Mid-Year Privacy Check-up

Privacy Data Security Law Updates & Using Assessments to Keep Your Privacy Program Healthy

May 30, 2024

Kelly DeMarchis Bastide
Partner and Co-chair, Privacy and Data Security Group

Ivy D. Orecchio
Project Manager, Cybersecurity and Privacy Services

Jamie Danker
Senior Director, Cybersecurity and Privacy Services

VENABLE LLP

Speakers

Kelly DeMarchis Bastide

Partner and Co-chair
Privacy and Data Security Group

Jamie M. Danker

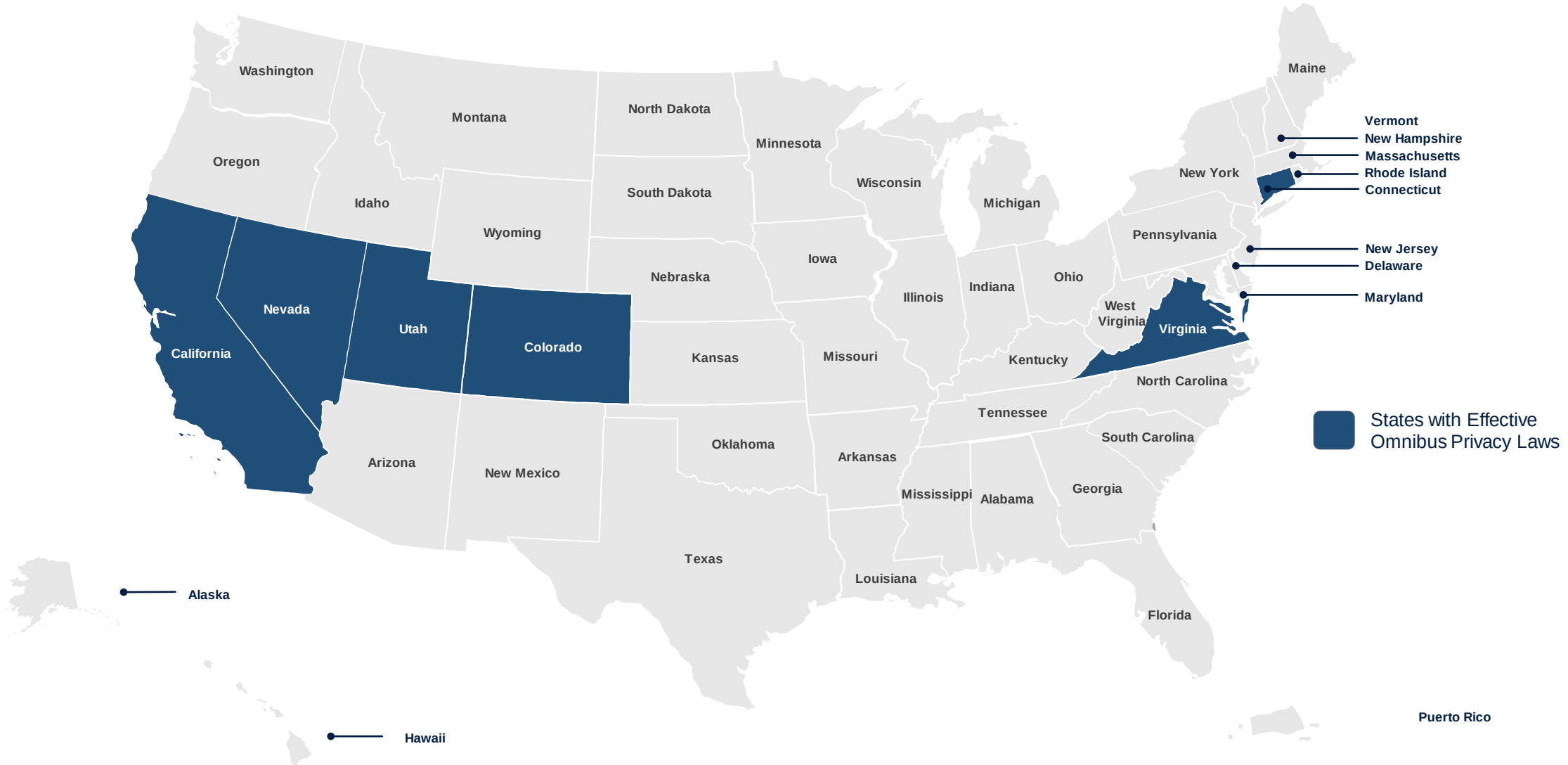
Senior Director
Cybersecurity and Privacy Services

