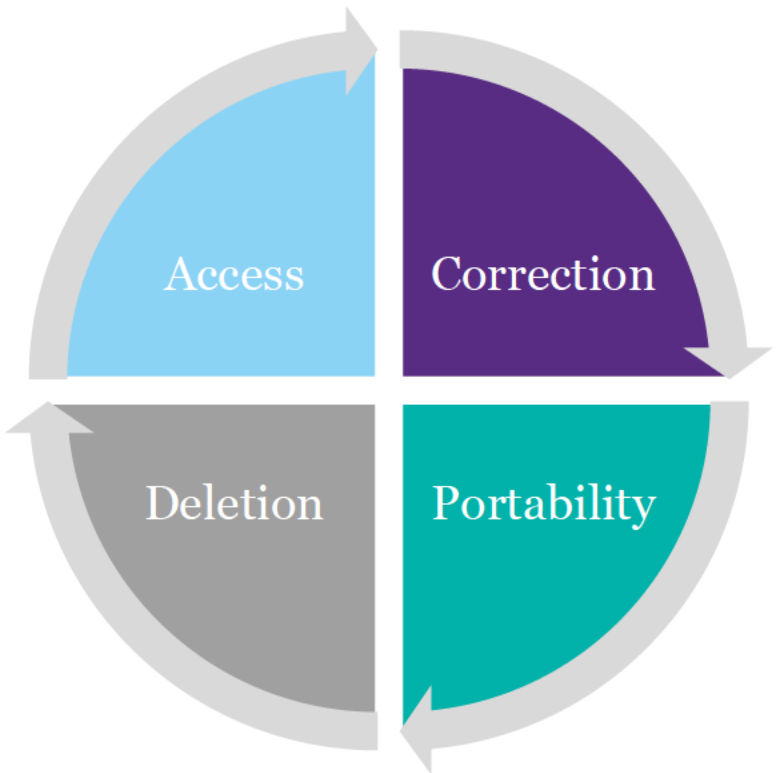
“Baseline Approach”

