State Privacy Law Workshop

Libbie Canter, Tanya Madison, and Olga Medina

May 10, 2023

COVINGTON

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

www.cov.com

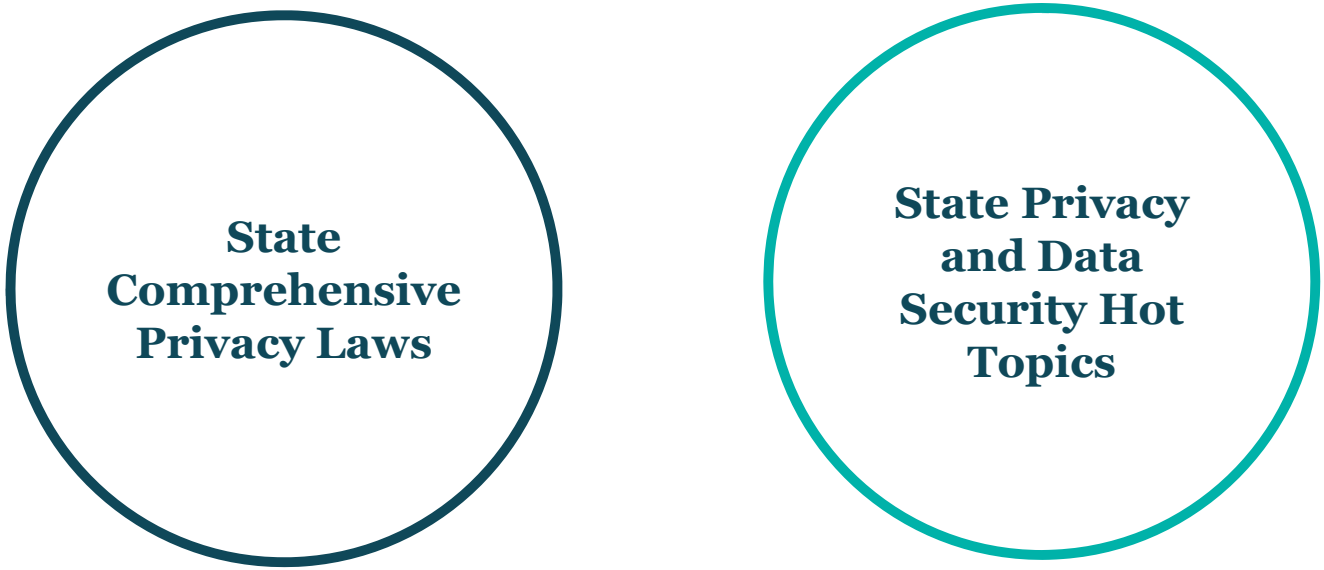
Presenters

Libbie Canter
Covington & Burling LLP

Tanya Madison
Aristocrat Technologies

Olga Medina
BSA | The Software Alliance

