Privacy Update

Briefing on New State Data Privacy Laws with a Spotlight on Tennessee's NIST Privacy Framework-Related Affirmative Defense

Mike Signorelli | Partner
MASignorelli@Venable.com

Jamie Danker | Senior Director of Cybersecurity and Privacy Services
JMDanker@Venable.com

Allaire Monticollo | Associate
AMMonticollo@Venable.com

Ivy Orecchio | Cybersecurity and Privacy Services Project Manager
IDOrecchio@Venable.com

June 7, 2023

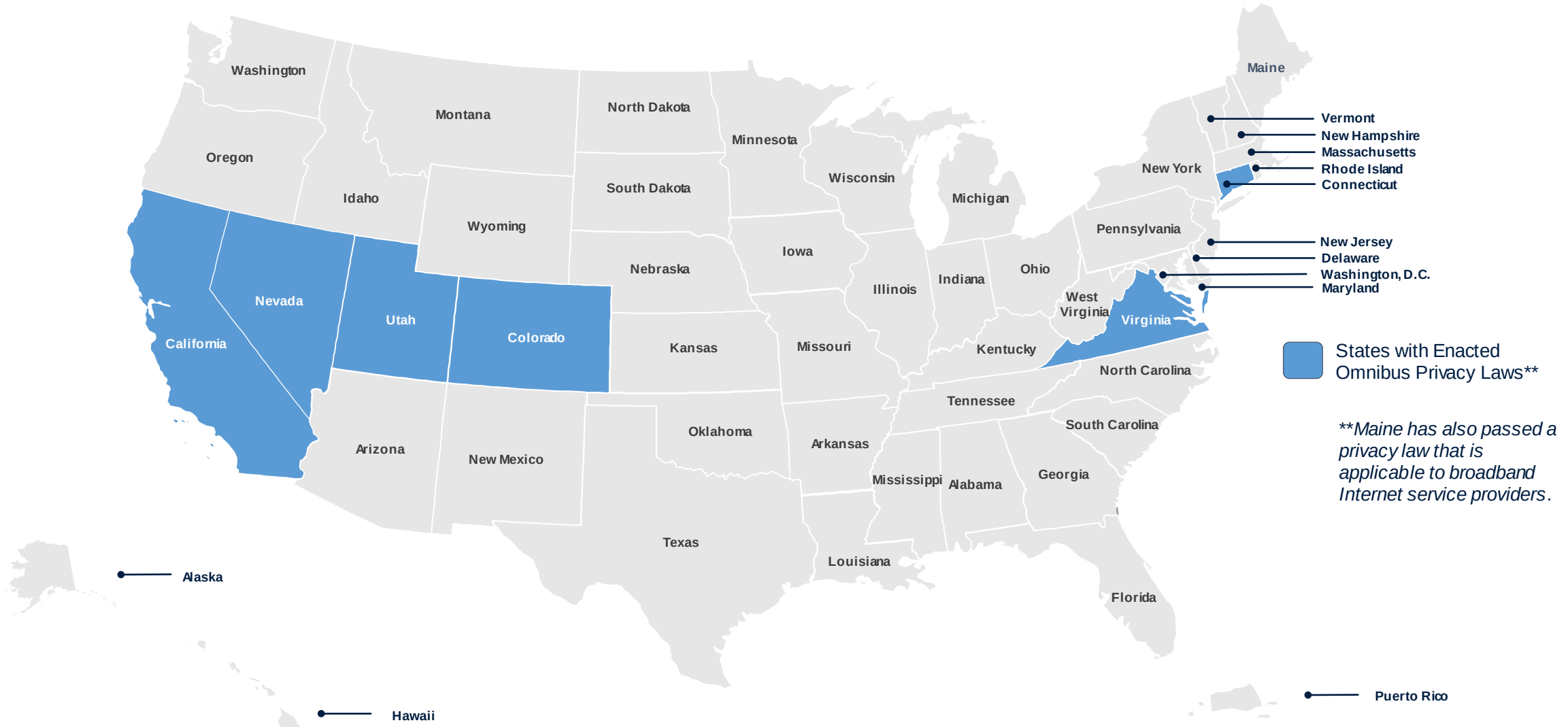
VENABLE LLP

A Step Back in Time

The State of the States on January 1, 2023

VENABLE LLP

State Privacy Laws as of January 1, 2023

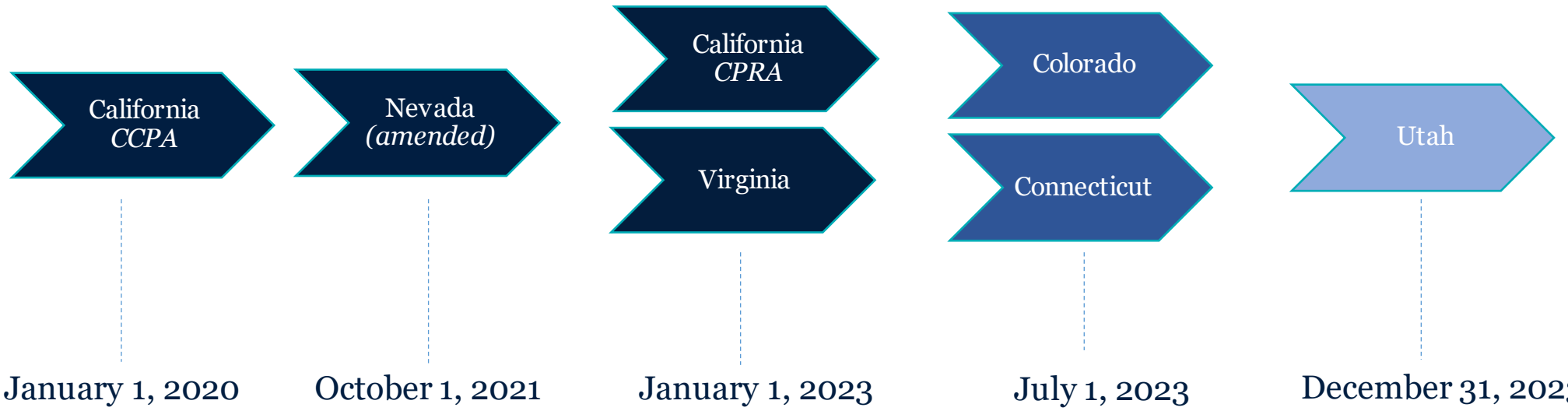


***Maine has also passed a privacy law that is applicable to broadband Internet service providers.*

VENABLE LLP

Timeline

Pre-2023 State Privacy Laws: Effective Dates



VENABLE LLP

Pre-2023 State Privacy Laws at a Glance

	CPRA	CO	CT	NV	UT	VA
Access	✓	✓	✓		✓	✓
Deletion	✓	✓	✓		✓	✓
Correction	✓	✓	✓			✓
Opt Out of Sales	✓	✓	✓	✓	✓	✓
Opt Out of Sharing for Cross-Context Behavioral Advertising	✓					
Opt Out of Targeted Advertising		✓	✓		✓	✓
Opt Out of Profiling		✓	✓			✓
Choice Regarding Sensitive Data	Opt-out / Right to limit	Opt-in	Opt-in		Opt-out	Opt-in
Appeals Process Explicitly Required		✓	✓			✓
Assessment Requirements	TBD in Regulations	✓	✓			✓
Consumer Rights Apply to Pseudonymous Data	✓	Some rights	Some rights	No explicit statement	Some rights	Some rights
Explicit Global Privacy Control Requirement	✓	✓	✓			

VENABLE LLP

Pre-2023 State Privacy Laws: Enforcement

- **California.** The law stands up the **California Privacy Protection Agency** to enforce its terms **alongside the California Attorney General**. CPPA enforcement is subject to a **discretionary 30-day cure period**. CPPA enforcement is set to begin on July 1, 2023. The CPRA also provides a limited **private right of action related to certain data breaches**, which is subject to a **30-day cure period**.
