

# State Privacy Law Workshop

---

Hanna Abrams, Olga Medina, Libbie Canter, and Liz Lyons  
May 8, 2024

**COVINGTON**

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

[www.cov.com](http://www.cov.com)

# Presenters

---



**Libbie Canter**  
*Covington & Burling LLP*



**Liz Lyons**  
*HP*



**Olga Medina**  
*BSA | The Software Alliance*



**Hanna Abrams**  
*Maryland Office of the Attorney  
General*

# Agenda

---

State  
Comprehensive  
Privacy Laws

State Privacy and  
Data Security  
Hot Topics

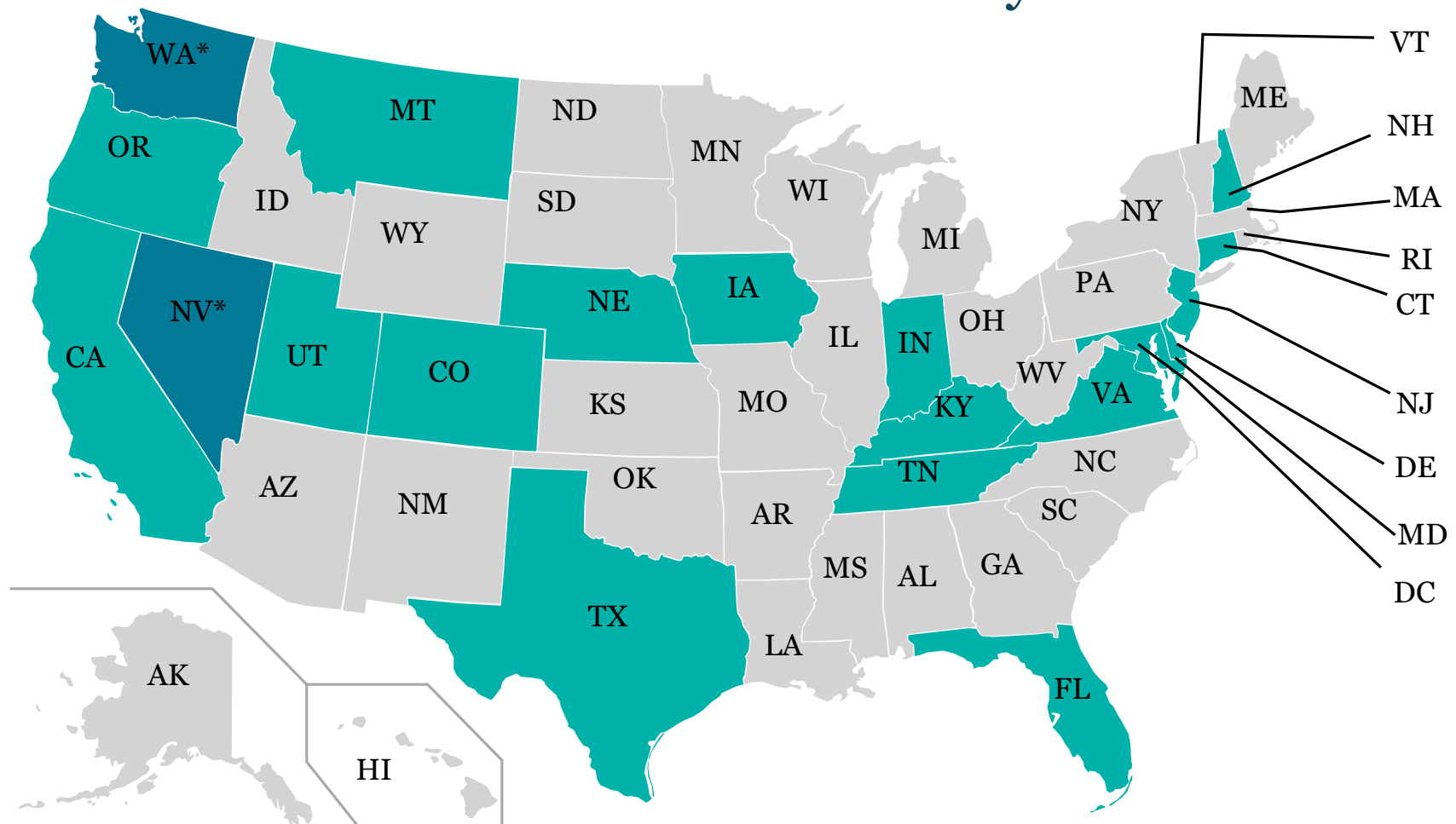
# Part I

---

## Comprehensive Privacy Laws

COVINGTON

# 16 States With Enacted Privacy Laws



*\*WA has enacted consumer health data laws, rather than a comprehensive privacy law; NV is narrower than other state laws.*