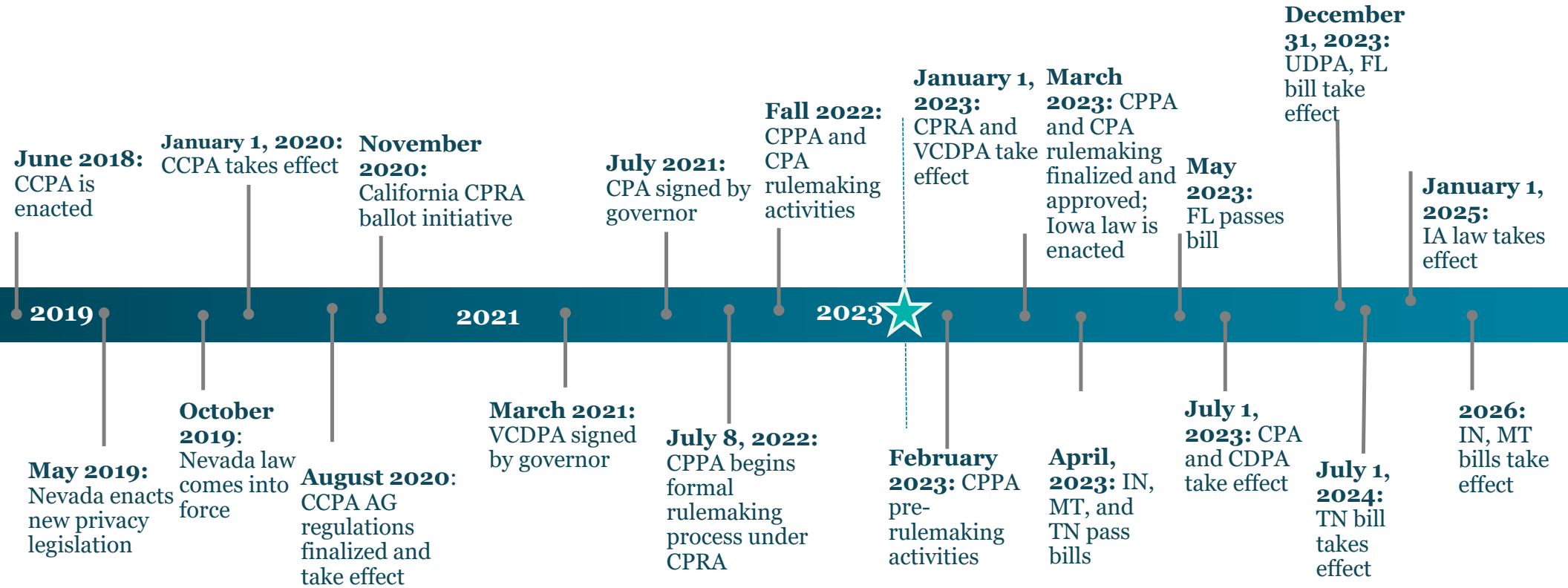
Agenda


State Comprehensive Privacy Laws
State Privacy and Data Security Hot Topics

Part I

Comprehensive Privacy Laws

Timeline of Activity

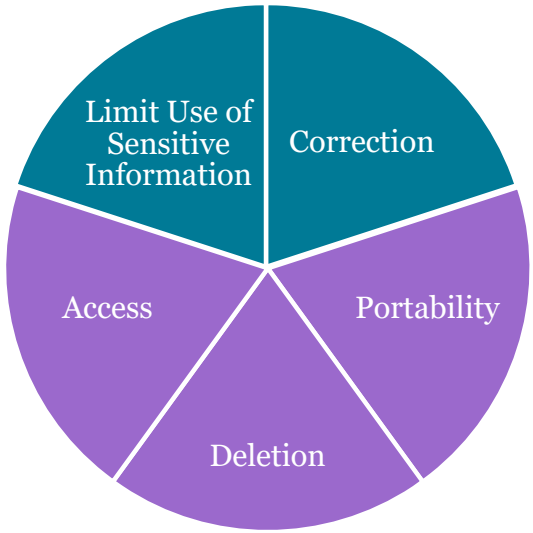


Enacted Laws: California

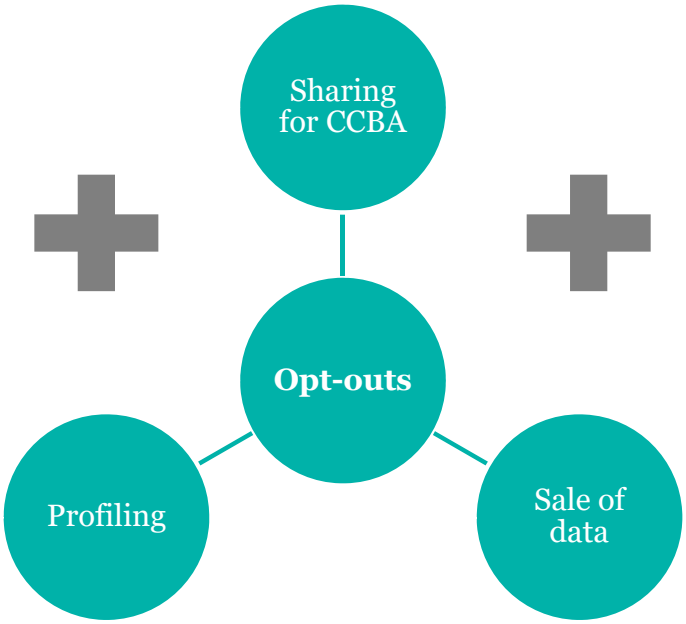
CCPA and CPRA

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?