- **Virginia.** The law is enforceable by the **Virginia Attorney General**, and a **30-day cure period** is available. The law does not provide for a private right of action.
- **Colorado.** The law is enforceable by the **Colorado Attorney General and district attorneys**. If a cure is "**deemed possible**," a **60-day cure period** is available to controllers **until January 1, 2025**. The law does not provide for a private right of action.
- **Connecticut.** The law is enforceable by the **Connecticut Attorney General**, and violations will constitute an unfair trade practice for purposes of Connecticut's UDAP statute. A **60-day cure period** is available **until December 31, 2024**, if a cure is "**deemed possible**." Beginning on January 1, 2025, the Connecticut Attorney General has discretion to provide a cure period. The law does not provide for a private right of action.
- **Utah.** The law tasks the Utah Division of Consumer Protection with investigating violations and referring them to the **Utah Attorney General** for enforcement, and a **30-day cure period** is available. The law does not provide for a private right of action.
- **Nevada.** The law is enforceable by the **Nevada Attorney General**. **A one-time 30-day cure period is available for certain violations**. The law does not provide for a private right of action.

VENABLE LLP

Pre-2023 State Privacy Laws: Regulatory Processes

- **California.** Initial CPRA implementing regulations issued by the California Privacy Protection Agency (CPPA) took effect on March 29, 2023.
    - **Enforcement Start Date:** July 1, 2023.
    - **What's Next.** The CPPA began preliminary activities related to a future rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking on February 10, 2023. The preliminary comment period closed on March 27, 2023, and the Agency has not yet taken further action.