Ivy D. Orecchio

Project Manager
Cybersecurity and Privacy Services

VENABLE LLP

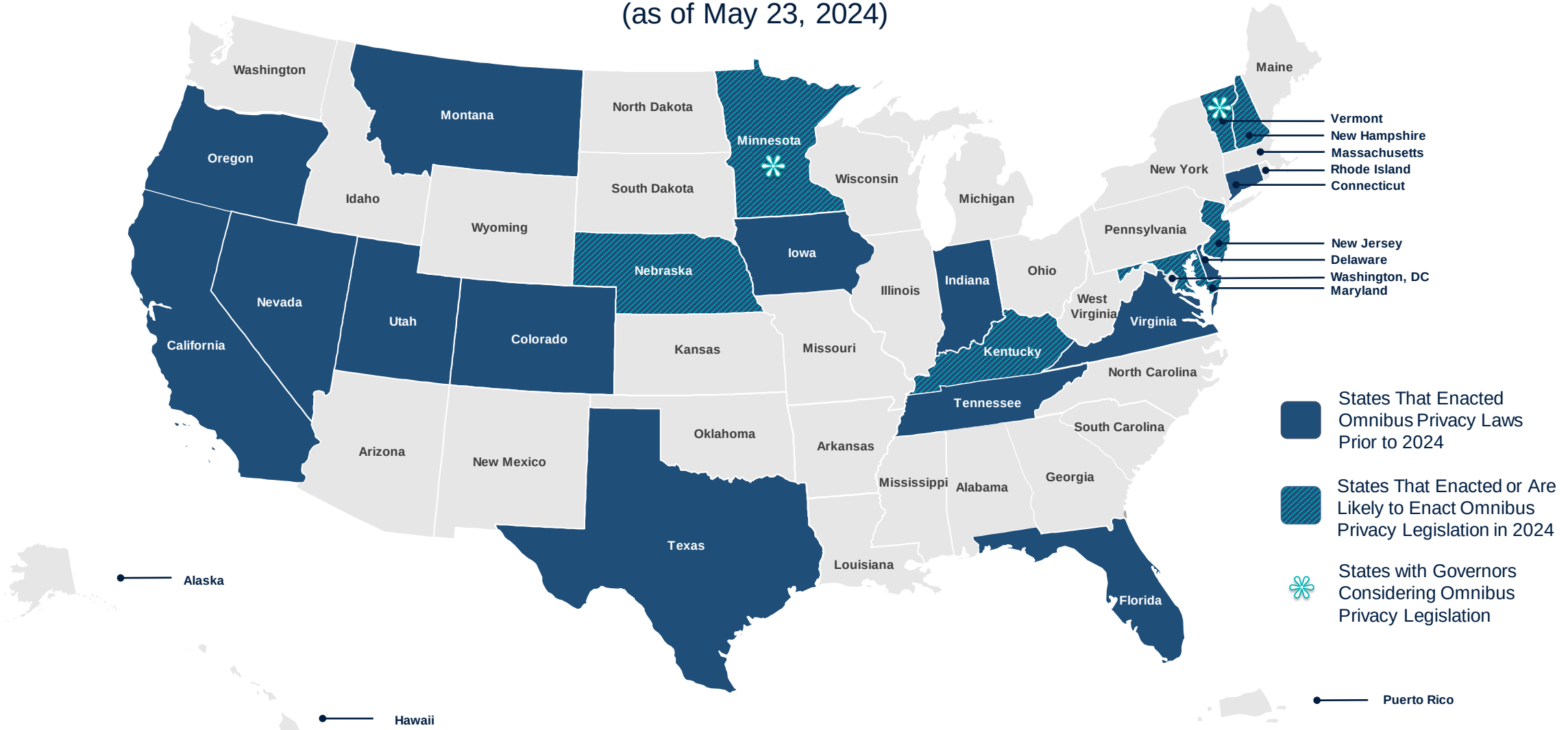