Initial wave of rulemaking was finalized on March 30, 2023 and it addresses a number of key topics:

- Consent to process PI for secondary, incompatible processing
- Dark patterns
- Correction requests
- Opt-out preference signals
- Rights to limit
- Privacy notice requirements
- Service provider obligations

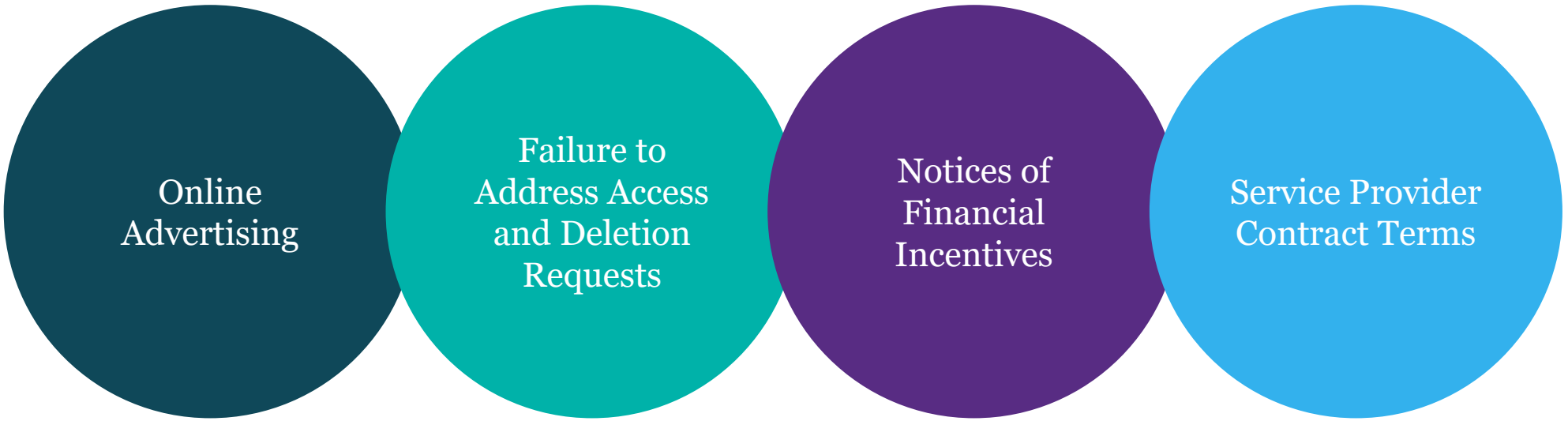
Agency has commenced pre-rulemaking activities for new rules in additional areas, including:

- Automated decision-making access and opt-out rights
- Risk assessments
- Cyber security audits

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



Enacted Laws: Nevada

Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA)

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

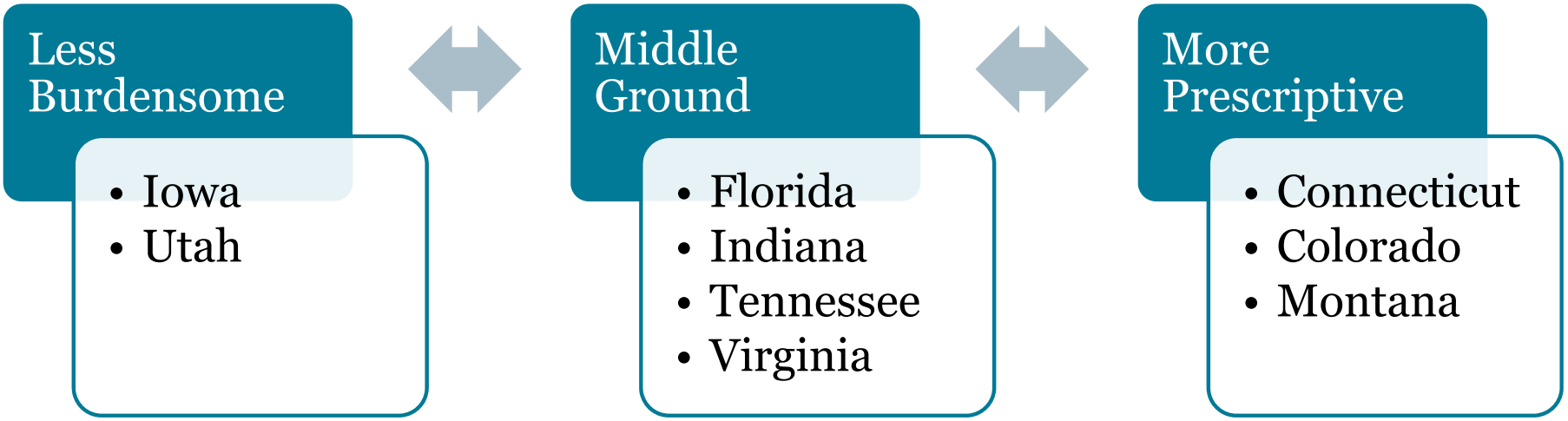
DSRs

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

Other State Approaches

Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Utah, and Virginia

Three "Buckets"