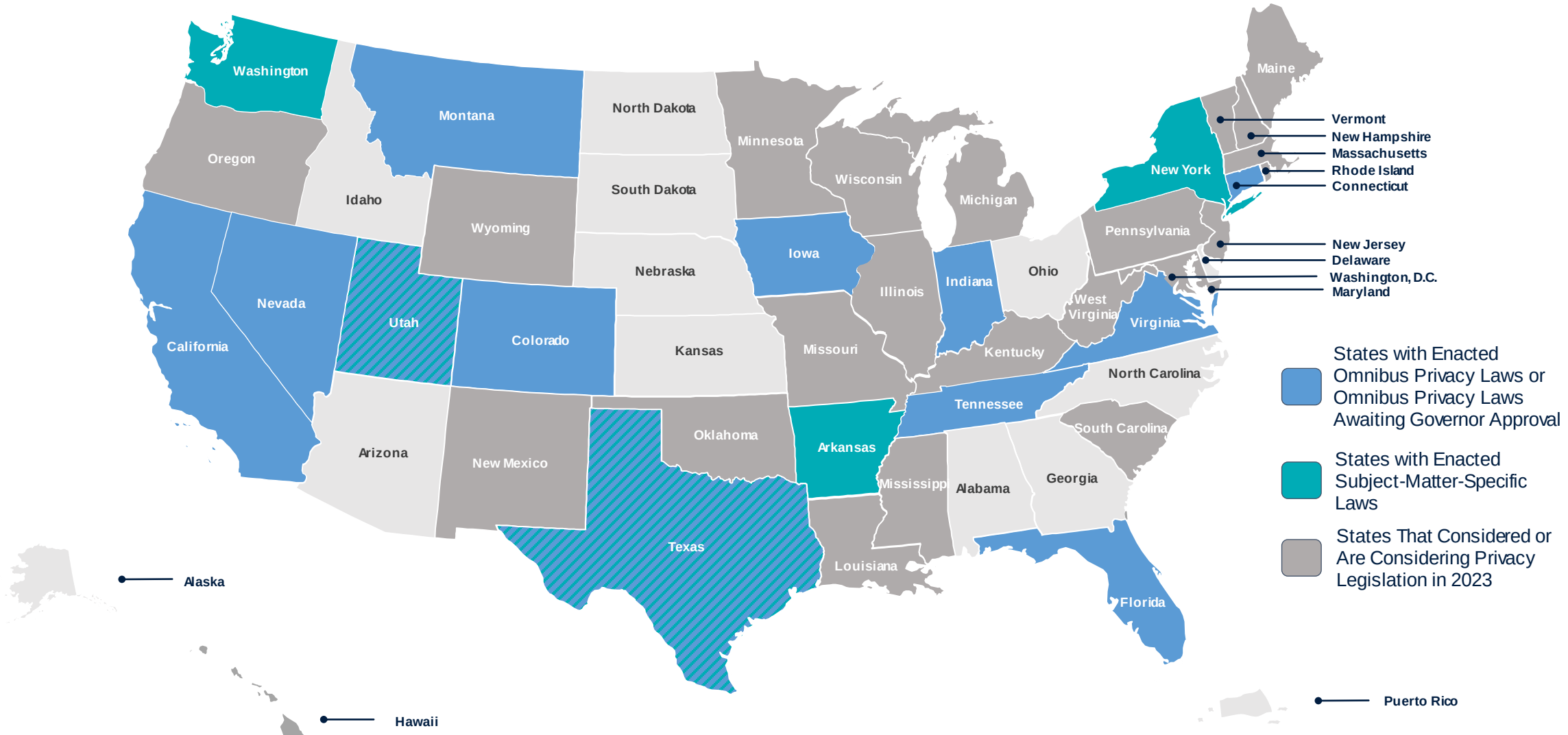
- **Colorado.** The Colorado Attorney General issued final rules implementing the CPA in March 2023, and these rules were subsequently published in the Colorado Register.
    - **Enforcement Start Date:** July 1, 2023.

Fast Forward

The State of the States Today

VENABLE LLP

2023 State Privacy Bills (June 2023)



VENABLE LLP

Key Trend: Minors

Utah Social Media Regulation Act

- Applies to a "**social media company**" that runs a "**social media platform**," *i.e.*, a person or entity that provides an online forum to an account holder to create a profile, upload posts, view posts, and interact with other account holders, that has at least 5 million account holders worldwide, and is an interactive computer service.
- Prohibits social media platforms from using practices, designs, or features that would cause an individual under age 18 to become addicted to the platform.
- Requires parental consent for individuals under age 18 to use social media accounts and requires social media platforms to verify users' ages.
- Limits minors' hours of access to social media and prohibits advertising to minors via social media accounts.
- Enforceable via a private right of action and the Utah Attorney General.
- **Effective on March 1, 2024**.

Arkansas Social Media Safety Act

- Applies to a "**social media company**," *i.e.*, an online forum that a company makes available for an account holder to create a public profile/account, upload or create posts, view posts, and interact with other account holders or users, subject to certain exceptions. Applies to a "**social media platform**," *i.e.*, a public or semipublic internet-based service or application that has users in Arkansas and connects users in order to allow them to interact socially with each other within the service or application.
- Requires parental consent for individuals under age 18 to hold social media accounts and requires social media platforms to verify users' ages through third-party vendors or other commercial entities.
- Creates civil liability for failing to verify age and damages resulting from access by an individual under age 18 to social media without parental consent.
- Creates liability for any commercial entity or third-party vendor that retains identifying information of an individual after access to the social media platform is granted.
- Enforceable via a private right of action, the Arkansas Attorney General, and state prosecutors.
- **Effective on September 1, 2023**.

VENABLE LLP

Key Trend: Minors

Texas Securing Children Online Through Parental Empowerment (SCOPE) Act

- Applies to any "**digital service provider**" that allows users to socially interact with other users on the digital service; allows a user to create a public or semi-public profile; and allows a user to create or post content that can be viewed by other users of the digital service, including sharing content on a message board, chat room, landing page, video channel, or main feed that presents to a user content created and posted by other users.
- A digital service provider may not enter into an agreement with a person to create an account with a digital service unless the person has **registered the person 's age** with the digital service provider.
- Digital service providers may not allow a known minor (U-18) to **make purchases** or engage in financial transactions through the digital service; **sell, share, or disclose** the known minor's personal identifying information; use the digital service to collect **precise geolocation information** related to the known minor; or use the digital service to **display targeted advertising to the known minor**.
- Digital service providers must **develop a strategy to prevent a known minor's exposure to harmful material** and other content that glorifies suicide, self-harm, eating disorders, substance abuse, stalking, bullying, harassment, grooming, trafficking, child pornography, or other sexual exploitation or abuse. The law contains specific requirements for the required strategy, including a requirement to "**mak[e] available the digital service provider's algorithm code to independent security researchers**," subject to certain trade secret protection exceptions.
- Digital service providers must create and provide to a **verified parent parental tools** to allow the verified parent to supervise the known minor 's use of a digital service.
- Digital service providers must use commercially reasonable effort to prevent advertisers from targeting a known minor with advertisements that offer a product or service that is unlawful for a minor.
- Digital service providers must observe certain **disclosure requirements related to use of algorithms**.
- Permits enforcement by the Texas Attorney General under the state's UDAP statute and private actions for declaratory judgment or injunctions, as well as class action lawsuits.
- Includes requirements for electronic devices and software applications used by students in a school district or open-enrollment charter school.