U.S. Privacy Landscape – One Year Ago



VENABLE LLP

Enacted Omnibus State Privacy Laws

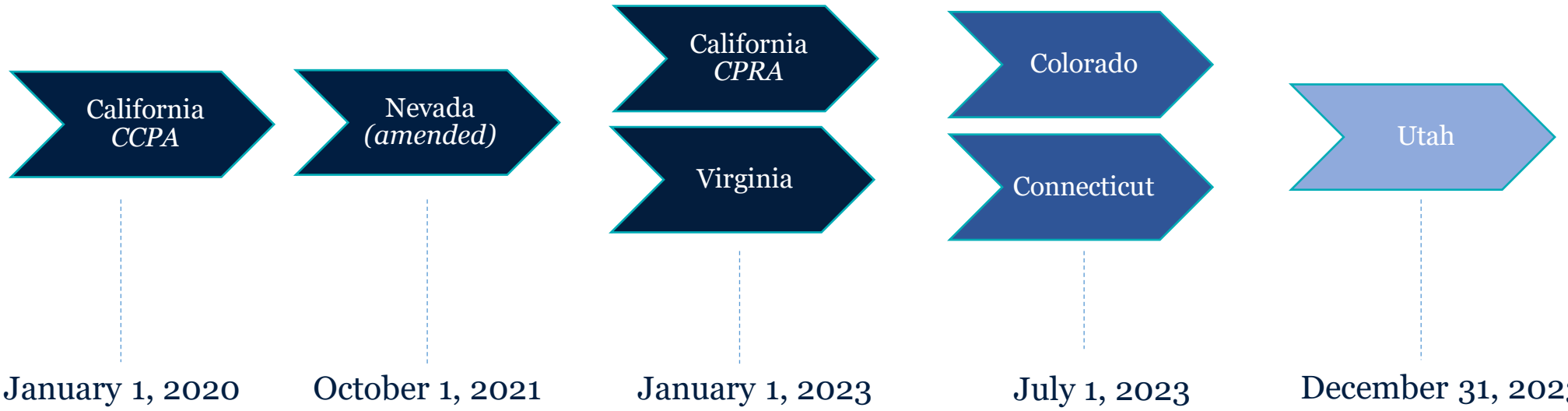
(as of May 23, 2024)