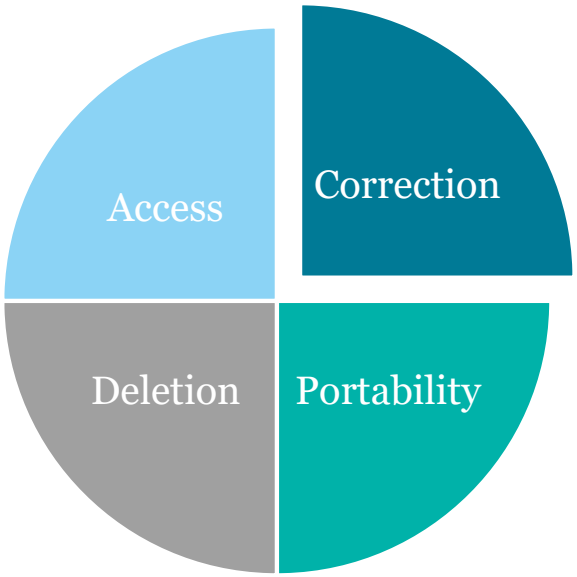


Middle Ground

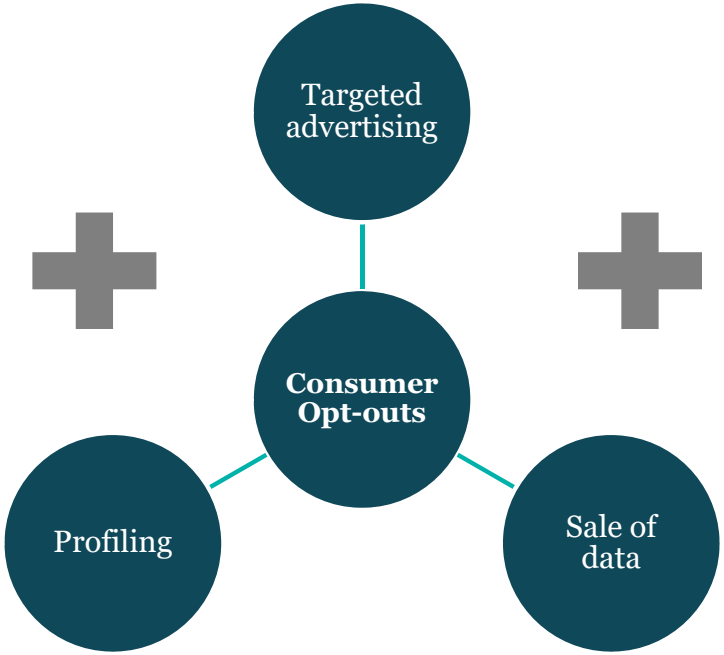
Florida, Indiana, Tennessee, and Virginia

Virginia, Indiana, Tennessee, and Florida

GDPR/CCPA-like rights



CPRA-like rights



Opt-in for sensitive personal information

Florida, Indiana, Tennessee, and Virginia

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

Differences

- Tennessee: Written privacy program that conforms with NIST framework; targeted advertising opt out is less clear
- Indiana: Scope of consumer rights
- Florida: When it applies, protections for minors, and non-privacy digital provisions

Less Burdensome

Iowa and Utah

Iowa and Utah

Similarities to VA	Differences from VA
• GDPR/CCPA-like rights: access, deletion, and portability • CPRA-like rights: opt-out rights to sale and processing for targeted advertising • Exemptions, including B2B and employee data • Definition of "sale" is for monetary consideration only (although note that prior category of states diverge on this issue) • No express private right of action • Cure period that does not sunset, although length of cure period varies	• No correction right • Deletion right covers only personal information provided by the consumer, and not all data the controller has obtained about the consumer • No right to opt-out of "profiling" • Right to opt-out of processing sensitive data • In the case of Iowa only, the right to opt out of targeted advertising is not listed under the required "consumer rights," although controllers must disclose the manner in which a consumer may opt out • No data protection impact assessments • Some differences in required contract terms