Virginia, Indiana, Tennessee, Florida, and Texas

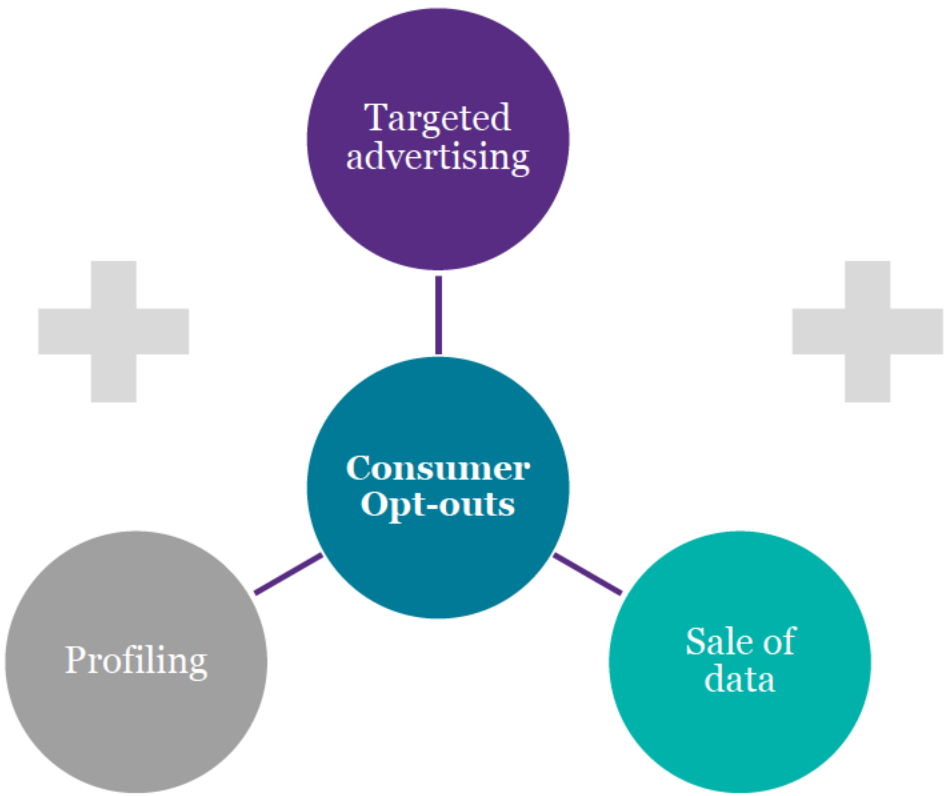
COVINGTON

“Baseline”: Virginia, Indiana, Tennessee, Texas, and Florida

GDPR/CCPA-like rights



CPRA-like rights



Opt-in for sensitive personal information

“Baseline”: Virginia, Indiana, Tennessee, Texas, and Florida

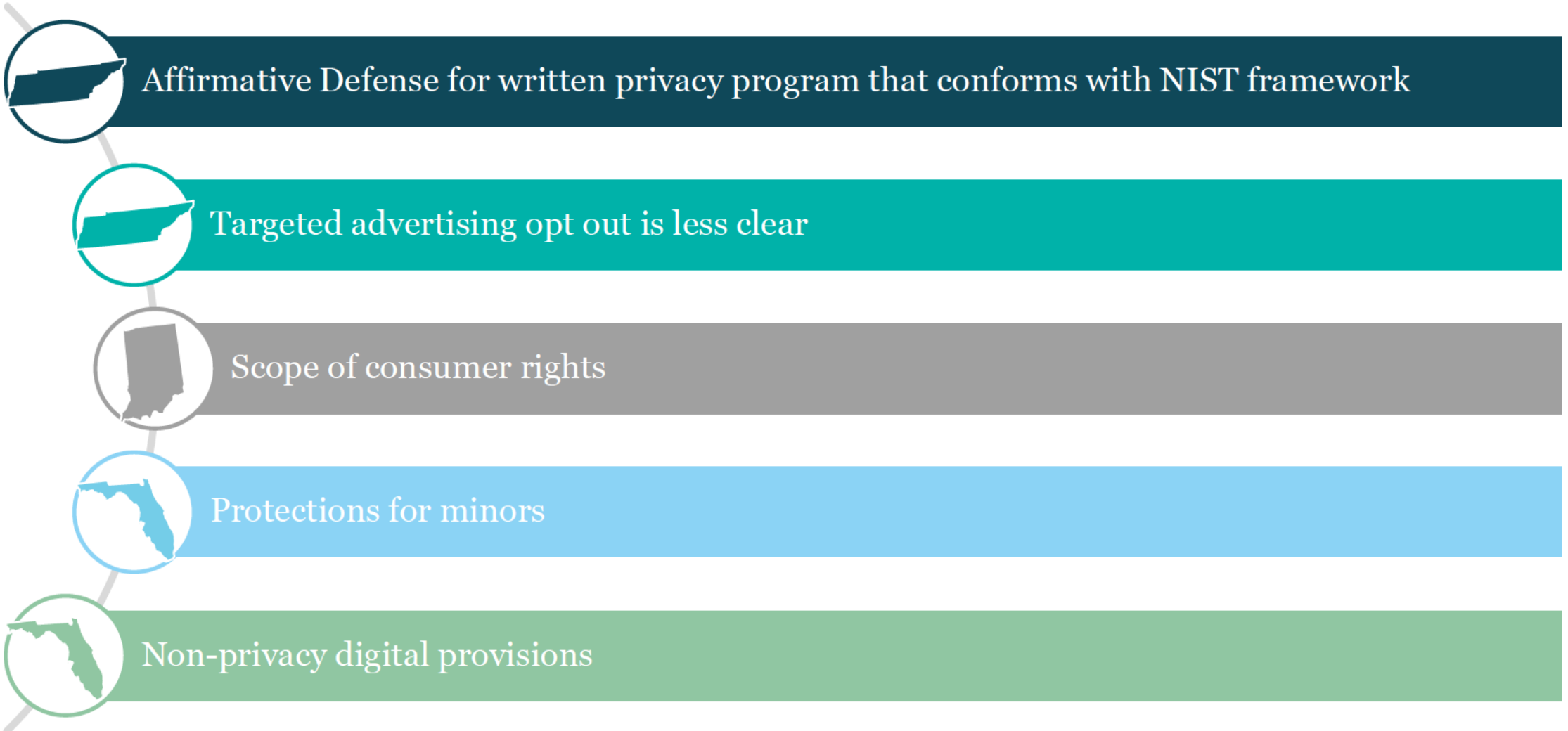
Controller Obligations

- Data Minimization
- Purpose Specification
- Consent: Sensitive Data + Unexpected Uses
- Reasonable Security Measures
- Data Protection Assessments for Specific Activities
- Prohibition on Retaliation
- Prohibition on Discrimination