VENABLE LLP

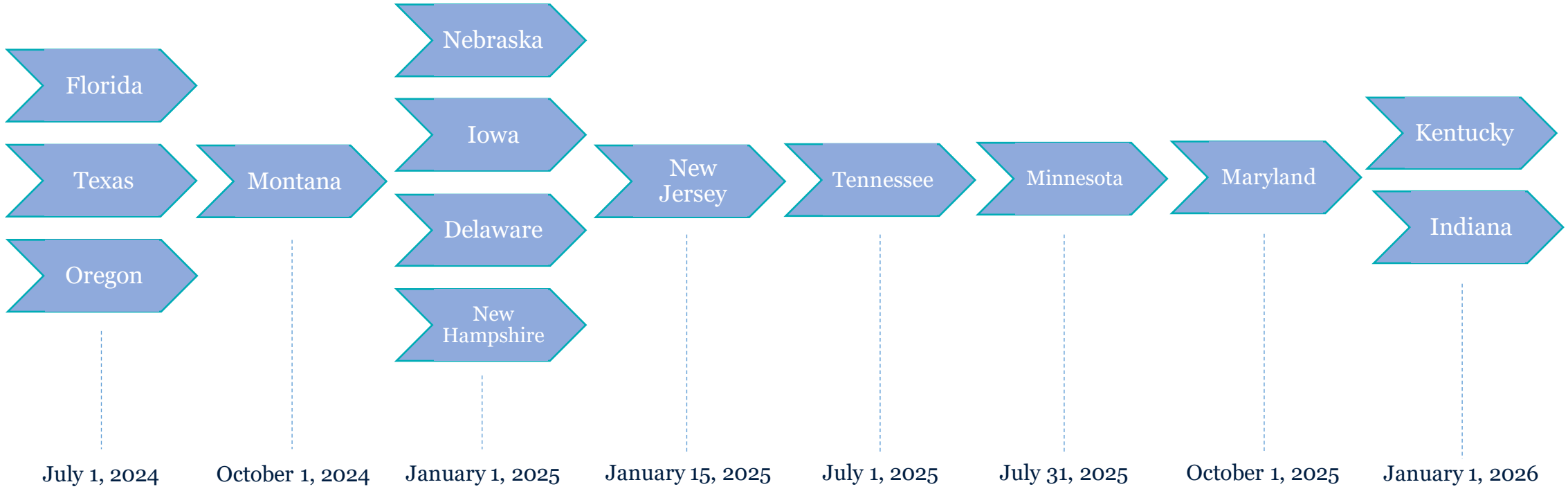
Timeline

State Privacy Laws: Currently in Effect



VENABLE LLP

Timeline
Laws Coming Into Effect



VENABLE LLP

Omnibus State Privacy Laws at a Glance

	CA	CO	CT	NV	UT	VA	DE	FL	IN	IA	MT	OR	TN	TX	NJ	NH
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-in	Opt-out	Opt-in	Opt-in	Opt-in	Opt-in	Opt-in	Opt-in
Assessment Requirements	TBD in Regs	✓	✓			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Consumer Rights Apply to Pseudonymous Data	✓	Some rights	Some rights	No explicit statement	Some rights	Some rights	Some rights	Some rights	Some rights		Some rights	✓		Some rights	✓	Some rights
Explicit Global Privacy Control Requirement	✓	✓	✓				✓				✓	✓		✓	✓	✓

VENABLE LLP

Making Sense of State Omnibus Privacy Laws

- California remains the most prescriptive and detailed. Regulations go beyond statutory language in certain respects. Anomalous features include:
  - Coverage of personnel and B2B data
  - No exceptions for pseudonymous data
  - Opt-out of "sharing" for targeted advertising but not mere processing (more on this later)
- Colorado also has detailed regulations.
- A few laws are more limited in scope:
  - Nevada is limited to opting out of sales.
  - Florida applies mainly to tech titans, with only sensitive data provisions applying to other companies.
  - Texas law appears to exempt pseudonymous data fully unless mixed with identifiable data.
- Most other laws follow a common pattern, with more limited variations on the theme. BUT variations are increasing as states pass "special issue" privacy laws – more on this later!

VENABLE LLP

State Privacy Laws Hygiene

- New state privacy law requirements go into effect (roughly) biannually—January 1 and July 1. Create an annual cadence for review of **privacy policy, contract clauses, consumer rights requests, and approach to sensitive data** to validate whether existing approaches work for forthcoming laws.
  - NOTE: Significant changes will not be needed to address changes in law in 2024-2025 (as of today). That trend seems to be holding, for now.
  - Privacy policy must be updated annually, at a minimum, for CCPA statistical reporting.
- **Conduct or refresh data protection assessments where required** – Most of the new state laws require a company to **conduct and document data protection assessments** when it processes personal data for targeted advertising, sells personal information, or processes "sensitive" data as defined by these laws.
- Schedule more frequent **privacy "working group" sessions** to stay proactive on the more dynamic aspects of these laws and the desired approach of the business.

