Cyber Spotlight: Federal and State Privacy Legislation and Associated Requirements

WHERE ARE WE NOW?

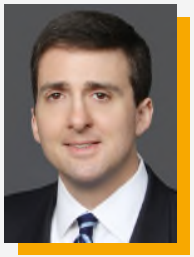
October 25, 2022

CYBERSECURITY AWARENESS MONTH 2022

MAYER | BROWN

Today's Presenters

Arsen Kourinian
Partner, Los Angeles



Howard Waltzman
Partner, Washington DC

Today's Agenda

Privacy Landscape in the US

General Structure
State Activity
US Biometric and AI Laws

Federal Privacy Legislation

The American Data Privacy and Protection Act
Key Elements
Issues of Contention

Privacy Landscape in the US

WHAT YOU NEED TO KNOW

US Privacy Laws – General Structure

- **Sector-specific federal legislation** (e.g., Gramm-Leach-Bliley Act, HIPAA).
- **State laws fill gaps or raise standards** (e.g., consumer privacy, breach notification, and data security).
- **Enforcement by state and federal agencies,** including the Federal Trade Commission (FTC), Health and Human Service (HHS), banking regulators, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and State Attorneys General.

US Privacy Laws – State Activity

1. **California Consumer Privacy Act (CCPA)**
   - Effective January 1, 2020
2. **California Privacy Rights Act (CPRA)**
   - Effective January 1, 2023
3. **Virginia Consumer Data Protection Act (VCDPA)**
   - Effective January 1, 2023
4. **Colorado Privacy Act (CPA)**
   - Effective July 1, 2023
5. **Utah Consumer Privacy Act (UCPA)**
   - Effective December 31, 2023
6. **Connecticut Data Privacy Act (CTDPA)**
   - Effective July 1, 2023

US Privacy Laws – State Activity

COMPARING CONSUMER RIGHTS UNDER STATE PRIVACY LAWS

Right	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Access	Yes	Yes	Yes	Yes	Yes	Yes
Correct	Yes	No	Yes	Yes	Yes	No
Delete	Yes (data provided by or obtained about consumer*)	Yes (data that consumer provided to controller)	Yes (personal data concerning consumer)	Yes (data provided by or obtained about consumer*)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes	Yes	Yes
Opt-out of sale	Yes	Yes	Yes	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes	Yes	Yes	Yes
Appeals process	Yes	No	Yes	Yes	No	No

* The CTDPA authorizes businesses that collect data indirectly (about, rather than from, a consumer) to opt the consumer out of processing as an alternative or to retain (suppress) minimal data to ensure continued deletion. The VCDPA was amended on April 11, 2022, in like fashion.

US Privacy Laws – State Activity

DATA CONTROLLER OBLIGATIONS UNDER STATE PRIVACY LAWS

Obligation	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Data minimization	Yes	Yes	Yes	Yes	Yes	No
Purpose limitation	Yes	Yes	Yes	Yes	Yes	Yes
Security requirements	Yes	Yes	Yes	Yes	Yes	No, but the private right of action applies to security breaches
Consent for sensitive data	Yes	No, consumers can opt-out	Yes	Yes	No, consumers can limit use to what is reasonably necessary	No
Special requirements for children's data	Yes (sale of personal information of children under 16 years)	Yes (personal data for a known child under 13 years)	Yes (personal data for a known child under 13 years)	Yes (sensitive data of children under 13 years)	Yes (sale of personal information of children under 16 years)	Yes (sale of personal information of children under 16 years)
Privacy notice	Yes	Yes	Yes	Yes	Yes	Yes
Disclose sale	Yes	Yes	Yes	Yes	Yes	Yes
Data protection assessment	Yes	No	Yes, available upon request by CO AG	Yes	Yes, risk assessments submitted to CA Privacy Protection Agency	No
Requirements for de-identified data	Yes	Yes	Yes	Yes	Yes	Yes