Processor Obligations

- Contract Required
- Data Security Obligations
- Subcontractor Requirements
- Assist with Consumer Rights Requests
- Duty of Confidentiality
- Delete or Return Data at End of Services
- Reasonable Assessments

Key Differences: "Baseline Approach" Laws



Fewer Substantive Obligations

Utah and Iowa
Nevada

COVINGTON

Fewer Substantive Obligations: Utah and Iowa

Key Differences from "Baseline" Approach

- No correction right
- Deletion right covers only personal information provided by the consumer, and not all data the controller has obtained
- No right to opt-out of "profiling"
- Right to opt-out of processing sensitive data
- No DPIAs
- Some differences in required contract terms
- For Iowa, right to opt out of targeted advertising is less clear
- For Oregon, consumers have right to list of specific third parties to which data has been disclosed

Nevada Approach (NPICICA)

Scope

- As initially drafted, applied only to operators of Internet websites and online services
- As of October 2021, applies certain requirements to "data brokers"

Sale

- Narrower opt out right (requires monetary consideration; narrow scope of information)
- No opt-in requirements, regardless of age
- Opt-out requests can be processed by email, telephone, or website

DSRs

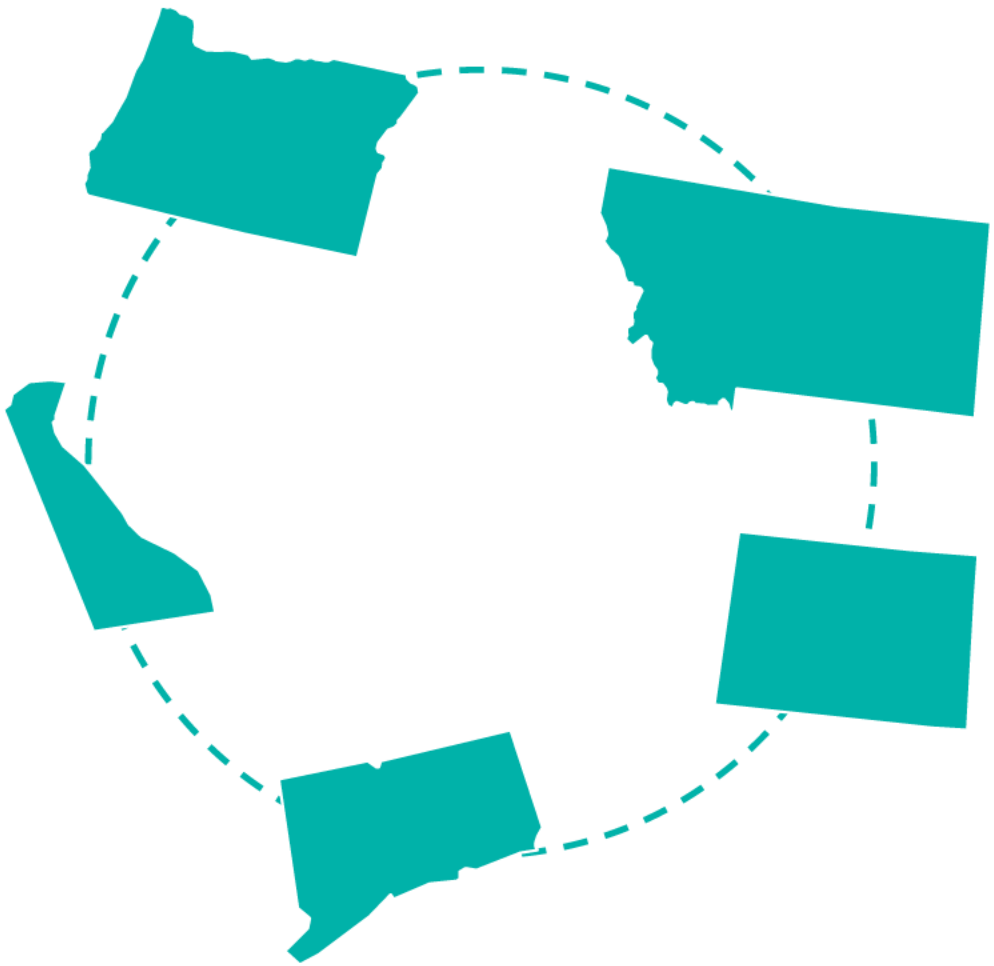
- No right to access, data portability, deletion, or non-discrimination