More Prescriptive

Colorado, Connecticut, and Montana

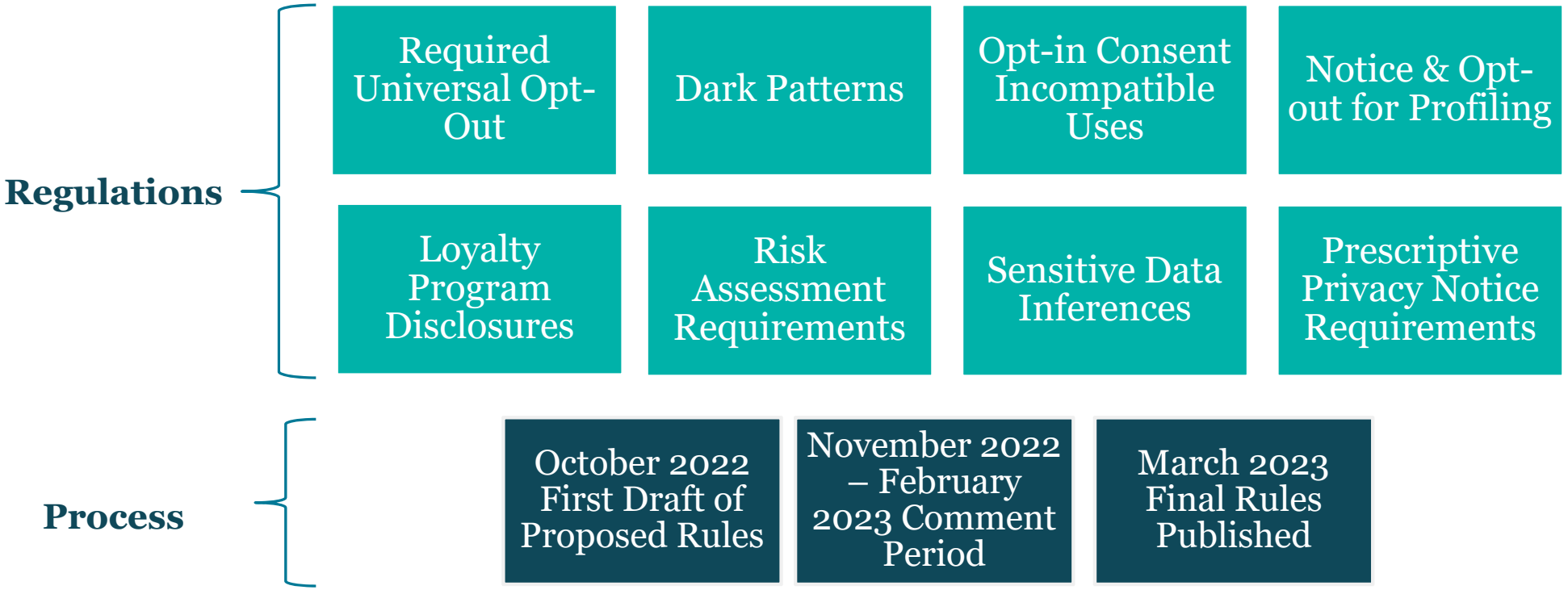
Colorado, Connecticut, and Montana

Similarities to VA	Differences from VA
• GDPR/CCPA-like rights: access, portability, correction, and deletion • CPRA-like rights: opt-out rights for sale, targeted advertising processing for purposes of targeted advertising and profiling • Exemptions, including B2B and employee data • Requirement to opt-in for sensitive data • Creation of an appeals process • Required data protection assessments • Comparable processor contract obligations • No express private right of action • Cure period, although mandatory cure period expires in CO and CT and does not in MT	• Some language references "duties" • 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 • Contracts must afford the controller the opportunity to reject subcontractors • More formal audit rights for controllers • Additional requirements and restrictions for 13-16 year olds

