



## U.S. State Privacy Laws

How Companies Can Best Juggle Evolving U.S. State Compliance Requirements

Presented by Jordan Fischer | August 29 2023

1

### Jordan L. Fischer

CIPP/E, CIPP/US, CIPM  
Partner



[jfischer@constangy.com](mailto:jfischer@constangy.com)  
267.536.9376

Jordan Fischer is a Partner in Constangy's Cyber and Privacy team and has extensive experience in the intersection of law and technology, regularly evaluating and assessing legal and business opportunities and risk to provide public and private sector clients with critical data privacy and cybersecurity assessments and strategy. With a global perspective, Jordan represents clients regarding contractual negotiations related to technology, data management, security, and privacy and helps to build out compliance programs to address a multitude of regulatory requirements and best practices. She also counsels clients in cross-border data management and information governance, creating cost-effective and business-oriented strategies for information security, data privacy, and technology compliance.

Jordan is a globally recognized speaker on a variety of technology law topics. Additionally, she is the host of the American Bar Association's 'Cybersecurity and Data Privacy: The New Frontier' podcast, which focuses on data security, privacy, and related legal topics. On the podcast, Jordan discusses key considerations across industries related to the intersection of law and technology.



2

## Data Security vs. Data Privacy?

**Data Security** protects data from unauthorized compromise by external attackers and malicious actors

**Data Privacy** governs how data is collected, shared and used.

Attorneys have both a **Legal AND Ethical** obligation to keep information **SAFE** from unauthorized access.

3

## Data Privacy Landscape

Privacy – Governs how data is collected, shared and used.

**No Federal Law**

**Industry Specific Laws**  
HIPAA, GLBA, GDPR, PCI-DSS

**Patchwork of State Privacy Laws**

4

## How the United States Addresses Privacy

Gramm-Leach-Bliley Act (GLBA)	Health Insurance Portability and Accountability Act (HIPAA)	Children's Online Privacy Protection Act (COPPA)	Federal Trade Commission (FTC) Enforcement

5

## 2023 State Privacy Landscape

<b>CPRA</b>	January 1, 2023 Effective Date	July 1, 2023 Enforcement Date
<b>VCDPA</b>	January 1, 2023 Effective Date	Enforcement: Attorney General provides a controller or processor 30 days' written notice
<b>CPA</b>	July 1, 2023 Effective Date	Enforcement: 60-Day Cure Period by AG. Cure period only provided until January 1, 2025
<b>CTDPA</b>	July 1, 2023 Effective Date	Enforcement: 60-Day Cure Period by AG. Cure period ends on December 31, 2024.
<b>UCPA</b>	December 31, 2023 Effective Date	Enforcement: 30 days' written notice

6

## 2024 - 2026 State Privacy Landscape

<b>FL</b> 	July 1, 2024 Effective Date	Enforcement: 45-Day Cure Period by AG (except for violations involving a known child).
<b>TX</b> 	July 1, 2024 Effective Date	Enforcement: 30-Day Cure Period by AG.
<b>MT</b> 	October 1, 2024 Effective Date	Enforcement: 60-Day Cure Period by AG. Cure period ends on April 1, 2026
<b>OR</b> 	July 1, 2024 Effective Date	Enforcement: 30 day's notice. 30-day cure period sunsets on January 1, 2026
<b>IO</b> 	January 1, 2025 Effective Date	Enforcement: 90 days' written notice
<b>TN</b> 	July 1, 2025 Effective Date	Enforcement: 60 days' written notice
<b>IN</b> 	January 1, 2026 Effective Date	Enforcement: 30 days' written notice

WB4



7

## So What? Key Data Privacy Risks



Increased Activity from State Attorney Generals



Federal Trade Commission (FTC) Enforcement



Data Protection Authorities



Loss of Consumer Trust/Brand Reputation



8

## Slide 7

---

**WB4** Oregon "added" and all rearranged by date and then alphabetical

Williams, Be, 6/29/2023

## What's on the Line?

	Private Right of Action and Penalties
CCPA/CPRA 	<ul style="list-style-type: none"> <li>• There is a private right of action</li> <li>• The penalty for violation is up to a \$750 fine per consumer per incident, or actual damages</li> </ul>
VCDPA 	<ul style="list-style-type: none"> <li>• No private right of action</li> <li>• The attorney general can impose up to a \$7,500 fine per violation</li> </ul>
CPA 	<ul style="list-style-type: none"> <li>• No private right of action</li> <li>• A violation is a "deceptive trade practice" under the Colorado Consumer Protection Act, which carries up to a \$20,000 fine per violation</li> </ul>
CTDPA 	<ul style="list-style-type: none"> <li>• No private right of action</li> <li>• The attorney general can impose up to a \$5,000 fine per violation</li> </ul>
UCPA 	<ul style="list-style-type: none"> <li>• No private right of action</li> <li>• The attorney general can impose up to a \$7,500 fine per violation</li> </ul>
IOWA 	<ul style="list-style-type: none"> <li>• No private right of action</li> <li>• The attorney general can impose up to a \$7,500 fine per violation</li> </ul>