More Substantive Obligations

Colorado, Connecticut, Montana Delaware, and Oregon

COVINGTON

More Substantive Obligations: CO, CT, MT, DE, OR



Key Differences from "Baseline" Approach

- Sale defined more broadly, as an exchange for monetary or *other valuable consideration*
- Requirement that controllers permit consumers to exercise their opt-out rights through a universal opt-out mechanism
- More detailed specifications that consent cannot be obtained through acceptance of terms of service or through dark patterns; right to revoke consent through mechanism "as easy" as mechanism used for consent
- More formal audit rights for controllers
- Additional requirements and restrictions for 13-16 year olds

Colorado Rulemaking Process

Regulations

- Required Universal Opt-Out*
- Dark Patterns
- Opt-in Consent Incompatible Uses
- Notice & Opt-out for Profiling
- Loyalty Program Disclosures
- Risk Assessment Requirements
- Sensitive Data Inferences
- Prescriptive Privacy Notice Requirements

Process

- October 2022 First Draft of Proposed Rules
- November 2022 – February 2023 Comment Period
- March 2023 Final Rules Published

Key Trends in State Privacy Laws

COVINGTON

Overview of Key State Proposals

Category	Topic	CA	VA/IN/TN/FL/TX	CO/CT/MT/DE/OR	UT/IA
Notice	At or before point of collection	✓			
	In a reasonably accessible privacy notice	✓	✓	✓	✓
Opt-Outs	Sale	✓	✓ (In some cases, narrower sale definition)	✓	✓ (Narrow Sale Definition)
	Targeted Advertising / Cross-Context Behavioral Advertising	✓	✓*	✓	✓*
	Profiling	Rulemaking	✓	✓	
Sensitive Data	Consent to Process	Opt-out	✓	✓	Opt-out

* Even though right to opt-out is not an enumerated consumer right in TN and IA, controllers must disclose to consumers how they may opt-out.

Overview of Key State Proposals (Continued)

Category	Topic	CA	VA/IN/TN/FL/TX	CO/CT/MT/DE/OR	UT/IA
Consumer Rights	Access, Deletion, Portability, Correction, Non-Discrimination	✓	✓	✓	✓ No Correction
Business Obligations	Data Minimization	✓	✓	✓	
	Impact Analysis	To be addressed by AG	✓	✓	
	Fiduciary Duty				
Enforcement	Dedicated Data Privacy Protection Agency	✓			
	Private Right of Action	✓			
	AG Enforcement; Fine/Civil Penalty	✓	✓	✓	✓
	Mandatory Cure Period That Has Not Yet Expired		✓	✓	✓

Looking Ahead:

State Comprehensive Privacy Laws & Trends

COVINGTON

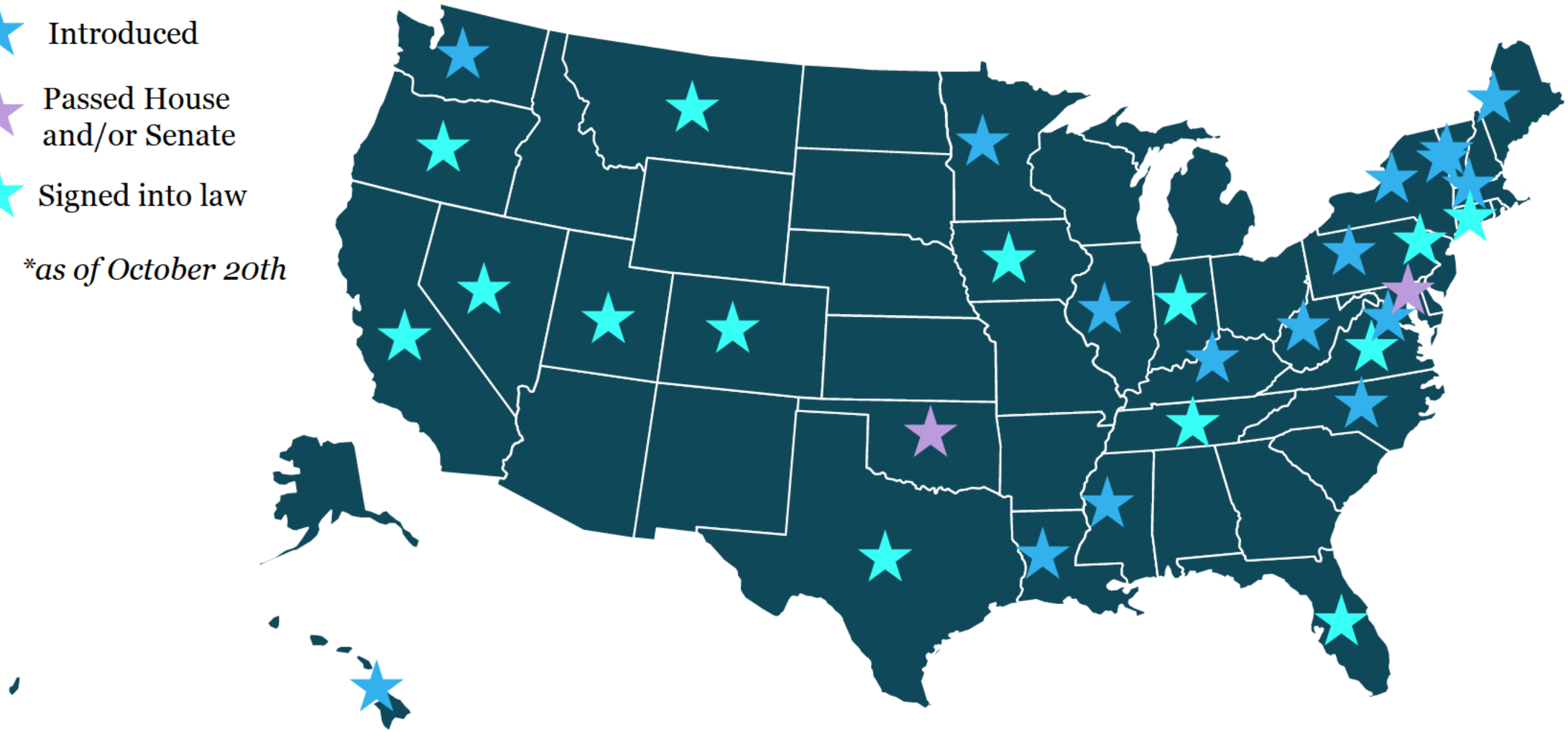
2023 State Comprehensive Privacy Proposals

Introduced

Passed House and/or Senate

Signed into law

**as of October 20th*



Legislative Sessions Adjourning in 2023

Timeline	
November 2023	Massachusetts
December 2023	Michigan, New Jersey, Ohio, Pennsylvania, Wisconsin

California Model or Virginia Model

California Model

- Businesses & Service Providers
- Individual Rights
- Opt Out of Sale/Sharing
- Limitation For Sensitive Data Use & Disclosure
- Obligations for Service Providers
- Potential Requirements for Assessments or Profiling

Virginia Model (or Variation)

- Controllers & Processors
- Individual Rights
- Opt Out of Sale, Targeted Advertising, Profiling
- Consent For Sensitive & Unexpected Uses
- Obligations on Data Processors
- Assessments

Novel Approaches

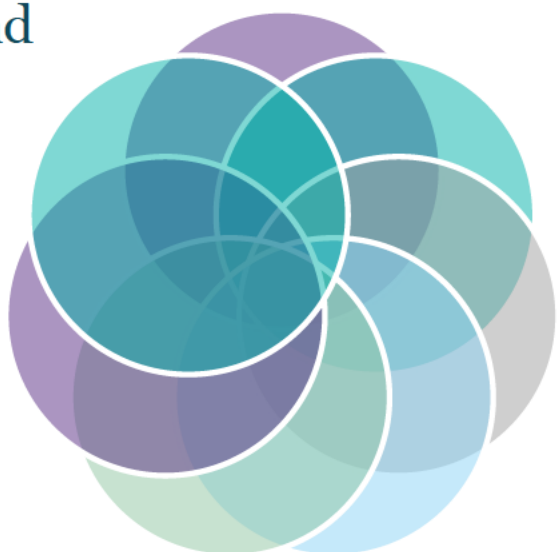
- Focus on Consumer Health Data
- Focus on Data Broker Registration
- ULC Model
- Duty of Loyalty
- Opt-in for Processing
- Expanded Access Rights
- Opt-in Consent for Collection of Location or Biometric Information
- Opt-in Consent for ADM

Key Battleground Issues

Enforcement and Cure Periods

Duties of Care and Loyalty

Personal Information



Data Minimization

Controller / Processor Distinctions

Rights and Obligations

Employee & B2B Exemptions

Federal Interplay

COVINGTON

Federal Developments

American Data Privacy Protection Act

- Data Minimization Requirements & Purpose Limitations
- Consumer Rights
- Algorithmic Assessments
- Preemption with Exceptions
- Enforcement by FTC, AGs, and Private Actors