Colorado Privacy Act

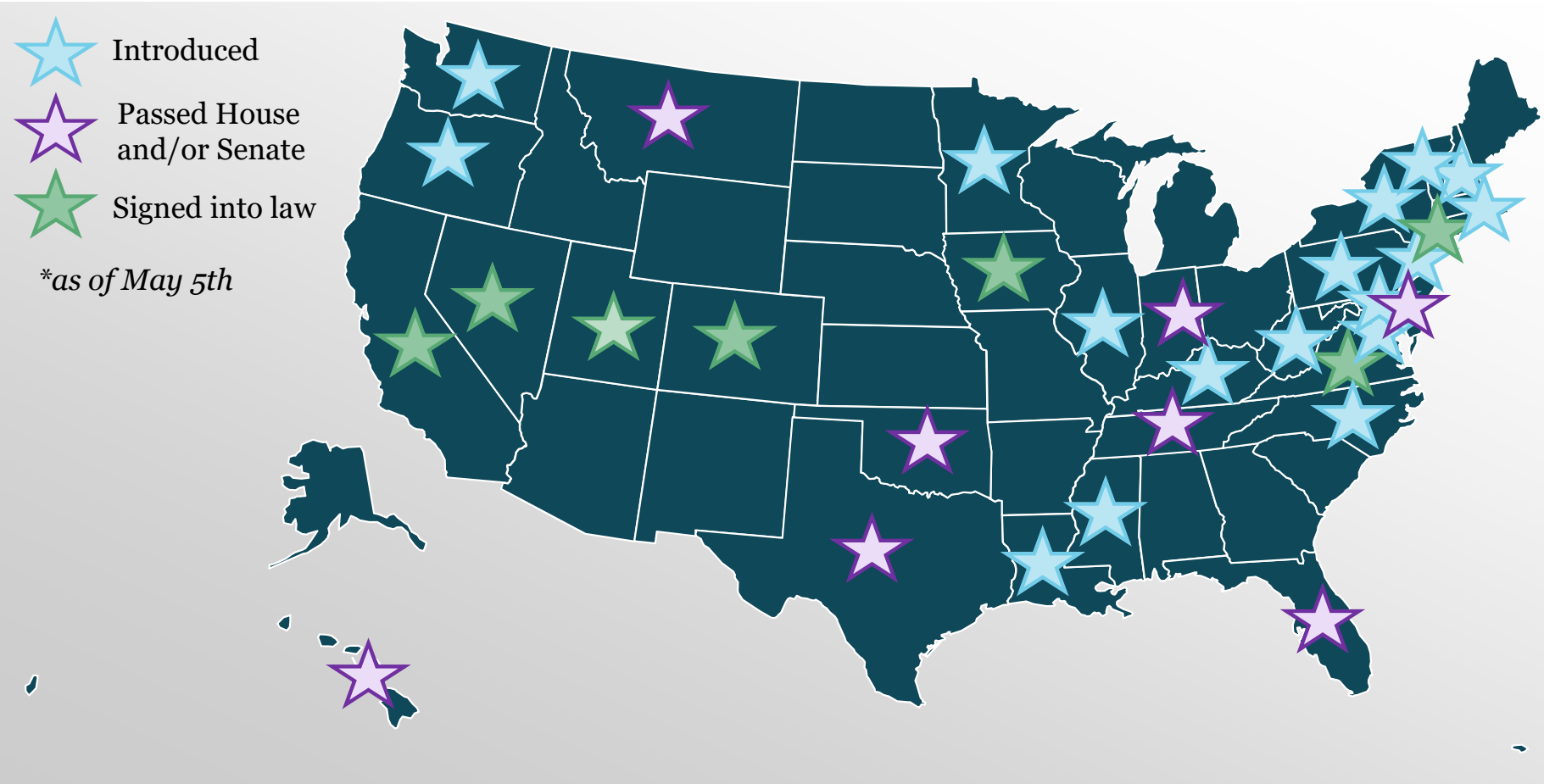
Rulemaking

Colorado Rulemaking Process



Other States

2023 State Comprehensive Privacy Proposals



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

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

Novel Approaches

- 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

Data Broker Bills

- Registration
- Prohibition on Processing Sensitive Data without Consent to the Data Broker
- Instructions for Courts to Disregard Steps Taken to Avoid "Sale" or "Profiling" Requirements