VENABLE LLP

Key Trend: Health Data

Washington My Health My Data Act

- Requires entities that conduct business in Washington to obtain separate and distinct consent to collect, share, or sell consumer health data, subject to few exceptions.
- Requires a consumer health data privacy policy that makes certain disclosures.
- Consumer health data is defined broadly to include "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."
- Grants consumers rights of access and deletion, and a right to withdraw consent. The right of access includes the right to obtain a list of all third parties with whom health data has been shared or to whom it has been sold.
- Bars geofencing around entities that provide in-person health care services where the geofence is used to (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.
- Enforceable via a private right of action and the Washington Attorney General.
- **Effective on July 23, 2023**; most operative requirements do not commence until **March 31, 2024** for most regulated entities and **June 30, 2024** for small businesses.

New York State Health and Mental Hygiene Budget Bill (A3007C)

- Passed as part of a budget package; adds a provision to NY's UDAP statute that bars geofencing around health care service providers by any entity other than the owner of the health care facility for purposes of delivering digital advertisements, building consumer profiles, or inferring health or medical information of a person.
- Enforceable via a private right of action and the New York Attorney General.
- **Effective on July 1, 2023**.

VENABLE LLP

Deep Dive

New Omnibus Privacy Laws

VENABLE LLP

Newly Enacted Omnibus Privacy Laws (as of June 7, 2023)

Florida Digital Bill of Rights

Montana Consumer Data Privacy Act (MCDPA)

Iowa

"An Act Relating to Consumer Data Protection"

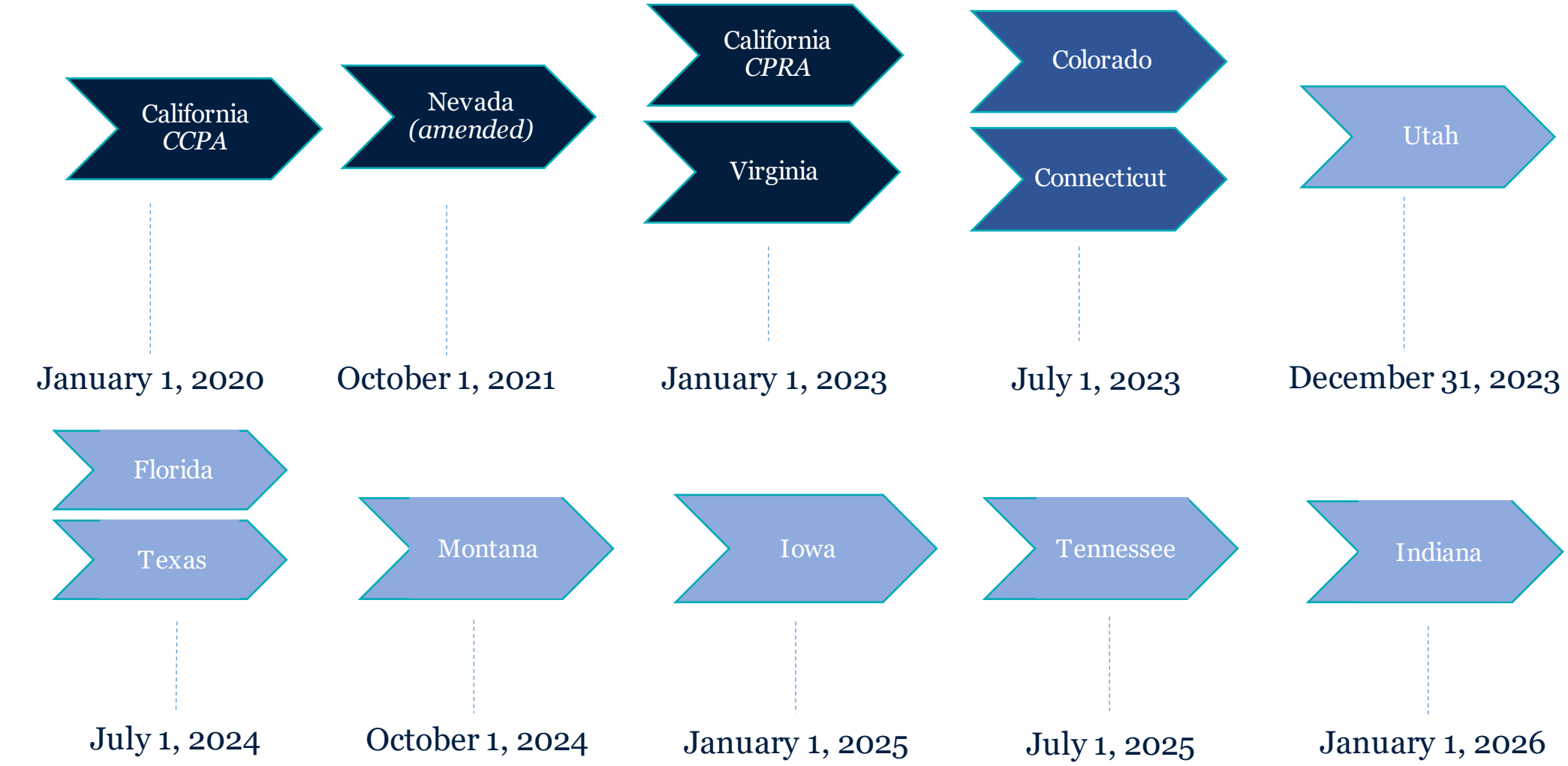
Tennessee Information Privacy Act (TIPA)