State Law Enforcement Overview

- State omnibus privacy laws generally provide for regulatory enforcement. Money penalties are possible, but these laws do not **yet** authorize class action lawsuits.
- States other than California currently provide for cure periods in advance of bringing enforcement.
  - Some of these cure period provisions will sunset in future years.
- California has been active in enforcing its omnibus privacy law — other states, not so much!
  - California is following up with companies on consumer complaints and proactively investigating potential violations.
  - Connecticut has focused on privacy policies and is interested in sensitive data, teen data, and data brokers. Cure notices and inquiry letters sent to app developers, grocery stores, genetic testing companies, and car manufacturers.
  - Texas has begun enforcing its data broker registry.

VENABLE LLP

State Laws Effective in 2024

- **4 new state laws** will go into effect by the end of the year
  - July 1: Florida, Oregon, Texas
    - Texas applies broadly to businesses that do not qualify as “small businesses”
    - Oregon applies to nonprofits
    - Certain sensitive data requirements apply to any business that collects personal data about Florida consumers
  - October 1: Montana

- **Key Provisions**
  - Right to obtain a list of specific third parties (OR)
  - New categories of sensitive data (e.g., national origin, status as transgender or nonbinary, status as a victim of a crime) (OR)
  - Specific notice relating to sensitive or biometric data sales (FL, TX)
  - Universal opt-out mechanism obligations beginning Jan. 1, 2025 (MT, TX)

VENABLE LLP

Spotlight on State Health Data Laws

- New laws in **Washington**, **Connecticut**, and **Nevada** regulate the collection, use, and disclosure of "consumer health data," though the laws define this term differently.
  - In **Connecticut** and **Nevada**, definitions of consumer health data are focused on personal information that an entity **"uses to identify"** a consumer's health condition or diagnosis (CT) or health status (NV).
  - **Washington** defines consumer health data more broadly to include any information that is linked or reasonably linkable to a consumer and identifies health status.
    - For purposes of the WA law, it does not matter how a company "uses" consumer health data. If the company collects such data, it will be subject to the law.

- In addition to being the broadest of these laws, **Washington's "My Health, My Data Act"** poses the most risk due to its **private right of action** (in addition to enforcement by the state attorney general). Significant enforcement is therefore expected.

- Other states are also moving to regulate geofencing around health-related locations.

VENABLE LLP

Washington: "My Health My Data" Law

- 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. **Written authorization is required for sales**.
- Requires a **consumer health data privacy policy** that makes certain disclosures, to include a list of affiliates with which consumer health data is shared.
- 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."
  - Includes procedures, interventions, medication, bodily functions, geolocation data.
  - Includes data derived or extrapolated from non-health data.
- 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 and affiliates** with which health data has been shared or to which it has been sold and an active online mechanism to contact such entities.
  - The right of deletion includes a flow-down requirement to third parties and affiliates.
- Bars geofencing around entities that provide in-person healthcare services where the geofence is used to (1) identify or track consumers seeking healthcare services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or healthcare services.
- **Effective on July 23, 2023,** and provisions related to geofencing take effect on that date; other operative took effect on **March 31, 2024** for regulated entities and **June 30, 2024** for small businesses.

VENABLE LLP

Why Every Organization Should Examine Its Privacy Health

Potential Fines

Customer Trust

Innovation

Future-Proofing

VENABLE LLP

Privacy Peace of Mind Starts with Regular Check-ups….

Let's Assess Your Privacy Health!

VENABLE LLP

Types of Assessments

- Legally Required
- Programmatic Assessments
- Other Ways to Check Your Health

VENABLE LLP

GDPR and DPIAs

A Data Protection Impact Assessment (DPIA) is required under Art. 35 of the GDPR anytime you begin a new project that is likely to involve “a high risk” to other people’s personal information.

WP 29 DPIA Criteria (aka “DPIA Triggers”)

- Evaluation and Scoring
- Automated Decision Making
- Systematic Monitoring
- Sensitive Data
- Large Scale
- Matching or Combining Datasets
- Data of Vulnerable Subjects
- Use of New/Innovative Solutions
- Cross-border Data Transfers
- Preventing Individuals from Exercising a Right/ Executing a Contract

VENABLE LLP

State Privacy Laws and Privacy Impact Assessments

Generally required when:

- processing sensitive data*
- selling personal data
- targeting advertising

PIAs should be documented and updated to reflect changes

VENABLE LLP

Programmatic Assessments

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 with the NIST Privacy Framework an affirmative defense in TIPA actions.