Key Trends and Battlegrounds

Overview of Key State Proposals

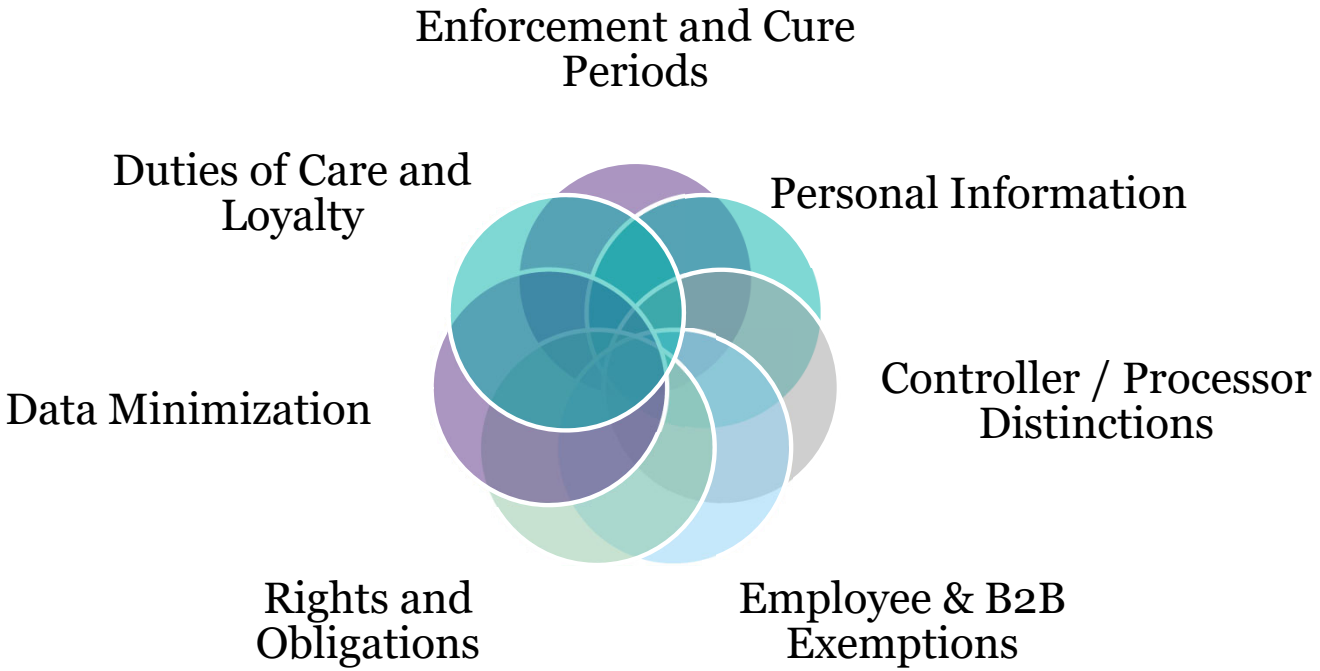
Category	Topic	CA	VA/IN/TN/FL	CO/CT/MT	UT/IA
Notice	At or before point of collection	✓			
	In a reasonably accessible privacy notice	✓	✓	✓	✓
Opt-Outs	Sale	✓	✓ (In some cases, narrower sale definition)	✓	✓ (Narrow Sale Definition)
	Targeted Advertising / Cross-Context Behavioral Advertising	✓	✓*	✓	✓*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

Key Battleground Issues



Legislative Sessions Adjourning in 2023

Timeline	
May 2023	Alaska, Arizona, Illinois, Kansas, Minnesota, Missouri, Oklahoma, South Carolina, Texas, Vermont
June 2023	Alabama, Connecticut, Delaware, Louisiana, Nebraska, Nevada, New Hampshire, New York, Oregon, Rhode Island
August 2023	North Carolina
September 2023	California
November 2023	Massachusetts
December 2023	Michigan, New Jersey, Ohio, Pennsylvania, Wisconsin

**Maine's special session is expected to adjourn this summer, but an end date has not been set.*

Federal Interplay

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
- Legislative Proposals
  - Kids Online Safety Act
  - COPPA 2.0

Part II

Privacy Hot Topics in 2021

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

- Connecticut, Illinois, Maryland, Minnesota, Nevada, New Jersey, New Mexico, New York, Oregon, Texas

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

Facial Recognition Technology

Restrictions on Use

- **Citywide restrictions on private use of facial recognition technology**
- **Citywide restrictions on government use of facial recognition technology**
  - Restrictions on municipal use and private use on public property
- **Statewide restrictions on use of facial recognition technology**
  - Restrictions on use by law enforcement and/or other public officials, and for certain use cases
- **Trend – greater restrictions or repeal?**

Health and Genetics

Consumer Health Data

- States have introduced legislation to grant consumers' greater rights over their health data, particularly with respect to reproductive health data and mental health data
- States continue to prohibit businesses / governmental entities from requiring proof of vaccination

Genetic Testing

- Several states have enacted or recently proposed genetic privacy laws with explicit consent requirements and stricter penalties
- There is a trend of states regulating "direct-to-consumer" genetic testing companies

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
- **Obligations:** Places several obligations on Washington businesses, including:
  - 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

Washington – My Health My Data Act (HB 1155)

Scope: Governs "consumer health data"

