Privacy Developments at the State and Federal Levels

…for those who can't spend all of their time on privacy

Kelly DeMarchis Bastide
Partner | 202.344.4722 | KABastide@Venable.com

Erik C. Jones
Partner | 312.820.3411 | ECJones@Venable.com

Julia Tama
Partner | 202.344.4738 | JKTama@Venable.com

VENABLE LLP

Speakers

Kelly DeMarchis Bastide

Erik C. Jones

Julia Kernochan Tama

VENABLE LLP

Agenda

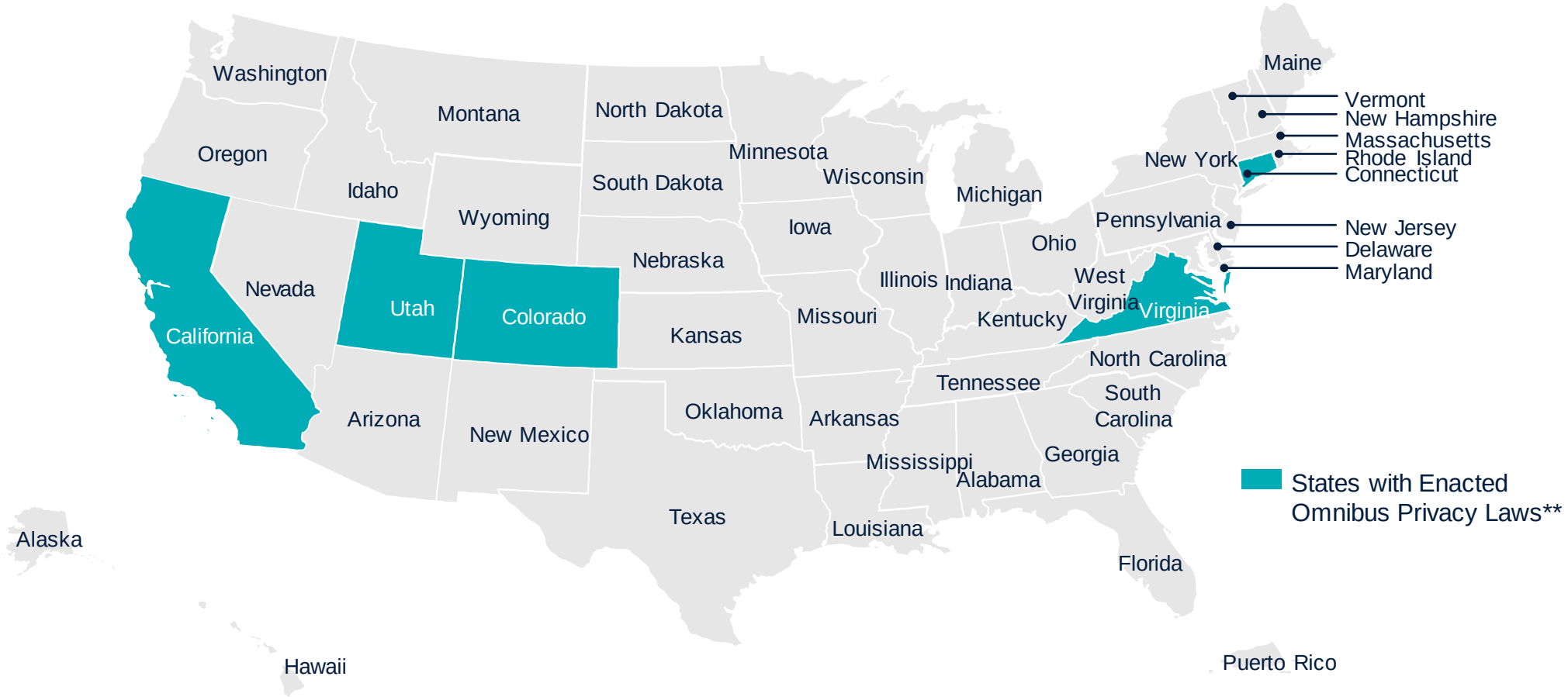
- Overview of State Developments
- Key Distinctions Between the States
- Tackling State Law Compliance
- Enforcement at the State Level
- Developments at the Federal Trade Commission
- EU-U.S. Data Privacy Framework