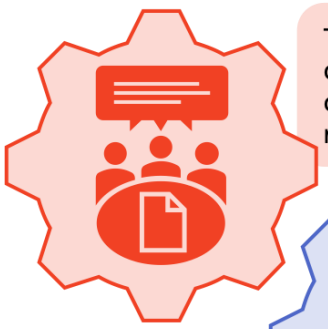
To qualify for the affirmative defense, entities must:

1. Create, maintain, and comply with a written privacy program;
2. Design this program in reasonable conformity with the **NIST Privacy Framework**;
3. Disclose the commercial purpose for which personal information is collected, controlled, or processed;
4. Provide consumers the rights granted by TIPA; and
5. Update this privacy program not later than one year after publication of future updates to the NIST Privacy Framework.

VENABLE LLP

Programmatic Assessment - 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

NIST Privacy Framework Functions

Identify-P	Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
Govern-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.
Control-P	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
Communicate-P	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.
Protect-P	Develop and implement appropriate data processing safeguards.

VENABLE LLP

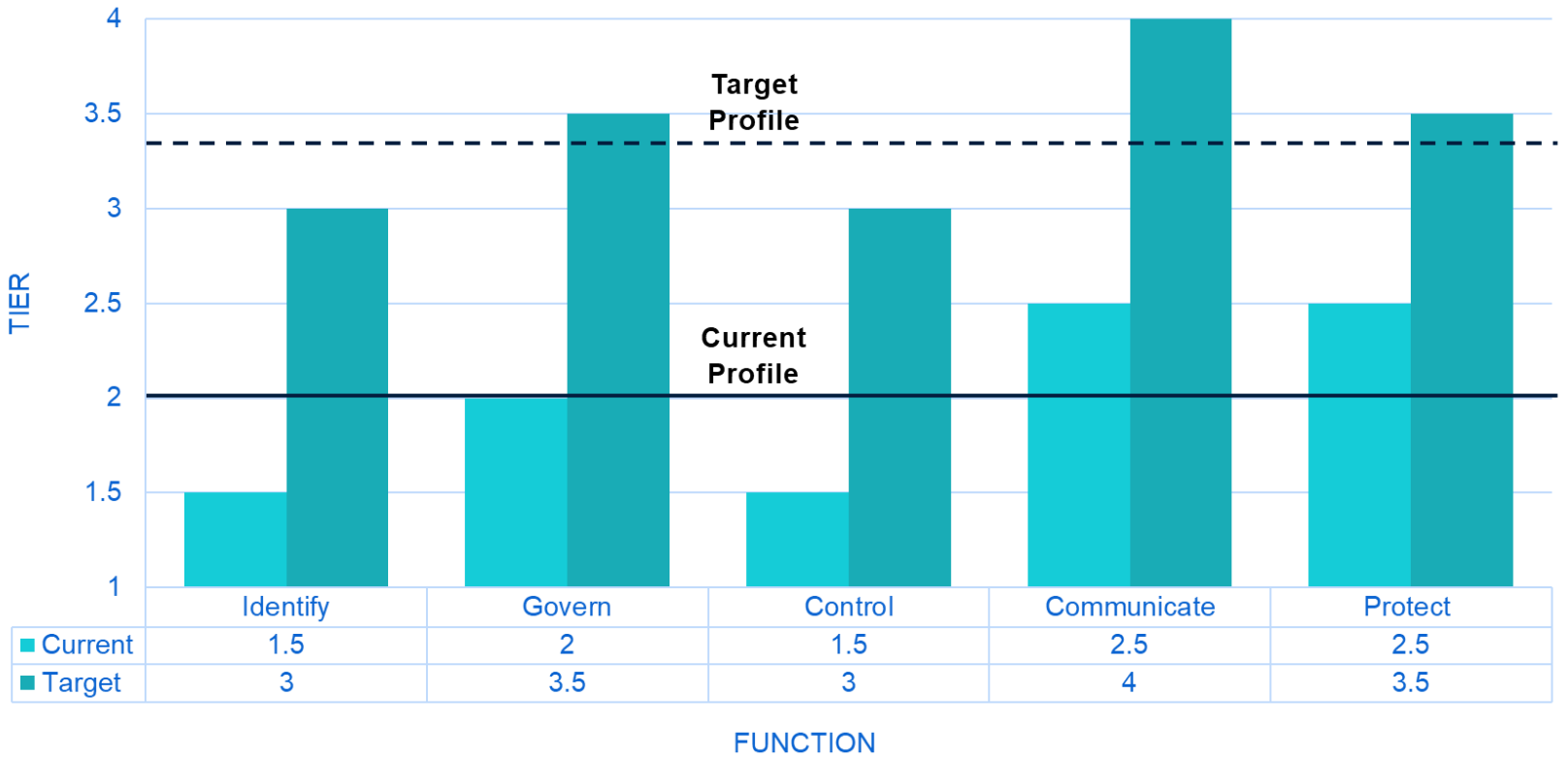
Legal Compliance Relationship to the NIST Privacy Framework