# California

---

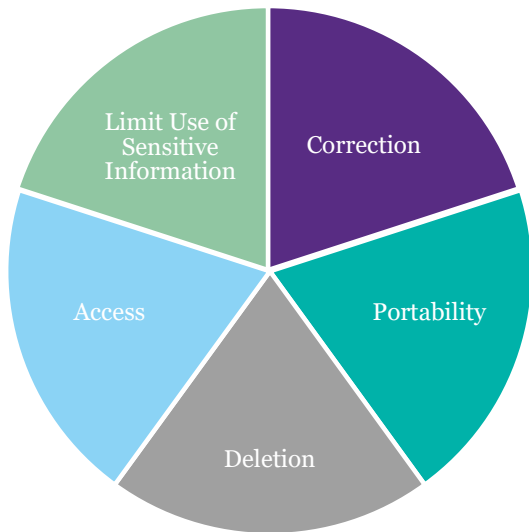
CCPA and CPRA



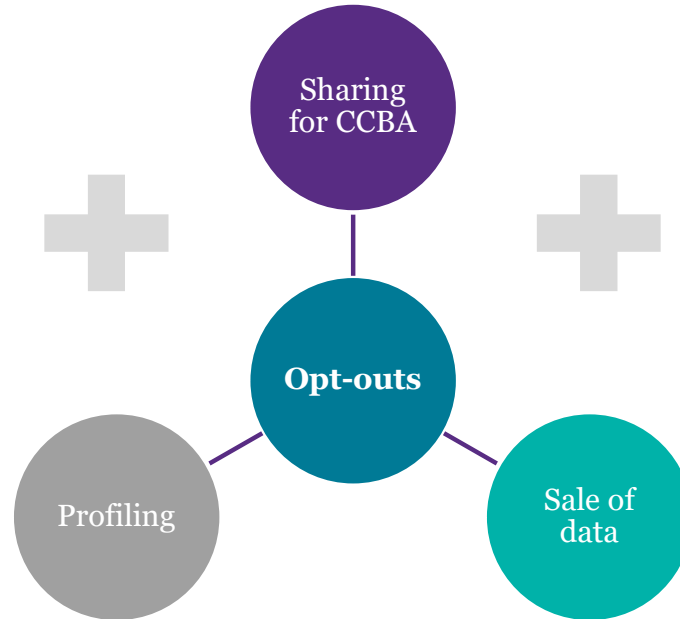
COVINGTON

# 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

# Other State Comprehensive Privacy Approaches

---

Colorado, Connecticut, Delaware,  
Florida, Indiana, Iowa, Kentucky,  
Maryland, Montana, Nebraska, New  
Hampshire, New Jersey, Oregon,  
Tennessee, Texas, Utah, and Virginia