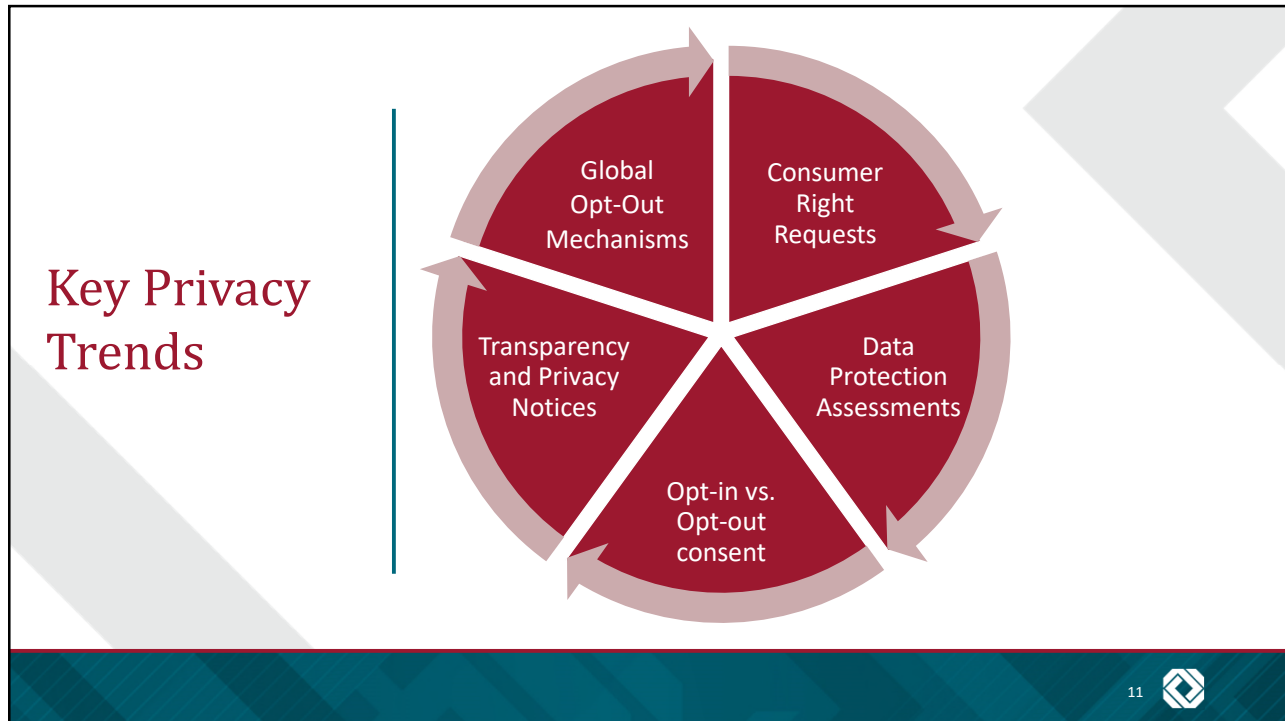
9



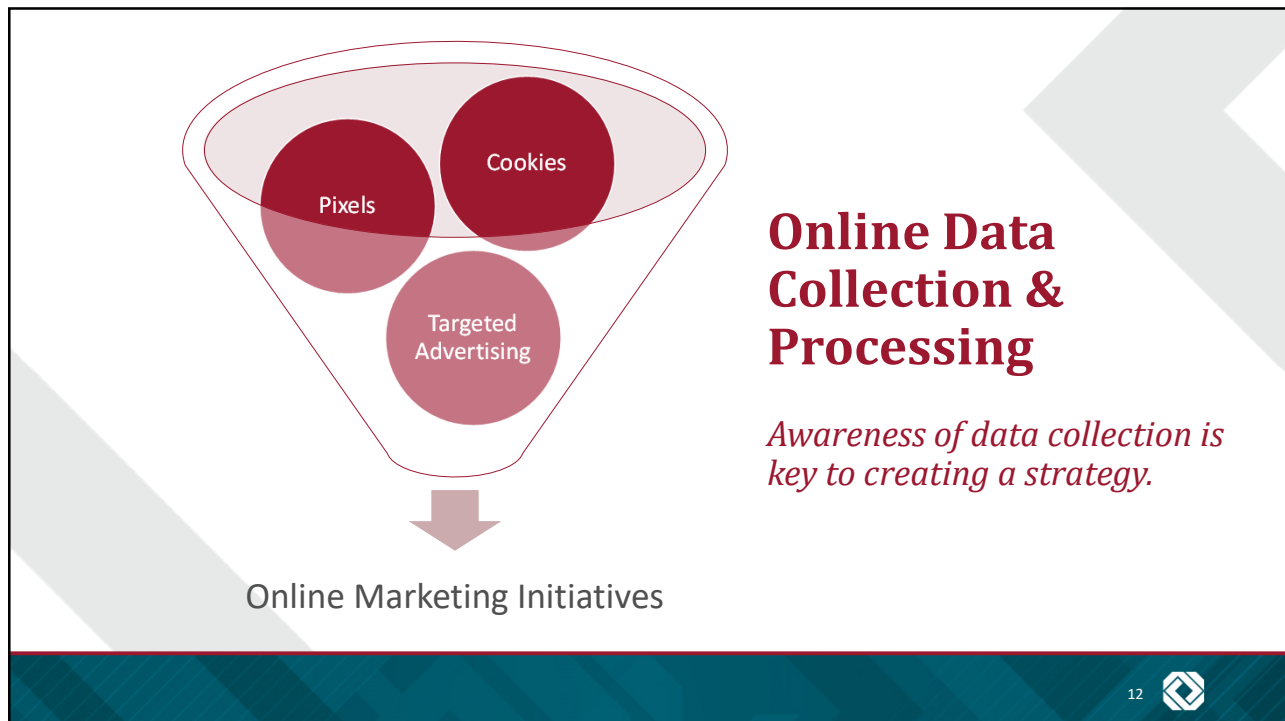
# Key Trends in State Privacy Law

10






11






12



## Overview of Consent

Two main forms of consent:

-  Opt-In: express, affirmative, or explicit consent
-  Opt-Out: soft opt in, default opt in, assumed, deduced, deemed, or implicit consent

13 


13

## Data Subject Rights & Responses

Rights and procedures vary by state, federal and international law

**Consumer Rights :**

- Disclose how you are collecting, using and disclosing data
- Opt Out of Sale or Sharing of Data
- Access Data
- Restrict Disclosures
- Correct Data
- Request Deletion of Data
- Accounting of Disclosures
- Know the categories of information collected or sold

14 

14



## Universal Opt-Out / Global Privacy Control Requirements

### Universal Opt-Outs / Global Privacy Control:

- A mechanism by which consumers can exercise their right to “opt out” of a platform or technology processing their personal data for targeted advertising or of the sale of their personal data.
- Applied at the browser level.

### Requirements:

- ✓ Allow for consumers to automatically communicate their opt-out choice with multiple controllers
- ✓ Allow consumers to clearly communicate one or more opt-out rights available under various privacy laws
- ✓ Recognize these browser-level signals and comply with those signals