VENABLE LLP

Overview of State Developments

VENABLE LLP

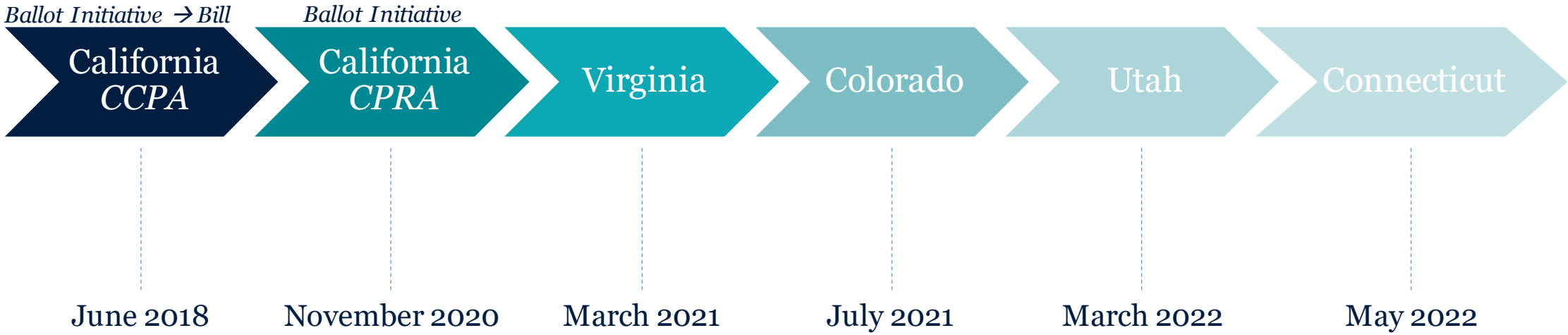
State Privacy Laws



**Nevada passed a law addressing the right to opt out of sales. Maine also passed a privacy law that is applicable to broadband Internet service providers.