COVINGTON





# Three Categories of State Privacy Laws

---

## **“Fewer Substantive Obligations”**

- Utah
- Iowa
- *Nevada*

## **“Baseline Approach”**

- Virginia
- Indiana
- Kentucky
- Tennessee
- Florida
- Texas
- Nebraska

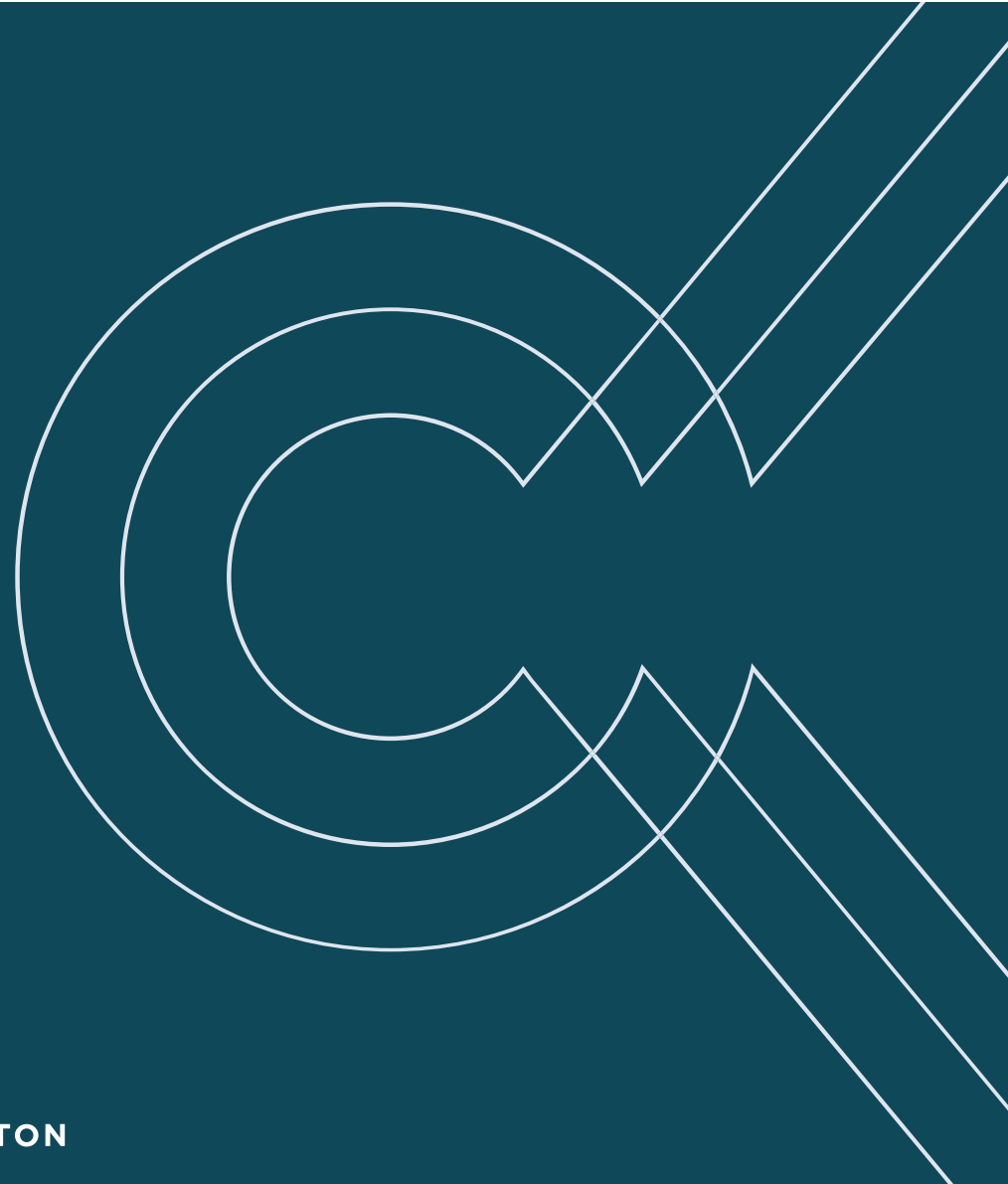
## **“More Substantive Obligations”**

- Colorado
- Connecticut
- New Hampshire
- New Jersey
- Montana
- Delaware
- Oregon
- Maryland\*

# “Baseline Approach”

---

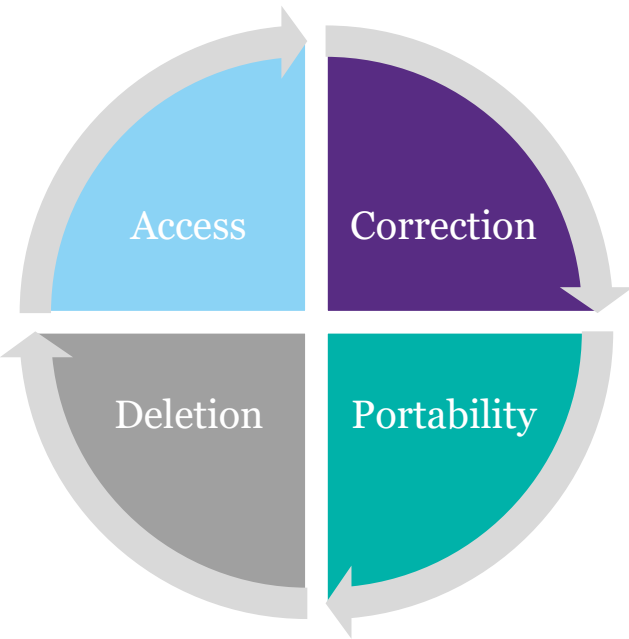
Virginia, Florida, Indiana,  
Kentucky, Nebraska, Tennessee,  
and Texas