US Biometric Laws

Comparative Chart

Illinois, Texas, and Washington Biometric Privacy Statutes

	Illinois 740 ILCS 14	Texas Tex. Bus. & Com. Code Ann. § 503.001	Washington Engrossed Substitute House Bill 1493 (signed May 16, 2017)
Is the scope of the statute limited to a commercial purpose?	No	Yes. A commercial purpose may include a security purpose.	Yes. A commercial purpose may not include a security purpose.
Notice and consent requirements	Both notice and consent must be in writing. Notice must state (1) the fact that a biometric identifier or biometric information is being collected or stored, and (2) the specific purpose and length of term for which it is being collected, stored, and used.	Notice must precede the capture of the biometric identifier.	The exact notice and type of consent required is "context-dependent." Notice must be "given through a procedure reasonably designed to be readily available to affected individuals." A new use or disclosure requires new consent.
Retention requirements	Retention is permitted until "the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." Retention schedule must be publicly posted.	Destruction is required "within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires," absent enumerated exceptions.	A business may retain a biometric identifier "no longer than is reasonably necessary" to (1) comply with law or a court order, (2) protect against fraud, criminal activity, claims, security threats, or liability, and (3) provide the services for which the biometric identifier was enrolled.
Does the statute create a private right of action?	Yes	No	No
What damages are authorized?	Negligent violations: the greater of $1,000 or actual damages. Intentional or reckless violations: the greater of $5,000 or actual damages. (Statute also provides for attorney's fees.)	Maximum of $25,000 per violation.	Maximum of $500,000.
Is the sale of biometric identifiers permitted?	No	Yes, under enumerated circumstances (see chart below).	Yes, under enumerated circumstance (see chart below).
Is disclosure of biometric identifiers permitted?	Yes, under enumerated circumstances (see chart below).	Yes, under enumerated circumstances (see chart below).	Yes, under enumerated circumstances (see chart below).

US Biometric Laws

New State Comprehensive Privacy Laws Going into Effect in 2023:

- Opt-In: Colorado, Virginia and Connecticut
- Limit Use: California
- Opt-Out: Utah

US AI Laws

Automated processing regulated in comprehensive state privacy laws (California, Virginia, Colorado, Connecticut)

- Automated processing to evaluate, analyse or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- Opt-out extends to such activities (i.e., profiling) in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
- California standard TBD per draft regulations to be released.

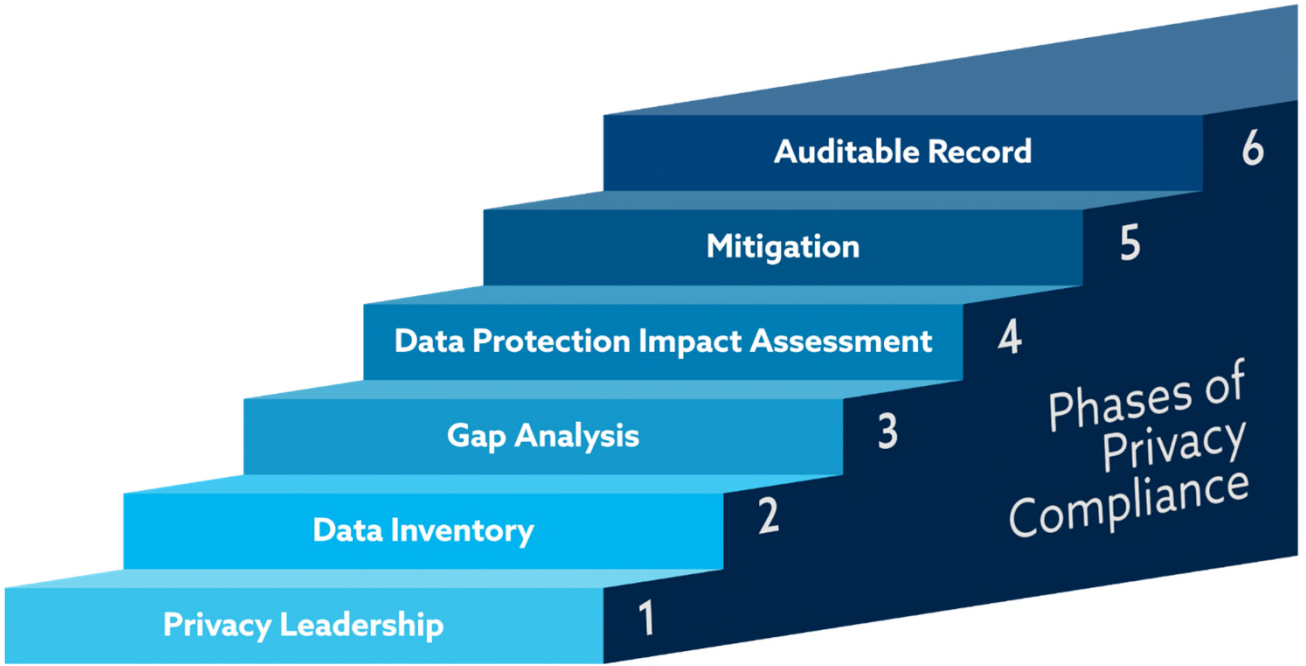
US Privacy Laws – State Activity

Effective Dates and Enforcement

The CTDPA adds to a growing timeline of comprehensive consumer privacy laws and regulations. The CCPA and its implementing regulations are already in effect. The CPRA becomes operative January 1, 2023, and enforceable on July 1, 2023, along with regulations to be adopted by the new California Privacy Protection Agency ("CPPA"). Draft CPRA regulations have been delayed until fall 2022. The Colorado AG also plans to issue draft regulations by fall 2022, to be finalized and adopted by July 1, 2023, when the CPA takes effect. The VCDPA (effective January 1, 2023) and UCPA (effective December 31, 2023) do not feature rulemaking or regulations. The CTDPA will slot in between the VCDPA and UCPA, taking effect on July 1, 2023, albeit without interpretive rulemaking or regulations.