FTC Rulemaking Privacy, Security, Algorithmic Decision-Making

- Notice and Consent
- Children & Teens
- Algorithmic Error & Discrimination
- Reasonable Security Program

Children & Teens

- FTC Workshop on Kids Advertising
- COPPA Rulemaking and Enforcement
- Dark Patterns
- Legislative Proposals
  - Kids Online Safety Act
  - COPPA 2.0

Part II

Hot Topics in Privacy

Children & Teens: Age Appropriate Design Code

Prohibitions

- Using children's personal information for ways the business knows or has reason to know "is materially detrimental" to the health or well-being of the child
- Default precise geolocation collection, selling, or sharing
- Dark Patterns
- Certain Profiling

Data Protection Impact Assessments

- Harm to Children
- Algorithms
- Targeted Advertising
- System Design Features to Increase Time Used
- Sensitive Personal Information

INTRODUCED

Illinois, Minnesota, Nevada, New Jersey, New York, Texas, South Carolina

Children & Teens: Social Media Laws

Common Requirements

- Age verification
- Parental consent for users under 18
- Restrict access for users under 18

PASSED

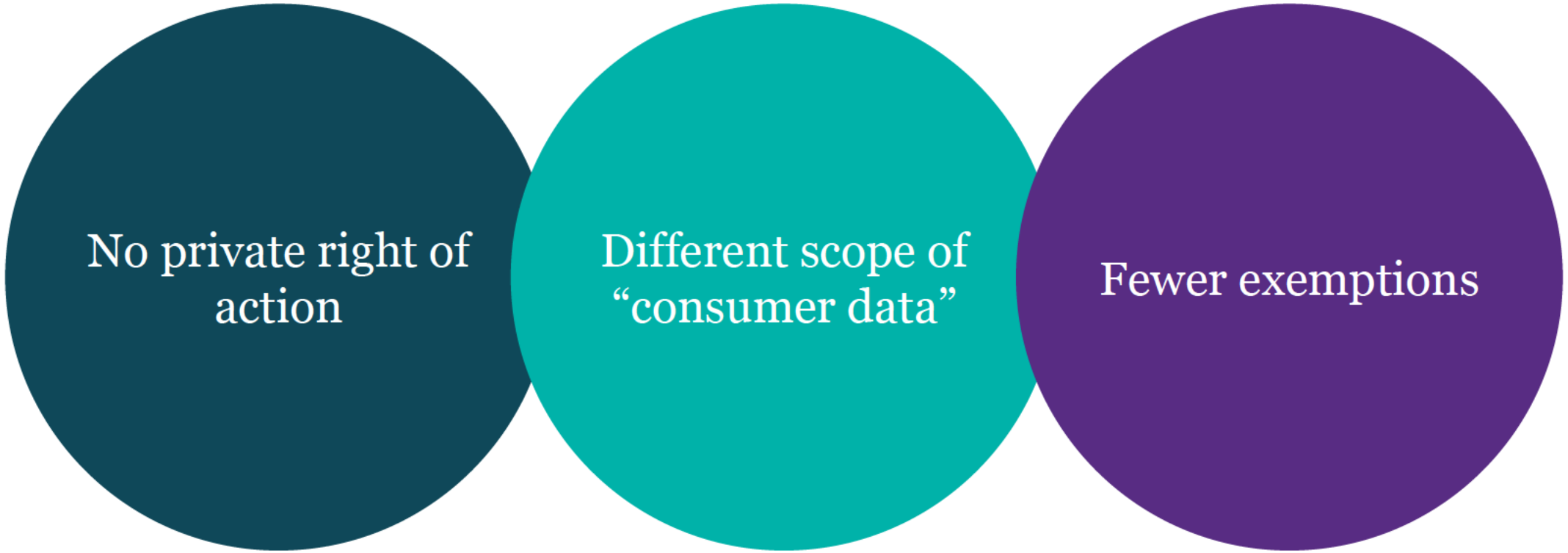
INTRODUCED

Iowa, Massachusetts, New Jersey

Washington – My Health My Data Act (HB 1155)

Scope	Applies to "regulated entities" and governs "consumer health data"
Consumer Rights	(1) access; (2) withdraw consent from the collection and sharing of their health data; and (3) deletion
Key Obligations	▪ Maintain and publish a privacy policy for consumers' health data; ▪ Requiring consent to collect and share consumers' health data; ▪ Prohibit the selling of consumers' health data absent valid authorization; ▪ Stop geofencing around health care facilities.
Exemptions	PHI under HIPAA, Part 2 information, certain research information, HIPAA de-identified information, among others
Enforcement	Attorney General and private right of action