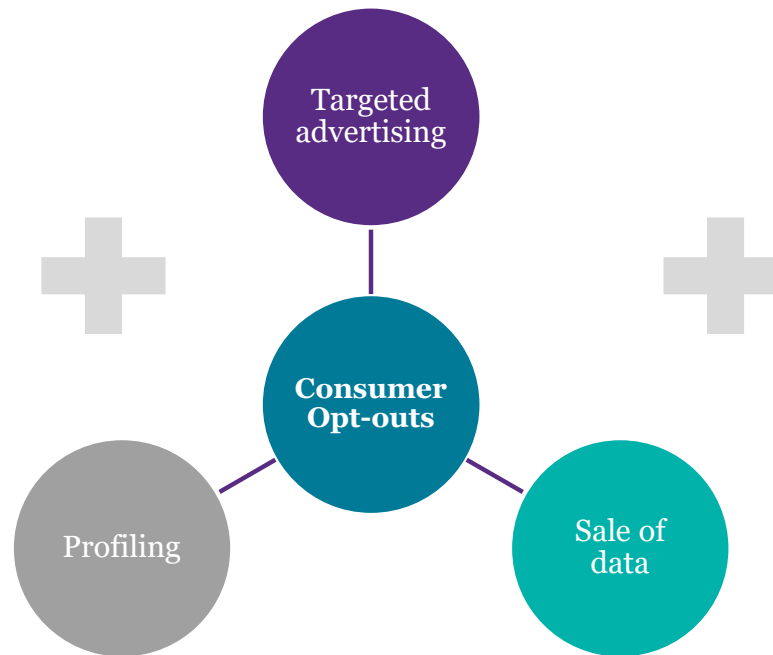
COVINGTON

# “Baseline”: VA, FL, IN, KY, NE, TN, and TX

GDPR/CCPA-like rights



CPRA-like rights



Opt-in for sensitive personal information



COVINGTON

# “Baseline”: VA, FL, IN, KY, NE, TN, and TX

---








## 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

-  Affirmative Defense for written privacy program that conforms with NIST framework
-  Special notice requirements for the sale of sensitive data
-  Scope of consumer rights
-  Protections for minors
-  Non-privacy digital provisions
-  Biometric data involves more limited scope
-  Utility exemption