Indiana Consumer Data Protection Act

Texas Data Privacy & Security Act

VENABLE LLP

Timeline
Laws Effective



VENABLE LLP

Omnibus State Privacy Laws at a Glance

	CPRA	CO	CT	NV	UT	VA	FL	IN	IA	MT	TN	TX
Access	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Deletion	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Correction	✓	✓	✓			✓	✓	✓		✓	✓	✓
Opt Out of Sales	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Opt Out of Sharing for Cross-Context Behavioral Advertising	✓											
Opt Out of Targeted Advertising		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Opt Out of Profiling		✓	✓			✓	✓	✓		✓	✓	✓
Appeals Process Explicitly Required		✓	✓			✓	✓	✓	✓	✓	✓	✓
Choice Regarding Sensitive Data	Opt-out / Right to limit	Opt-in	Opt-in		Opt-out	Opt-in	Opt-in	Opt-in	Opt-out	Opt-in	Opt-in	Opt-in
Assessment Requirements	TBD in Regs	✓	✓			✓	✓	✓		✓	✓	✓
Consumer Rights Apply to Pseudonymous Data	✓	Some rights	Some rights		Some rights	Some rights	Some rights	Some rights		Some rights		Some rights
Explicit Global Privacy Control Requirement	✓	✓	✓							✓		✓

VENABLE LLP

State Privacy Laws: Assessments

- **Iowa, Nevada, and Utah.** No specific reference to assessments.
- **California.** The CPPA is directed to issue regulations requiring businesses whose processing of personal information presents a significant risk to consumers' privacy or security to: (A) perform an annual cybersecurity audit; and (B) submit to the CPPA on a regular basis a risk assessment with respect to personal information processing, including whether the processing involves sensitive personal information.
- **Colorado, Connecticut, Florida, Indiana, Montana, Tennessee, Texas, and Virginia.** Requires controllers to conduct and document data protection assessments for any processing activities involving personal data that present a **heightened risk of harm**; processing personal data for purposes of **targeted advertising**; the **sale** of personal data; processing personal data for purposes of **profiling**, where such profiling presents a reasonably foreseeable risk of certain impacts, injuries, or harms; and processing **sensitive data**.
- Assessments across state laws must consider: the use of **deidentified data**, the **reasonable expectations of consumers**, the **context of the processing**, and **the relationship between the controller and the consumer**.
- Colorado, Connecticut, Florida, Indiana, Montana, Tennessee, Texas and Virginia allow a single data protection assessment to address a comparable set of processing operations that include similar activities.
- Colorado, Connecticut, Florida, Indiana, Montana, Tennessee, Texas and Virginia permit data protection assessments conducted for the purpose of compliance with other laws or regulations to be used for compliance with the state law requirements if the assessment has a reasonably comparable scope and effect.

VENABLE LLP

Sensitive Data Comparison

Data Element	CPRA	CO	CT	NV	UT	VA	FL	IN	IA	MT	TN	TX
Race or Ethnicity	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Religion	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Sexual Orientation	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	
Sexuality												✓
Sex Life	✓	✓	✓							✓		
Union Membership	✓											
Genetic or Biometric Data Used to Identify a Person	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Personal Data Concerning a Consumer's Health	✓				✓							
Mental or physical health diagnosis	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Precise Geolocation	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓
SSN, driver's license, state ID card, or passport number	✓											
Account number/login in combination with password/code	✓											
Contents of mail, email, or texts (unless business is intended recipient)	✓											
Personal data pertaining to a known child		✓	✓			✓	✓	✓	✓	✓	✓	✓
Citizenship or immigration status	TBD – CA AB 947	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓

VENABLE LLP

Florida Digital Bill of Rights

Thresholds.

- For-profit entity with global gross revenue in excess of $1 billion *and* meets at least one of the following criteria: (1) derives 50% or more of global gross revenue from online ad sales, including providing targeted advertising; (2) operates certain voice assistants; or (3) operates an app store offering at least 250,000 different apps. The definition also encompasses any entity that controls or is controlled by a controller.

Consumer Rights. *Pseudonymous data exemption for some rights.*

- Access; correction; deletion; portability; opt-outs of processing for (1) targeted advertising, (2) sales, and (3) profiling.
  - "Targeted advertising" means "displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across **affiliated** or unaffiliated websites and online applications used to predict the consumer's preferences or interests." *Note* that processing personal data solely for measuring or reporting advertising performance, reach, or frequency is exempt from the law.
- Opt-out of collection of personal data via a voice recognition feature.
- Opt-in for processing of sensitive data.
- Opt-out of collection and processing of sensitive data (revocation of consent).
- Opt-in to sales of sensitive data ***for any for-profit entity*** that conducts business in Florida and collects personal data.

Global Privacy Controls.

- No explicit requirements.

Enforcement.

- FL AG, with discretionary 45-day cure period for most alleged violations. Civil penalties may amount to $50,000 per violation, and such penalties may be tripled for certain violations (violations involving children; failure to delete or correct; continuing to sell or share after receiving an opt-out).

Regulatory Processes.

- Florida Department of Legal Affairs may issue rules (standards for authenticated rights requests, enforcement, data security, and authorized agents).

Unique Provisions.

- Requirements for online platforms likely to be "predominantly accessed" by U-18s prohibits government-directed content moderation of social media.
- If a controller engages in the sale of personal data that is sensitive data or biometric data, the controller must post the following "notices," respectively: "NOTICE: This website may sell your sensitive personal data." ***and/or*** "NOTICE: This website may sell your biometric personal data." Such notices must be posted in accordance with privacy notice requirements.
- Adds biometric data and geolocation data as data elements subject to breach notification when combined with a first name or first initial and last name.