Nevada SB 370 and Connecticut SB3: Differences from WA



Genetic Testing

State Legislative Trends

- Trend in favor of genetic privacy laws with **explicit consent requirements** and **stricter penalties**
- Increased regulation of **"direct-to-consumer"** genetic testing companies

Data Broker Laws & Proposals

California: AB 1202 (Enacted)

- Applies to handling of "Personal Information"
- Annual registration with AG
- Discretionary disclosures

California: DELETE Act (Enacted)

- Registration with the FTC
- Allows Californians to direct all data brokers to delete their personal information
- Audit, record maintenance, and fee requirements

Vermont: H 764 (Enacted)

- Applies to handling of "Personal Information"
- Annual registration with AG
- Mandatory disclosures
- Information security program

Oregon: HB 2052 (Enacted)

- Annual registration with the Department of Consumer and Business Services
- Mandatory disclosures

Texas: SB 2105 (Enacted)

- Applies to processing or transfer of "Personal Data"
- Annual registration with Secretary of State
- Mandatory disclosures
- Information security program

Biometric Privacy Requirements

Requirements of Illinois BIPA (Illustrative of Other Laws)

- Regulates "biometric identifiers" and "biometric information"
- Publicly Posted Retention Policy
- Notice
- Written Consent

Biometric Lawsuits Abound

Court rulings supercharge Illinois' strongest-in-nation biometric privacy law

WSIU Public Broadcasting | By Hannah Meisel | Capitol News Illinois
Published February 28, 2023 at 4:55 PM CST

Justices Say BIPA Claims Accrue With Each Scan

Microsoft, Amazon granted summary judgement in biometric data privacy lawsuits

First Jury Verdict Issued in Illinois Biometric Privacy Act Class Action

Thursday, October 20, 2022

BNSF Railway will settle biometric privacy case, after $228 mln verdict wiped out

By Mike Scarcella
September 18, 2023 4:28 PM EDT · Updated a month ago

Facial Recognition Technology

Restrictions on Use

- Citywide restrictions on **private use** or **government use**
  - Restrictions on municipal use and private use on public property
- Statewide restrictions on **law enforcement** use of facial recognition technology

Automated Decision-Making & Profiling

ADM Requirements in Comprehensive Privacy Statutes

- Profiling Opt-Outs (e.g., CO, CT)
- Heightened Requirements for ADM / AI Training and Use (CCPA Regulations)

Use of ADM in Certain Contexts

- Insurance (CO, NJ)
- Employment (NYC, IL, MD, MA)
- Generative AI (MA)
- Important Life Decisions (HI)

Prohibition on Discrimination

- CA, DC, NJ

Required Impact Assessments for Consequential Harm

- MA, ME

Employee Privacy Laws

New Jersey (Enacted)

- Prohibits employers from using tracking devices in vehicles operated by employees without providing notice
- Up to $2,500 per violation

New York (Enacted)

- Requires private sector employers to provide notice of electronic monitoring practices to employees

Connecticut (Enacted)

- Requires employers to provide notice of electronic monitoring practices to employees
- Prohibits employers from using electronic surveillance to monitor employees in specified work areas

California (Not enacted)

- Would have regulated employers use of employee data
- Afforded CCPA-like rights to employers
- Included a private right of action

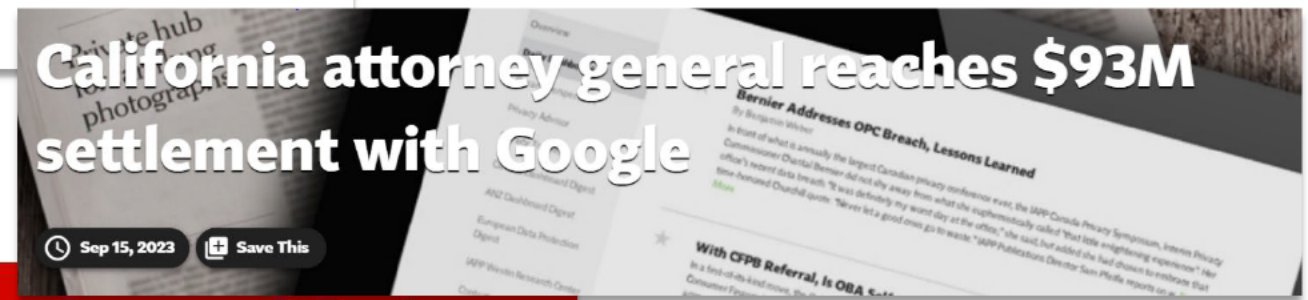
Privacy Enforcement by State Attorneys General