# Fewer Substantive Obligations

---

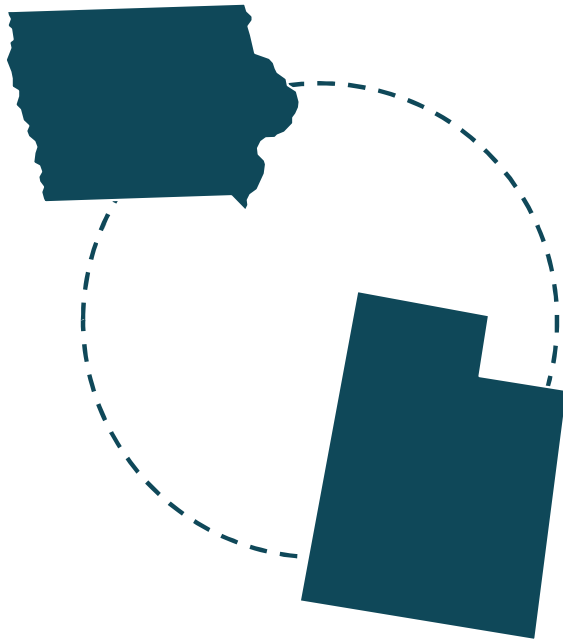
Utah and Iowa  
Nevada SB 220

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

# 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

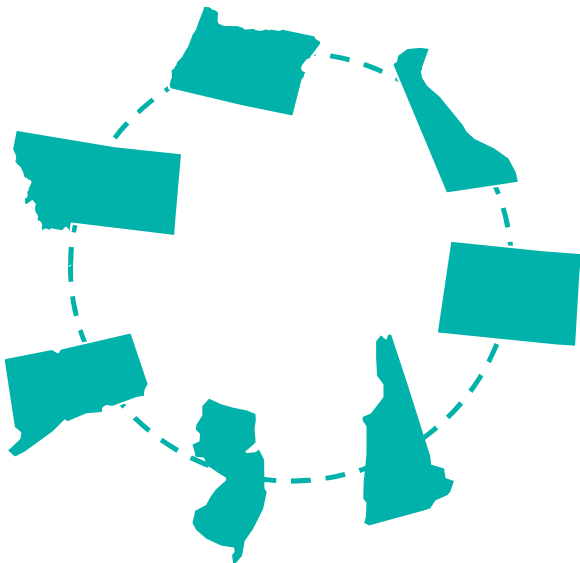
---

Colorado, Connecticut, Delaware,  
Maryland, Montana, New Hampshire,  
New Jersey, and Oregon

COVINGTON



# More Substantive Obligations: CO, CT, NH, NJ, 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 has detailed rulemaking, New Jersey has rulemaking, and New Hampshire has narrow rulemaking
- Oregon consumers have right to specific third parties list where data has been disclosed
- New Jersey includes a universal opt-out mechanism, and sensitive data definition that includes financial information with any security code
- For New Hampshire, access, correction, deletion, and portability rights do not extend to pseudonymized data

# Maryland: Deep Dive

---



COVINGTON

# Maryland Approach (MODPA)

---

## Data Minimization

- Requires collecting only what is reasonably necessary to provide/maintain consumer product or service requested

## Sensitive Data

- Prohibits collection unless strictly necessary for a specific consumer product or service requested
- No sale of sensitive data

## Children & Minors

- Restriction on sale of children's data when controller knows or *should have known* consumer is under the age of 18 years

## Unlawful Discrimination

- Targeted approach to prevent data collection/processing in a manner that unlawfully discriminates

## Geofencing

- Geofencing restrictions on health facilities

## Scope

- Low threshold for applicability

# Effective Dates

<b>Timeline</b>	
<b>July 1, 2024</b>	Florida, Texas
<b>October 1, 2024</b>	Montana
<b>January 1, 2025</b>	Delaware, Iowa, Nebraska, New Hampshire
<b>January 15, 2025</b>	New Jersey
<b>July 1, 2025</b>	Tennessee
<b>October 1, 2025</b>	Maryland
<b>January 1, 2026</b>	Indiana, Kentucky

# Comparing & Contrasting State Privacy Laws

---



COVINGTON

# Overview of Key State Proposals

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



# Emerging Areas of Divergence

## Data Minimization

- Utah: Silence
- Colorado: Reasonably necessary *for disclosed processing purposes*
- California: Reasonably necessary and proportionate to achieve *purposes consistent with reasonable expectations of the consumer*
- Maryland: Reasonably necessary *for maintenance of customer request*

## Sensitive Data

- Iowa: Opt-out
- Virginia: Opt-in consent
- Texas: Additional restrictions for sale of sensitive data (e.g., required notice language, small business provisions)
- Maryland: Prohibition on collection unless *strictly necessary*; prohibition on sale

*There are variations in scope/definitions of sensitive data*

## Children & Minors

- Virginia: Focus on adhering to COPPA
- California/Connecticut/Colorado: Additional protections for known 13-16 year olds
- Maryland: Additional protections when *know or should have known* consumer is under 18

*California, Connecticut, Florida, and Maryland\* also adopted separate age-appropriate design codes, discussed further below*

## Sale

- Virginia: Sale defined as exchange for *monetary* consideration
- California/Connecticut/Colorado: broader definition of sale (“valuable consideration”) and requirement to honor global opt-out preference mechanism

# Looking Ahead:

---

State Comprehensive Privacy  
Laws & Trends

COVINGTON



# Ongoing CCPA Enforcement Priorities



GOOGLE / TECH / POLICY

**Google to pay California \$93 million over location-tracking claims** / Google is settling California's claims that it tracked the locations of users without their consent.

CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies

*News: July 31, 2023*

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

**Attorney General Bonta Announces Settlement with DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws**

# CCPA Forthcoming Rulemaking

---

## Cyber Audits:

- Must complete a cyber audit if processing presents “significant risk” to consumers’ security (including processing PI of 250,000+ consumers)
- Audits must be completed using an independent auditor
- Prescriptive list of cyber audit requirements
- Submission of notice of compliance to CPPA

## Automated Decision-Making:

- Broad “automated decisionmaking technology” definition
- Applies to uses of ADMT beyond those that produce legal or similarly significant effects
- Pre-use notice requirements
- Access & opt-out rights

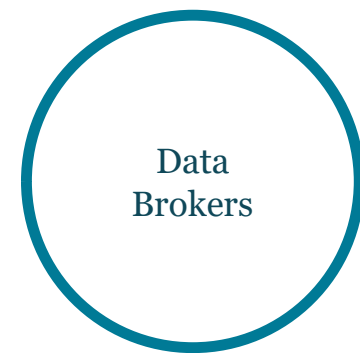
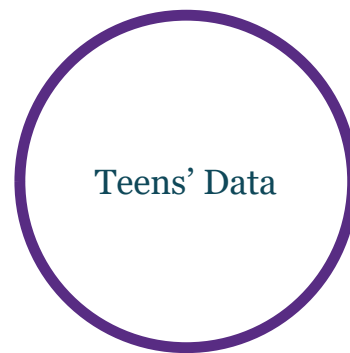
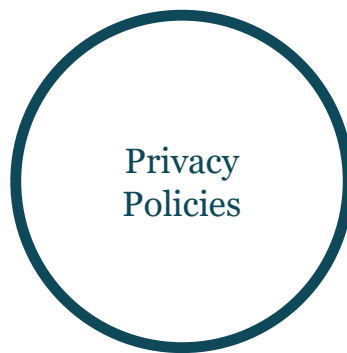
## Risk Assessments:

- Must complete a risk assessment if processing presents “significant risk” to consumers’ privacy (e.g., selling or sharing PI)
- Prescriptive list of risk assessment requirements, including ADMT-specific requirements
- Submission of risk assessment materials to CPPA

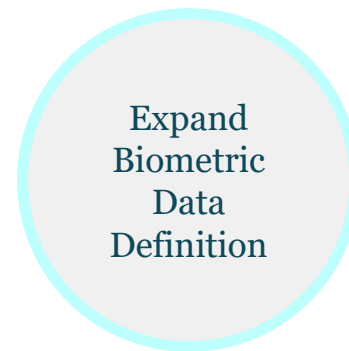
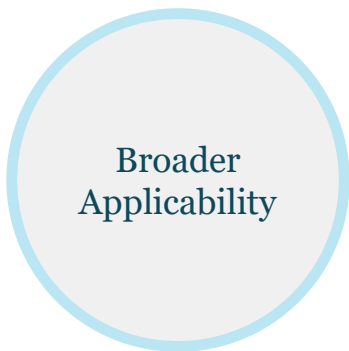
# CTDPA Enforcement Priorities & Legislative Recommendations

---

## Early Enforcement Priorities



## Legislative Recommendations



# Legislative Sessions Adjourning in 2024

<b>Timeline</b>	
<b>May 2024</b>	Alabama, Alaska, Arkansas, Colorado, Connecticut, Hawaii, Illinois, Kansas, Minnesota, Mississippi, Missouri, Oklahoma, South Carolina, Vermont
<b>June 2024</b>	Delaware, Louisiana, New Hampshire, New York, Rhode Island,
<b>July 2024</b>	Massachusetts, North Carolina
<b>August 2024</b>	California
<b>September – December 2024</b>	Michigan, New Jersey, Ohio, Pennsylvania

# Federal Interplay

---



COVINGTON

# Federal Developments

---

## American Privacy Rights Act

- Data Minimization Requirements & Purpose Limitations
- Consumer Rights (including centralized opt-out rights)
- Algorithmic Assessments
- Preemption with Exceptions
- Enforcement by FTC, AGs, and Private Actors