Exemptions: PHI under HIPAA, Part 2 information, certain research information, HIPAA de-identified information, among others

Enforcement: AG and private right of action

Transparency: Must publish a privacy policy for consumer health data

Consumer Rights: (1) access; (2) withdraw consent from the collection and sharing of their health data; and (3) deletion

Other Safeguards: Appropriate data security measures, data processing agreements with processors

Consent: Requires consent to collect and separate consent to share consumer health data

Authorization: Requires HIPAA-like authorization to sell consumer health data

Prohibitions: Prohibits geofencing around health care facilities for certain purposes, e.g., to track consumers seeking health care

Data Broker Laws & Proposals

California: AB 1202*

- Applies to Handling of "Personal Information"
- Annual Registration with AG
- Discretionary Disclosures
- **Amendments introduced*

Vermont: H 764*

- Applies to Handling of "Personal Information"
- Annual Registration with AG
- Mandatory Disclosures
- Information Security Program
- **State AG is considering amending this legislation*

Various states have proposals to enact or amend data broker laws. For example, California SB 362 would strengthen data broker registration requirements and allow Californians to direct all data brokers to delete their personal information.

Automated Decision-Making & Profiling

General ADM Requirements

- Required notice and assessments for automated decision-making
- Rulemaking to define the scope of access and opt-out rights for ADM

ADM Requirements for Higher Risk Contexts

- Required assessments for high-risk applications of algorithms.
- Prohibitions on use of discriminatory algorithms to make decisions about certain topics, like education or employment.
- Required disclosures and appeal process with human review for ADM resulting in a denial of certain services, such as housing or insurance.

State Agency Use

- Requirements for Procurement & Use

Recent 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

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

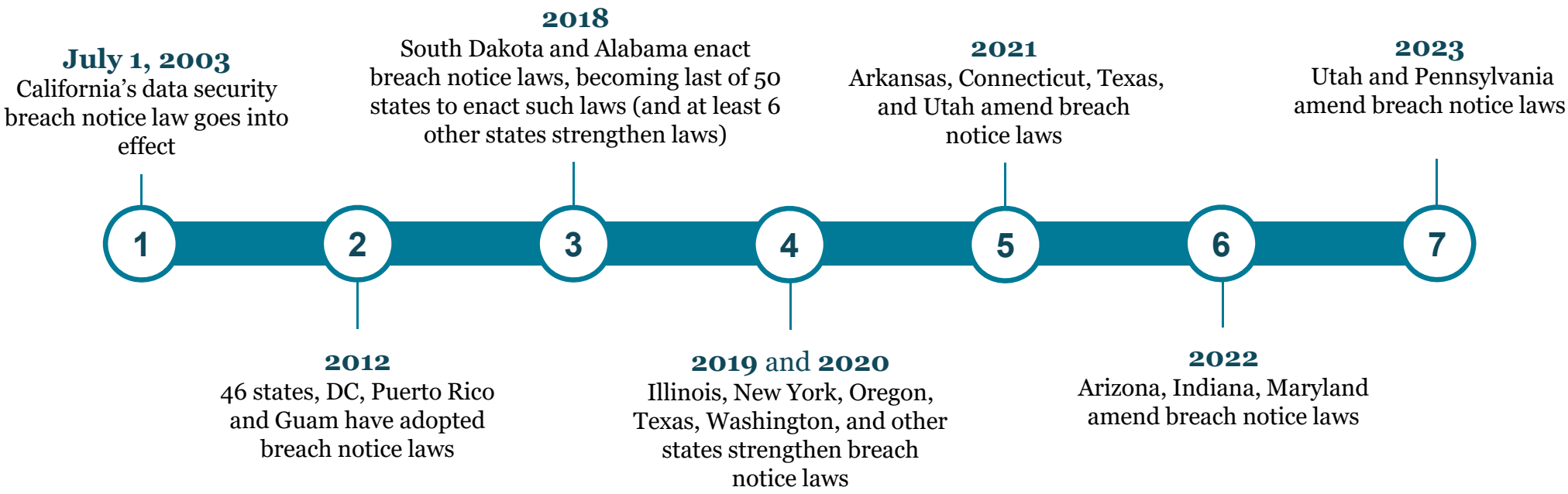
New York attorney general enters settlement with 'stalkerware' seller

AGs to Sue Google, Alleging 'Dark Pattern' to Track Users

Multiple states' attorneys general prepare to sue the search giant, accusing it of deploying deceitful tactics so it can track people.

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

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?