VENABLE LLP

Indiana Consumer Data Protection Act

Thresholds.

- Controls or processes personal data of at least 100,000 Indiana consumers, excluding collection or processing solely for payment processing; *or*
- Controls or processes personal data of at least 25,000 Indiana consumers and derives more than 50% of annual gross revenue from sales of personal data.

Consumer Rights. *Pseudonymous data exemption for some rights.*

- Access, correction, deletion, and portability.
- Opt-outs of processing for (1) targeted advertising, (2) sales, and (3) profiling.

Global Privacy Controls.

- No explicit requirements.

Enforcement.

- Indiana Attorney General, with a 30-day cure period. Civil penalties may amount to $7,500 per violation.

Regulatory Processes.

- The Indiana Attorney General may publish compliance resources for controllers, such as a model privacy notice.

VENABLE LLP

Iowa Act Relating to Consumer Data Protection

Thresholds.

- Controls or processes personal data of at least 100,000 Iowa consumers, excluding collection or processing solely for payment processing; *or*
- Controls or processes personal data of at least 25,000 Iowa consumers and derives more than 50% of annual gross revenue from sales of personal data.

Consumer Rights. *Pseudonymous data exemption.*

- Access, deletion, and portability.
- Opt-out of personal data sales and targeted advertising.

Global Privacy Controls.

- No explicit requirements.

Enforcement.

- Iowa Attorney General, with 90-day cure period. Civil penalties may amount to $7,500 per violation.

Regulatory Processes.

- None.

VENABLE LLP

Montana Consumer Data Privacy Act

Thresholds.

- Controls or processes personal data of at least 50,000 Montana consumers, excluding collection or processing solely for completion of a payment transaction; *or*
- Controls or processes personal data of at least 25,000 Montana consumers and derives more than 25% of annual gross revenue from sales of personal data.

Consumer Rights. *Pseudonymous data exemption for some rights*.

- Access, correction, deletion, and portability.
- Opt-outs of processing for (1) targeted advertising, (2) sales, and (3) profiling.

Global Privacy Controls.

- Requires recognition of opt-out preference signals by January 1, 2025.

Enforcement.

- Montana Attorney General, with a 60-day cure period that sunsets on April 1, 2026.

Regulatory Processes.

- None.

VENABLE LLP

Texas Data Privacy and Security Act

Thresholds.

- Applies to persons who (1) conduct business in the state or produce a product or service consumed by residents of the state; (2) process or engage in the sale of personal data; **and** (3) are not small businesses, as defined by the U.S. Small Business Administration (subject to certain exceptions, including the exception related to sensitive data sales, as noted below).

Consumer Rights. *Pseudonymous data exemption for some rights.*

- Access, correction, deletion, and portability.
- Opt-outs of processing for (1) sales, (2) targeted advertising, and (3) profiling.

Global Privacy Controls.

- A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of personal data for sales or targeted advertising. A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

Enforcement.

- Texas Attorney General, with 30-day cure period. Civil penalties may amount to $7,500 per violation.

Unique Considerations.

- Small businesses must obtain consent to engage in the sale of sensitive data.
- Texas Attorney General must post an online mechanism through which a consumer may submit a complaint and information related to the responsibilities of controllers and processors under the law.
- If a controller engages in the sale of personal data that is sensitive data or biometric data, the controller must post the following "notices," respectively: "NOTICE: We may sell your sensitive personal data." ***and/or*** "NOTICE: We may sell your biometric personal data." Such notices must be posted in the same location and in the same manner as the privacy notice.

Regulatory Processes.

- None.

VENABLE LLP

Tennessee Information Protection Act

Thresholds.

- Annual revenue of more than $25 million *and* (1) controls or processes personal information of at least 25,000 Tennessee consumers and derives more than 50% of annual gross revenue from sales of personal information; or (2) annually controls or processes personal information of at least 175,000 Tennessee consumers.

Consumer Rights. *Pseudonymous data exemption*.

- Access, correction, deletion, and portability.
- Opt-outs of processing for (1) sales, (2) targeted advertising, and (3) profiling.

Global Privacy Controls.

- No explicit requirements.

Enforcement.

- Tennessee Attorney General and Reporter, with 60-day cure period. Civil penalties may amount to $7,500 per violation, with treble damages available for willful or knowing violations.

Unique Considerations.

- Creates an affirmative defense for controllers and processors that implement a privacy program that conforms to the NIST Privacy Framework.

Regulatory Processes.

- None.

VENABLE LLP

Spotlight on Tennessee

TIPA's First-of-Its-Kind Affirmative Defense

VENABLE LLP

TIPA + The NIST Privacy Framework = Affirmative Defense

TIPA creates a **first-of-its-kind affirmative defense** for controllers and processors. Specifically, the law provides controllers and processors that implement written privacy programs in reasonable conformance to the NIST Privacy Framework an affirmative defense in TIPA actions.

To qualify for the affirmative defense, entities must:

1. Create, maintain, and comply with a written privacy program;
2. Design this program in reasonable conformity to the **NIST Privacy Framework**;
3. In doing so, take into account the size and complexity of the business, the nature and scope of processing activities, the sensitivity of personal information processed, the cost and availability of tools for improvement, and compliance with comparable state or federal laws;
4. Provide consumers the rights granted by TIPA; and
5. Update this privacy program within two years of publication of future updates to the NIST Privacy Framework.

VENABLE LLP

Benefits of a Comprehensive Assessment Using the NIST Privacy Framework

Future-proofing products and services while fulfilling compliance obligations.

Gain important insights by considering a different perspective.