Function	Category	Subcategory
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

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**.



VENABLE LLP

Other Types of Assessments

Staying in Shape – Other Helpful Tools

VENABLE LLP

Staying in Shape – Other Helpful Tools


FICTIONAL MEDICAL
Healthcare Service

MEDICAL FORM

PERSONAL INFORMATION

Full Name : (PLEASE USE CAPITAL)

Place Of Birth : / / Gender : Male Female

Address :

Phone Number : E-Mail :

ID Number : Social Security Number :

Status : Single Married Divorce Others

Occupation : Are You A Retiree ? : Yes No

This space is where you can share notes

Note :

HEALTH HISTORY

Allergies
Diabetes
Skin Irritation
Skin Inflammation
Arthritis
Blood Born Disease
Broken Skin
Hemophilia
Recent Surgery
Swelling
Athletes foot
Calluses
Nail Infection
Corns

OTHER RISKS

More Information :
123 Anywhere St., Any City, ST 12345
+123-456-7890 (Office)
www.reallygreatsite.com

THANK YOU

Privacy Threshold Assessment (PTA)

A Privacy Threshold Assessment (PTA) is a high-level evaluation of a process, system, or technology to identify potential privacy risks and determine whether additional reviews, such as Data Protection Impact Assessments (DPIAs) or Privacy Impact Assessments (PIAs), may be needed.

These reviews are not as in-depth as a DPIA or PIA and can help a team prioritize their efforts and allocate resources efficiently.

VENABLE LLP

Staying in Shape – Other Helpful Tools

Targeted Assessments

Rather than looking enterprise-wide, you can improve privacy in a specific area of your business (i.e., within a specific business unit or function).

- **State Data Privacy Law Assessments** – Until Congress passes a national, preemptive data privacy law, the market will only become more complex as additional state laws go into effect. This type of assessment looks at your compliance readiness with regard to state data privacy laws and provides remediation plans.
- **Sectoral/Industry Assessments** – COPPA (children), BIPA (biometric), and the HIPAA rule (and other consumer health data regulations) are some of the more common specifically tailored and focused assessments we perform. These may apply to your business if you collect information from children, if you are a covered entity or business associate under HIPAA, or if you collect and store biometric data about customers or employees.

Testing Your Procedures

Assess and remediate potential privacy problems by reviewing the procedures in place (e.g., DSAR Request Response Times, privacy complaints).

VENABLE LLP

Staying in Shape – Other Helpful Tools

	Function	Category
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.

Data Map

A data map is a visual representation of how an organization collects, uses, stores, and processes personal data.