Effective Date	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
January 1, 2020						✓
January 1, 2023				✓	✓	
July 1, 2023	✓		✓			
December 31, 2023		✓				

Six Phases of Privacy Compliance



Federal Privacy Legislation

WHAT YOU NEED TO KNOW

Comprehensive Federal Privacy Legislation

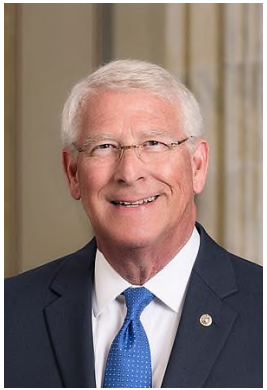
The Cry for a Bill

- With the increasing number of state privacy laws, industry has been clamoring for Congress to enact federal legislation that pre-empts the states.
- Civil rights and consumer advocacy groups have sought federal legislation to address their concerns about the use of algorithms and online tracking that produce discriminatory outcomes.

Comprehensive Federal Privacy Legislation

Early Developments

- Prior to 2019, Members of Congress mostly discussed principles for privacy legislation, but did not introduce legislation.
- At the end of 2019, Senators Wicker and Cantwell, the Chairman and Ranking Democrat on the Senate Commerce Committee, respectively, introduced competing, yet similar bills.
- Additionally, the leaders of the House Energy & Commerce Committee released a staff discussion draft.

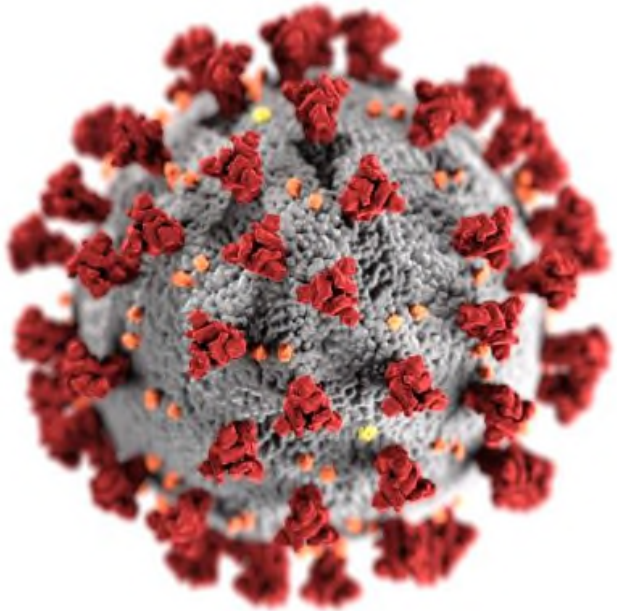


MAYER BROWN

Comprehensive Federal Privacy Legislation

Covid Hampers Progress

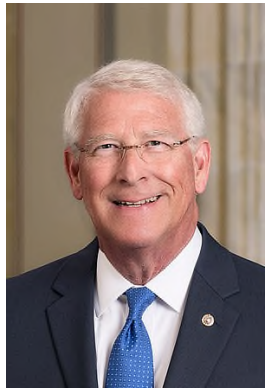
- The pandemic slowed these efforts, especially as Members of Congress focused on pandemic-related priorities.
- However, the key Members of Congress (Senators Wicker and Cantwell and Representatives Pallone and McMorris-Rodgers) and their staffs continued to meet to try to reach a compromise on legislation.
- These discussions broke down earlier this year.



Comprehensive Federal Privacy Legislation

ADPPA Emerges

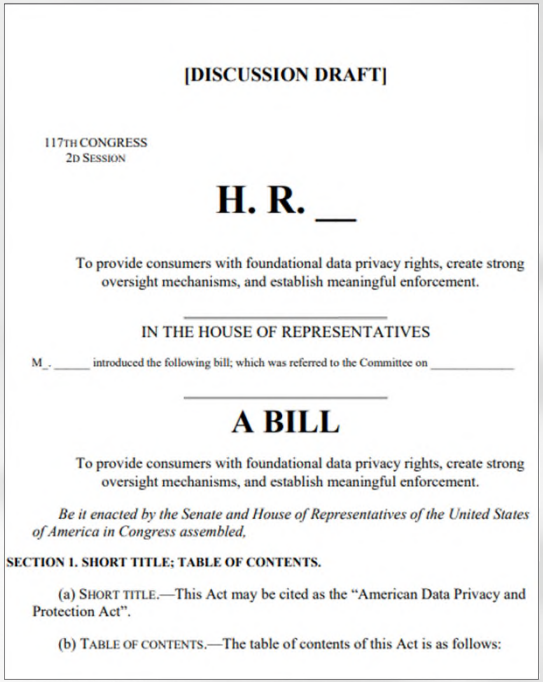
- Senator Wicker continued to negotiate with Representatives Pallone and McMorris-Rodgers.
- These discussions produced the release of a bill, the American Data Privacy and Protection Act ("ADPPA"), in June.
- The House Energy & Commerce Committee proceeded to mark up the legislation and reported it to the full House in July.