- ✓ Describe any limitations that may be applicable to the mechanism
- ✓ Represent the consumer’s affirmative, freely given, and unambiguous choice to opt-out

15



15

## Perform a Data Map/Inventory and Privacy Risk Assessment

### Data Map / Inventory

- Determines what data and technology your organization possesses that needs to be protected.

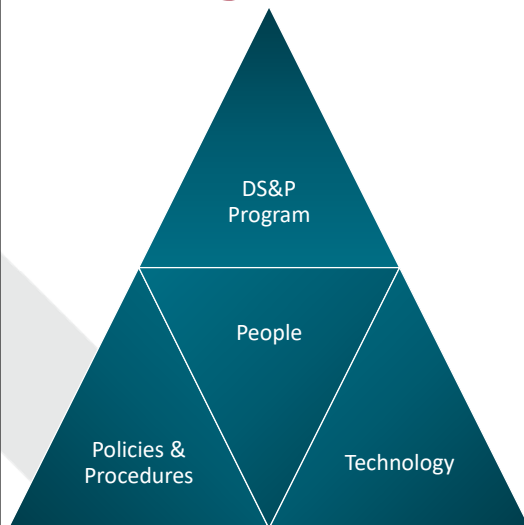
### Privacy Risk Assessment

- Identifies anticipated threats to information assets.
- Identifies the data collected and risk mitigation strategies.



16

## Building a Data Security & Privacy Program



All organizations should build a sustainable and scalable data security and privacy program that is tailored to the size of the organization and the sensitivity of its data and systems.

**\*\*Security should not be left solely to IT staff and tech consultants\*\***

17



17

## U.S. State Law Privacy: Best Practices



Know Your Data,  
its flows into and  
out of the  
business



Assess Your  
Administrative,  
Technical and  
Physical Controls  
(ATP's)



Update Your  
Forward-Facing  
Disclosures &  
Consent  
Mechanisms



Review Your DSR  
Policies and  
Training Program



Incident Response  
Plan Development  
and Tabletop  
Testing



20



20



# Questions?

## Thank You

Contact Information: [jfischer@constangy.com](mailto:jfischer@constangy.com)