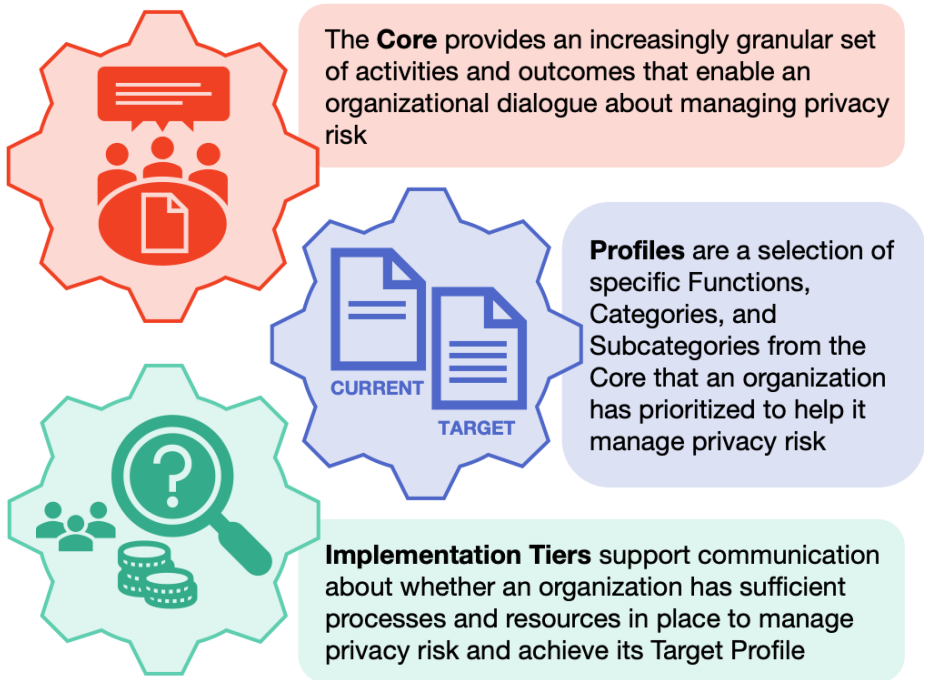
Increase trust by partners, customers, and other key stakeholders.

Strengthen accountability through current and target profiles.

VENABLE LLP

NIST Privacy Framework

A flexible, outcome-based voluntary tool intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy.



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk

Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

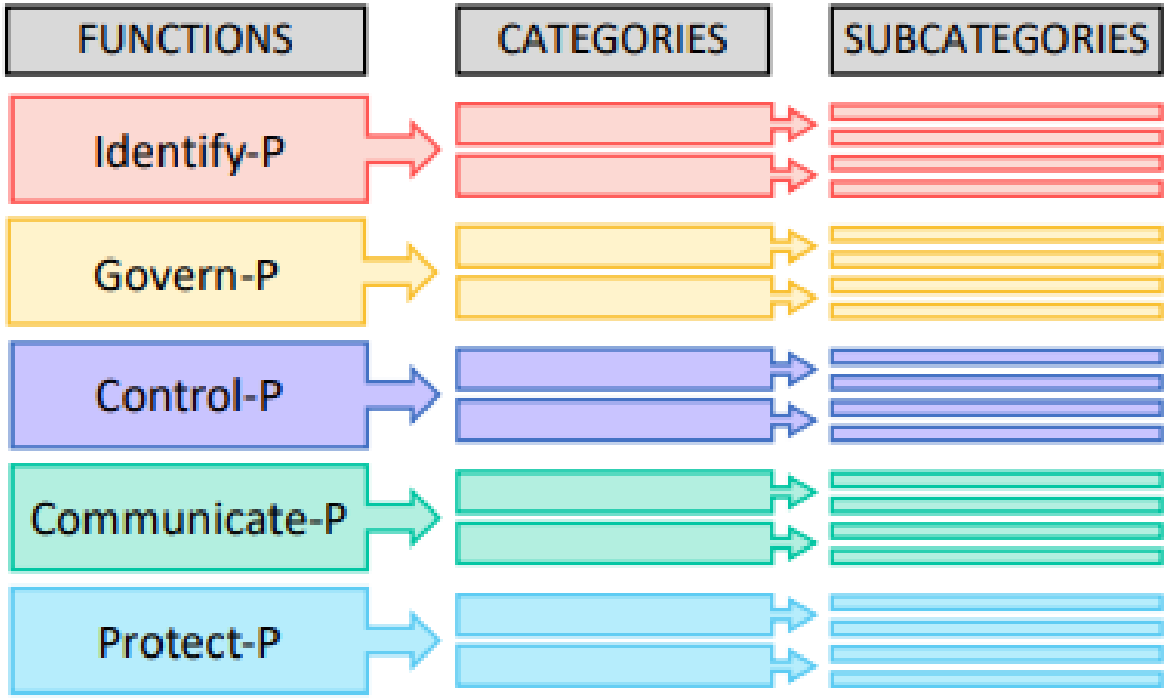
Uses of the Privacy Framework

- Establish a new privacy program
- Improve an existing privacy program
- Build privacy into products and services
- Support compliance activities and easily adapt to new or changing privacy requirements
- Be proactive about privacy risk
- Strengthen accountability, collaboration, and communication
- Establish privacy as a differentiator

VENABLE LLP

The NIST Privacy Framework Core

The NIST Privacy Framework Core consists of five **Functions**, which are further broken down into **Categories** and detailed **Subcategories** that describe programmatic needs and activities.