WESTLAW NEWS SEPTEMBER 17, 2020 / 6:07 PM / UPDATED A YEAR AGO

Calif. AG calls settlement with fertility app provider Glow a 'wake up call' for data privacy

Google Cannot Escape Location Privacy Lawsuit in Arizona, Judge Rules

Attorney General Formella Announces Multistate Settlement with Google Over Deceptive Location Tracking Practices

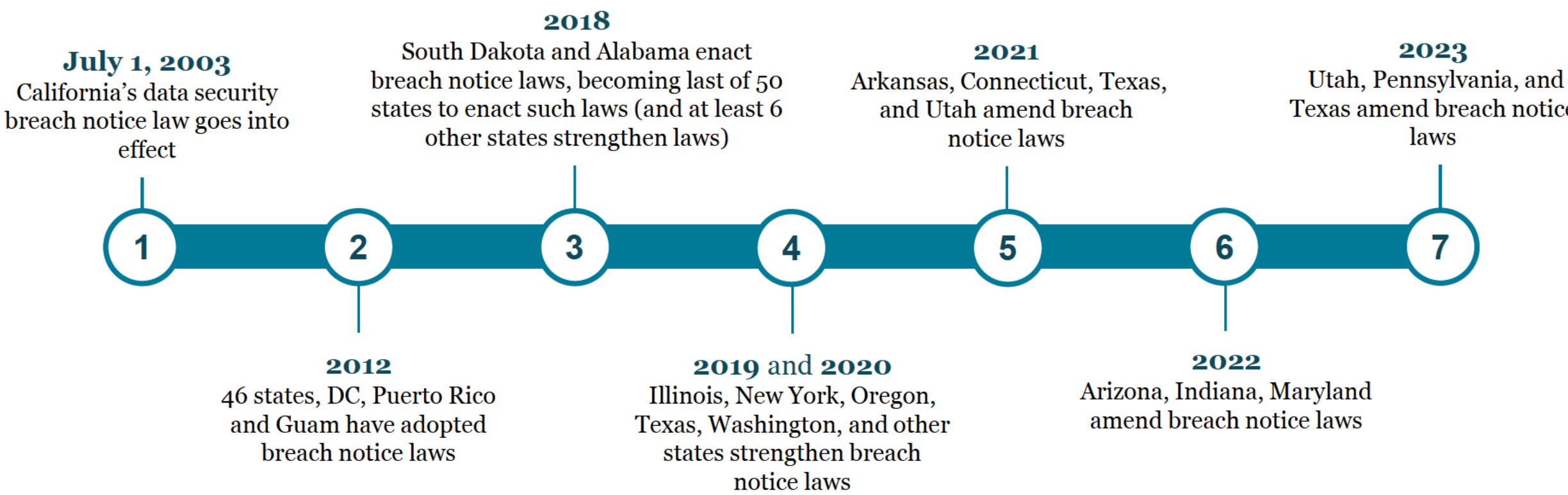


Feb 7, 2023

New York attorney general enters settlement with 'stalkerware' seller

Anthem Inc. Settles State Attorneys General Data Breach Investigations and Pays $48.2 Million in Penalties

State Data Breach Laws



Internet of Things

California

- Requires manufacturers of "connected devices" to equip the device with "a reasonable security feature or features"
- Features should be:
  - appropriate to the nature and function of the device
  - appropriate to the information it may collect, contain, or transmit
  - designed to protect the device and its information from unauthorized access, destruction, use, modification, or disclosure
- Effective January 1, 2020

Oregon

- Requires manufacturers of "connected devices" to equip the device with "reasonable security features" (defined similar to Cal.)
- "Connected device" limited to Internet-connected devices:
  - used primarily for personal, family or household purposes; and
  - that is assigned IP address or another device or address that identifies device for purpose of short-range wireless connections to other devices.
- Effective January 1, 2020

Future Proofing Your Privacy Program

COVINGTON

Future Proofing Your Privacy Programs

What to expect:

- Legislative, regulatory, and enforcement activity
- Additional consumer rights, e.g., correction, profiling
- Additional protections for sensitive personal data

Questions?