## FTC Rulemaking and Enforcement

- 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 harmful to 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

**PASSED**

California, Connecticut, Florida,  
Maryland\*

**INTRODUCED**

Colorado, Illinois, Minnesota,  
Nevada, New Jersey, New York,  
Texas, South Carolina, Vermont,  
Virginia

# Children & Teens: Social Media Laws

---

## Common Requirements

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

## INTRODUCED

Utah, Arkansas, Ohio,  
Louisiana, Texas,  
Florida

## INTRODUCED

Oklahoma, South  
Carolina, Georgia,  
Illinois, Idaho, New  
Jersey, Pennsylvania

# Washington – My Health My Data Act (HB 1155)

Scope	Applies to “regulated entities” and governs “consumer health data”
Consumer Rights	(1) confirm; (2) access; (3) withdraw consent; and (4) delete
Key Obligations	<ul style="list-style-type: none"><li>▪ Maintain and publish a privacy policy for consumers’ health data;</li><li>▪ Require separate and distinct consent to collect and share consumers’ health data;</li><li>▪ Prohibit the sale of consumers’ health data absent valid authorization;</li><li>▪ Prohibit the use of geofencing for certain purposes around health care facilities.</li></ul>
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, Connecticut SB 3, Maryland SB 541: Differences from WA MHMD

---

No private right of  
action

Different scope of  
“consumer data”

Fewer exemptions

# Genetic Privacy

---

## 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
- Recently enacted law in **Montana**, with **no exemption for de-identified data**



# 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

8 additional states are considering regulating data brokers

# 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

TECH / GOOGLE / POLICY

**Google to pay \$100 million to Illinois residents for Photos' face grouping feature**

**Justices Say BIPA Claims Accrue With Each Scan**

**Microsoft, Amazon granted summary judgement in biometric data privacy lawsuits**

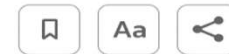
**First Jury Verdict Issued in Illinois Biometric Privacy Act Class Action**