- Asset overview with insight into specific systems, programs, and technologies
- Improved understanding of data flows, including data sources, internal and external recipients, and service providers that may handle personal data on your behalf.
- Leverage the data map to improve data governance

VENABLE LLP

How Assessments Help Your Business

Skincare Company

A company that sells skincare products specially formulated for individuals with allergies and other skin conditions is looking to expand its business offerings. While a prescription is not required to purchase its products, many of its customers are under the care of a dermatologist. The company sells products to U.S. consumers in all 50 states and has physical stores in New York, Chicago, Miami, Nashville, Las Vegas, San Francisco, and Seattle.

It maintains three websites that are used to sell products and educate potential consumers about various skin conditions.

VENABLE LLP

Privacy Check-up

Conduct a PTA/PIA to understand the privacy risks of each system/website.

Conduct a data mapping exercise (and keep the data map up to date) to better understand the data and how it flows into, through, and out of the organization.

VENABLE LLP

Data Inventory
May 2024

System Name	**Personal identifiers**	Name	Email	Phone	Address	Date of birth	Alias (i.e., Social media profile screen names)	**Online identifiers**	Device identifiers	IP address	Account name (eg., usernames, login info)	Third-party cookies	**Financial information**	Bank Account	Credit/Debit Cards	**Demographics**	Sex/gender	Race or ethnicity	Religion	Marital status	Age	Household info (e.g., number of people/children in household)	Language	**Health information**	Health conditions or health status	Medical history	Allergies	**Commercial information**	Records of products or services purchased	Records of products or services considered	Other purchasing or consuming histories or tendencies	Source awareness (i.e., how did you hear about our products?)	**Internet activity**	Browsing/search history	Information regarding interactions with online properties or emails	**Biometric Information**	Voice prints	Facial scans	Fingerprints	**Audio/visual data**	Images	Video	Voice recordings	**Other**	Consumer feedback	Consumer complaints	Comments on website content (e.g., product reviews, blog comments)
CRM	**Y**	Y	Y		Y			**Y**			Y											Y																					**Y**	Y	Y	Y
Social Media Planner	**Y**	Y	Y	Y	Y		Y	**Y**			Y																																	**Y**			
Marketing System	**Y**	Y	Y	Y	Y										**Y**	Y	Y	Y	Y	Y			**Y**	Y	Y	Y													**Y**				Y	**Y**	Y	Y	
Email marketing generator	**Y**		Y			Y																										**Y**		Y					**Y**					**Y**			
eCommerce platform	**Y**	Y	Y	Y	Y	Y		**Y**			Y												**Y**	Y		Y	**Y**	Y		Y		**Y**		Y														
Brand website								**Y**	Y	Y		Y																				Y	**Y**	Y	Y							**Y**	Y	Y			**Y**	Y	Y	Y
eCommerce website	**Y**	Y	Y	Y	Y	Y	Y	**Y**	Y	Y	Y	Y	**Y**		Y		Y				Y		Y	**Y**	Y		Y	**Y**	Y	Y	Y	Y	**Y**	Y	Y	**Y**		Y		**Y**	Y	Y		**Y**	Y	Y	Y

High-level categories of data
Data elements included in the data map template

Y = Yes, the system contains this type of consumer personal data.

VENABLE LLP

Privacy Check-up

Conduct a PTA/PIA to understand the privacy risks of each system/website.

Conduct a data mapping exercise to better understand the data and how it flows into, through, and out of the organization.

Talk to legal counsel about specific legal compliance risks.

VENABLE LLP

Thank you!

To learn more, please visit—

- **Privacy Assessments**: https://www.venable.com/services/practices/privacy-and-data-security/managed-privacy-services/privacy-assessments
- **Privacy Program Implementation and Support**: https://www.venable.com/services/practices/privacy-and-data-security/managed-privacy-services/privacy-program-implementation-and-support
- **Managed Privacy Services**: https://www.venable.com/services/practices/privacy-and-data-security/managed-privacy-services

VENABLE LLP

VENABLE LLP