VENABLE LLP

Sample Subcategory of the NIST Privacy Framework

FUNCTIONS	CATEGORIES	SUBCATEGORIES
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1**
		GV.PO-P2
		GV.PO-P3
		GV.PO-P4
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		GV.PO-P6
	Risk Management Strategy (GV.RM-P)	
	Awareness and Training (GV.AT-P)	
	Monitoring and Review (GV.MT-P)	

VENABLE LLP

Sample Subcategory of the NIST Privacy Framework

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P)**	
	Risk Management Strategy (GV.RM-P)	
	Awareness and Training (GV.AT-P)	
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1**
		GV.MT-P2
		GV.MT-P3
		GV.MT-P4
		GV.MT-P5
		GV.MT-P6
		GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.

NIST Privacy Framework Assessment Approach

Project Initiation

Meet with our team to establish a project plan, schedule interviews and workshops, share key artifacts, and discuss the assessment process.

Document Review

Establish a baseline understanding of your privacy program and its alignment with the NIST Privacy Framework.

Interviews and Workshops

Deepen knowledge and consider potential areas for growth through conversations with privacy, legal, and other relevant stakeholders.

Analysis

Define privacy program goals, evaluate current and target profiles, and identify gaps and areas for alignment.

VENABLE LLP

Assessment Results

Targeted Findings

Establish a baseline of your privacy program and build upon its foundation and strengths.

Tailored Recommendations

Our team of trusted experts will provide recommendations designed to meet your needs.

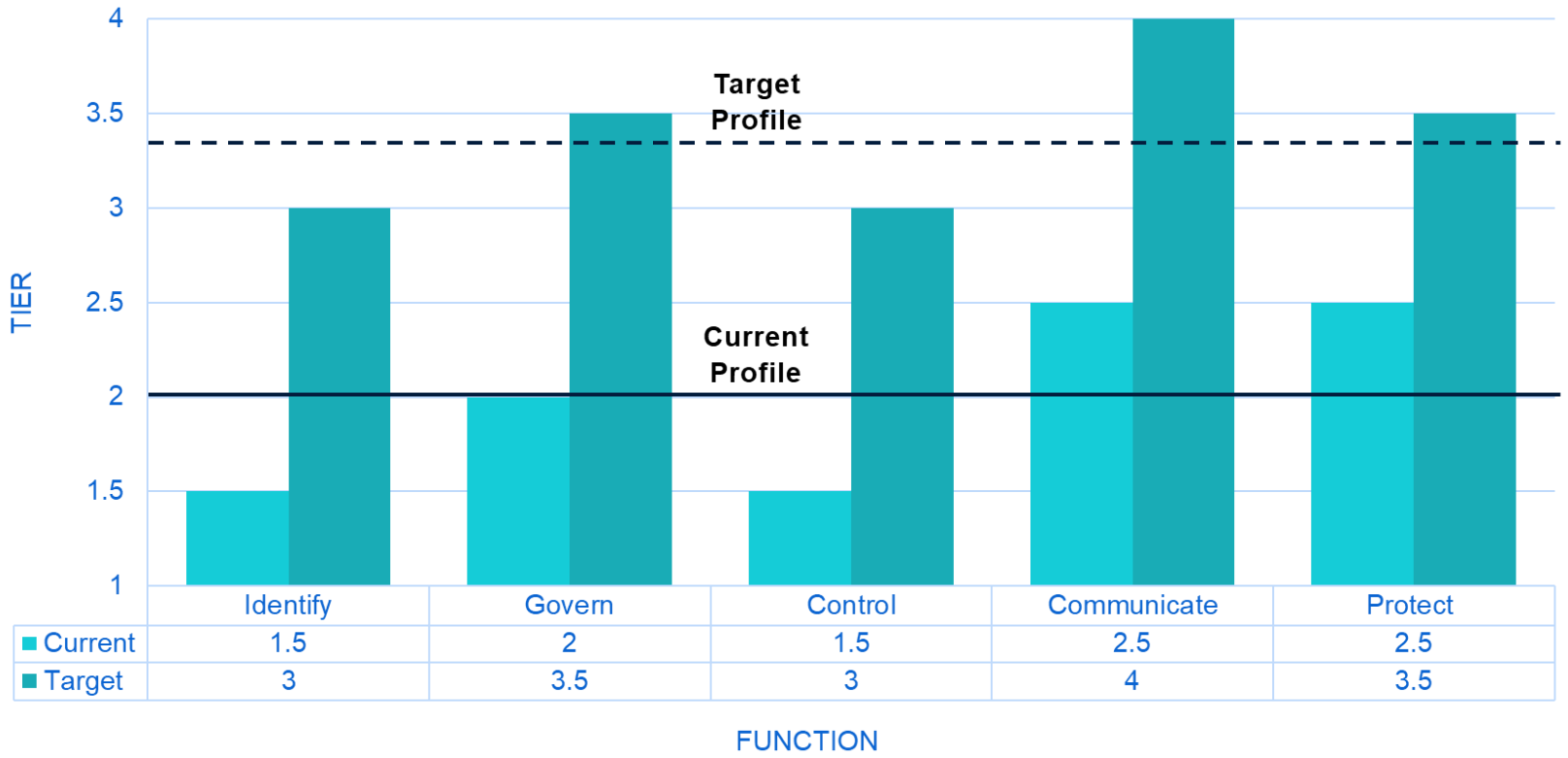
Roadmap

A best-in-class implementation plan will empower your team to grow, mature, and achieve its goals.

VENABLE LLP

Sample Current and Target Profiles

Targeted Findings establish a baseline of your privacy program to inform your **current profile** and establish strategic objectives represented by your **target profile**.



	Identify	Govern	Control	Communicate	Protect
Current	1.5	2	1.5	2.5	2.5
Target	3	3.5	3	4	3.5

VENABLE LLP

VENABLE LLP