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

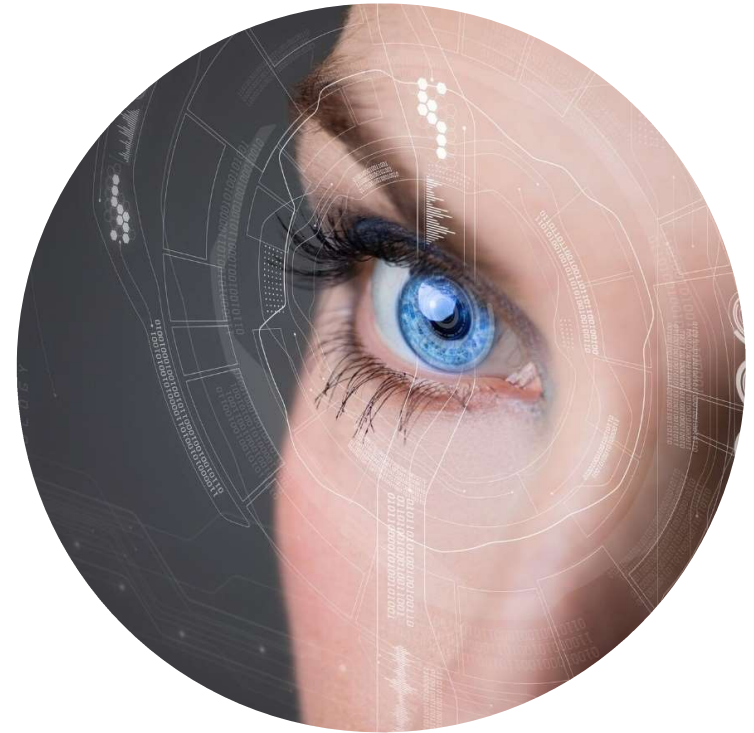


# Facial Recognition Technology

---

## Restrictions on Use

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



# Automated Decision-Making & Profiling

## State Legislative Trends

---

### Notice Requirements

- Notification for automated decisions that affect rights and opportunities

### Impact Assessments

- Aim to mitigate potential discrimination, privacy, and accuracy harms

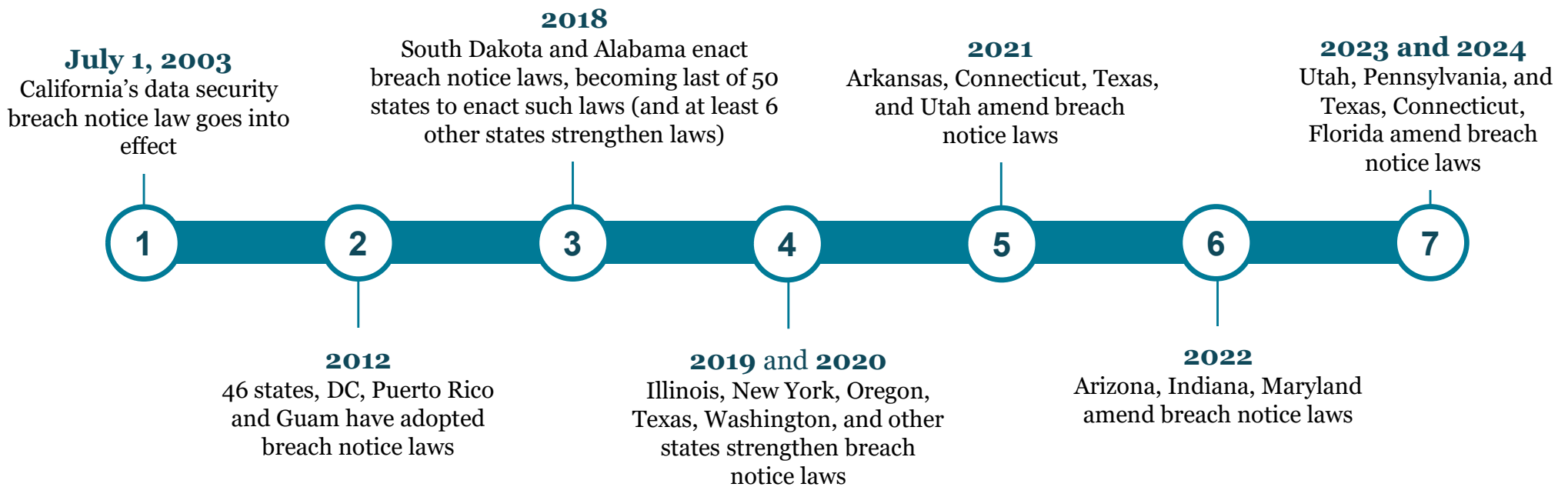
### Individual Rights

- Opt-outs and alternatives

### Licensing and Registration

- State-issued licenses for “high-risk” systems

# State Data Breach Laws



# Enforcement by State Attorneys General

## **Attorney General James Secures \$450,000 from Medical Company Providing Services in Western New York for Failing to Protect Patient Data**

US Radiology Experienced a Data Breach that Compromised Personal and Medical Data for Thousands of New Yorkers

November 8, 2023

▲ ZACKS

## **Morgan Stanley (MS) Agrees to Settle Charges on Customer Safety**

Zacks Equity Research  
Fri, Nov 17, 2023 • 4 min read

In This Article:

MS +0.63%

WASH +0.77%

**Morgan Stanley** MS has agreed on a \$6.5 million settlement with six state attorneys general, led by New York attorney general Letitia James. The firm's U.S. wealth management business, earlier known as Morgan Stanley Smith Barney LLC, was charged with failing to protect customers' personal information while shutting down two data centers in 2016.

PENNSYLVANIA NEWS

## **Attorney General announces settlement with Rutter's following data breach**

by: [Lara Bonatesta](#)  
Posted: Oct 11, 2023 / 01:45 PM EDT  
Updated: Oct 11, 2023 / 06:15 PM EDT

Blackbaud  
Oct 05, 2023

## Blackbaud Resolves Multi-State Attorneys General Investigation of 2020 Security Incident

## **Attorney General James Secures \$350,000 from Long Island Home Health Care Company for Failing to Protect Patient and Employee Data**

Personal Touch's Data Breach Compromised the Personal and Medical Data of More Than 300,000 New Yorkers  
AG James Secured Additional \$100,000 from Insurance Software Vendor for Compromising Personal Touch Employees' Data

October 18, 2023

COVINGTON

# 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?

---