The ADPPA

Key Elements

1. Data Minimization and Prohibited Practices
   - The bill also contains permissible purposes that ostensibly modify the data minimization and prohibited practices.
2. Transparency and Consumer Choice
3. Access, Correction, Deletion, and Data Portability
4. Civil Rights and Algorithmic Bias
5. Provisions Specific to Minors



[DISCUSSION DRAFT]

117TH CONGRESS
2D SESSION

H. R. __

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE HOUSE OF REPRESENTATIVES

M_. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

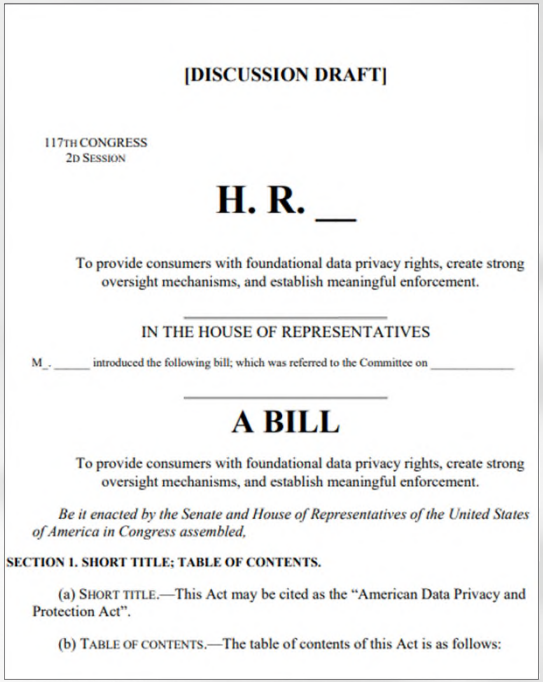
(a) SHORT TITLE.—This Act may be cited as the "American Data Privacy and Protection Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

The ADPPA

Key Elements (cont'd)

6. Data Brokers
7. Data Security
8. Sharing Consumer Data with Service Providers and Third Parties



[DISCUSSION DRAFT]

117TH CONGRESS
2D SESSION

H. R. __

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE HOUSE OF REPRESENTATIVES

M_. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

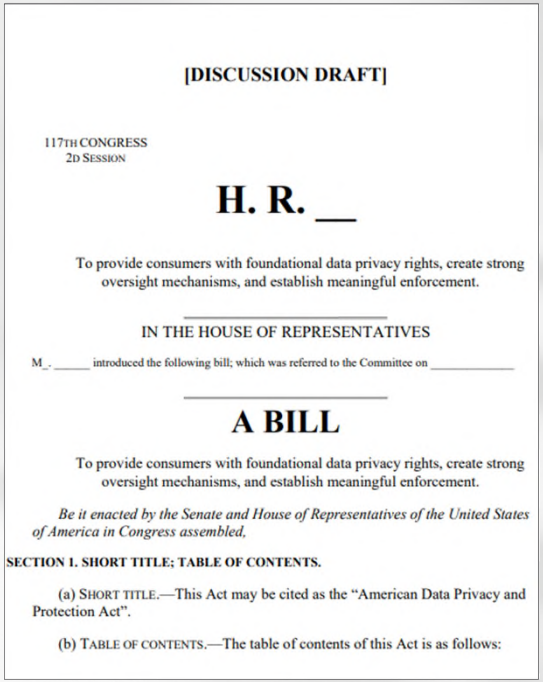
(a) SHORT TITLE.—This Act may be cited as the "American Data Privacy and Protection Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

The ADPPA

Key Elements (cont'd)

9. Enforcement
   - By the FTC
   - By State AGs
   - Private Rights of Action
10. The Relationship Between Federal and State Laws



[DISCUSSION DRAFT]

117TH CONGRESS
2D SESSION

H. R. __

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE HOUSE OF REPRESENTATIVES

M_. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "American Data Privacy and Protection Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

The ADPPA

Key Issues of Contention

1. State Preemption
   - California
   - Other state laws
2. Private Rights of Action
3. Permissible Purposes/Business Operations
4. Algorithmic Bias

Questions?

THANK YOU

Arsen Kourinian
akourinian@mayerbrown.com
+1 213 229 5141

Howard Waltzman
hwaltzman@mayerbrown.com
+1 202 263 3848

Americas | Asia | Europe | Middle East

mayerbrown.com