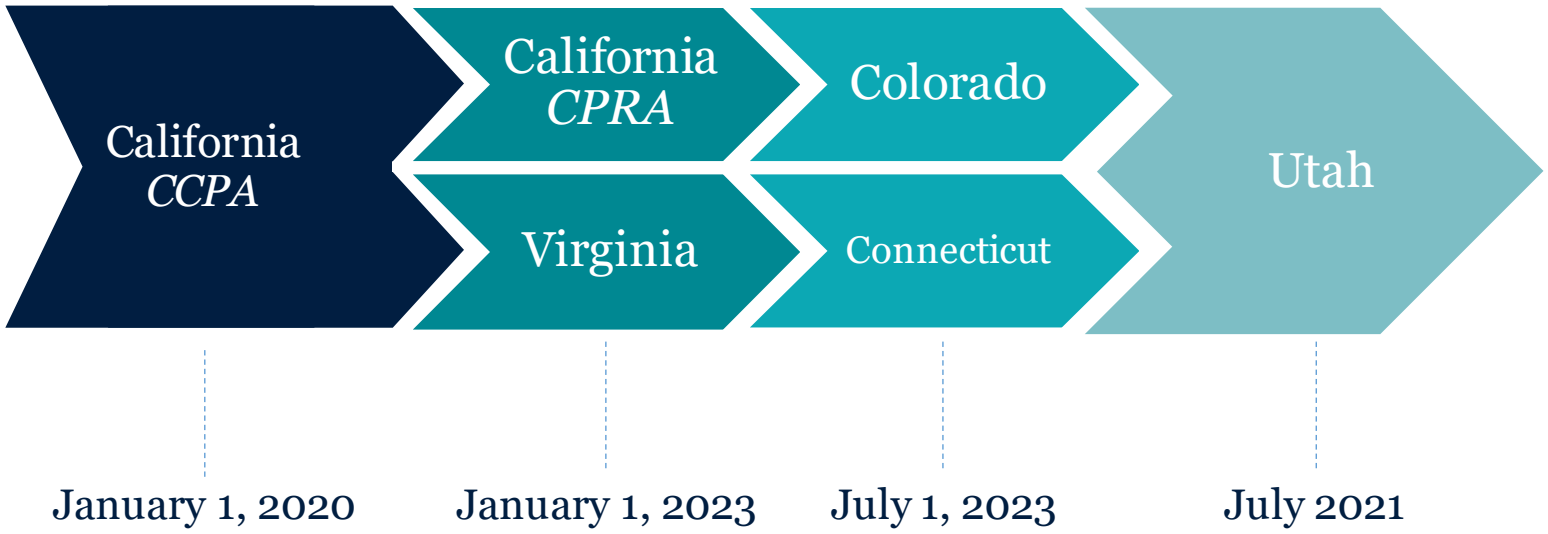
VENABLE LLP

Timeline
Bills Are Passed / Ballot Initiatives Are Approved



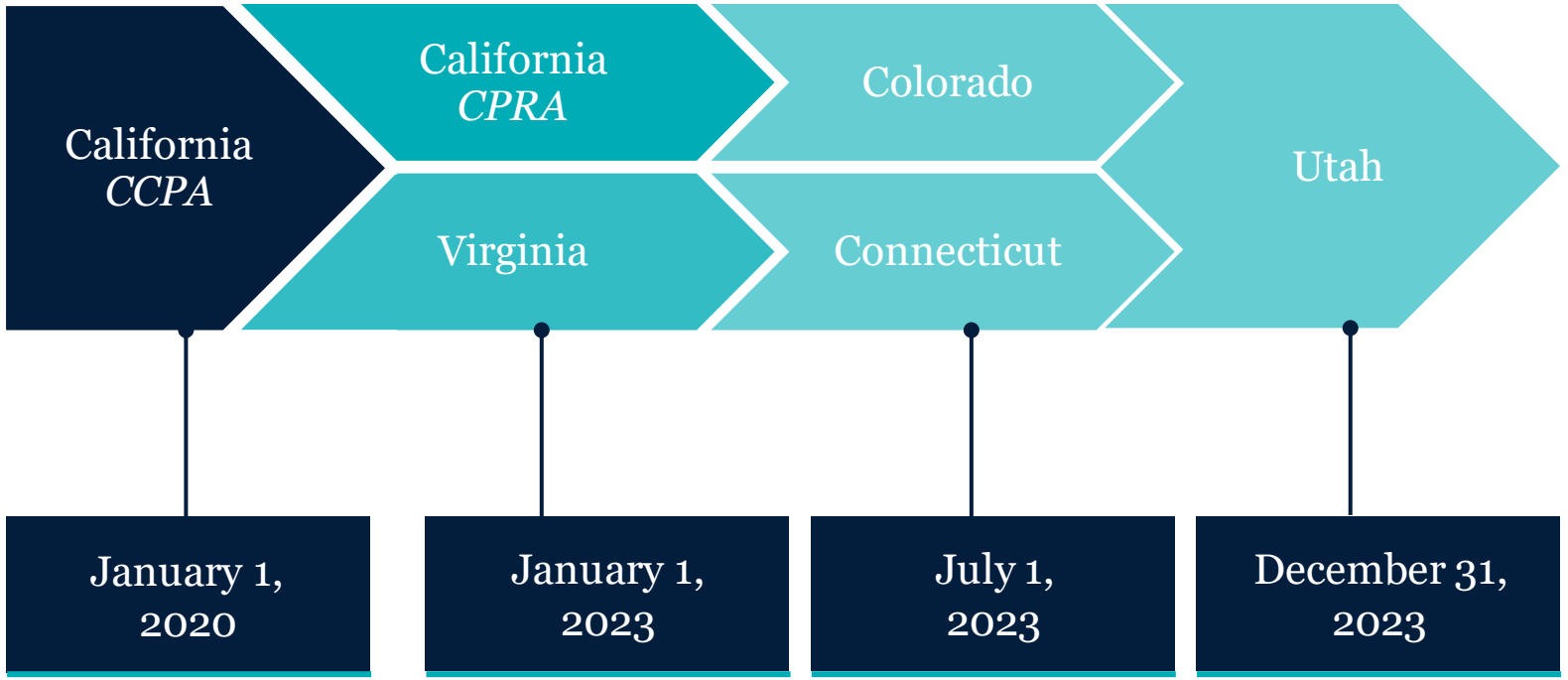
VENABLE LLP

Timeline
Laws Are Effective / Operative



VENABLE LLP

Timeline
Laws Are Effective / Operative



VENABLE LLP

Key Distinctions Between the States

VENABLE LLP

State Privacy Law Differences: Consumer Rights

	CPRA	VA	CO	CT	UT
Access	✓	✓	✓	✓	✓
Deletion	✓	✓	✓	✓	✓
Correction	✓	✓	✓	✓	
Opt Out of Sales	✓	✓	✓	✓	✓
Opt Out of "Sharing" for Targeted Advertising	✓				
Opt Out of Processing for Targeted Advertising		✓	✓	✓	✓
Opt Out of Profiling		✓	✓	✓	
Appeals Process Explicitly Required		✓	✓	✓	
Consumer Rights Apply to Pseudonymous Data	✓	Only rights to opt out	Only rights to opt out	Only rights to opt out	Only rights to opt out
Explicit Global Privacy Control Requirement	TBD		✓	✓	

VENABLE LLP

Tackling State Law Compliance

VENABLE LLP

Steps to Compliance

- **Data mapping**
- **Legal gap assessment**
- **Policies and notices**
- **Contracts (inbound and outbound data)**
- **Sensitive data**
- **California personnel and B2B data**
- **Consumer rights requests**

VENABLE LLP

Analysis and Assessment

- **Update or create a data map** – Not required, but it will make other compliance steps easier.
- **Conduct a legal gap analysis** – Review your **existing privacy program against the new laws** to identify potential gaps and open legal questions and **develop an implementation strategy**.
  - **Certain data and organizations** not previously governed by the CCPA are **now covered** by other state laws (e.g., nonprofits, employee data).
  - Take advantage of **available exemptions**.
- **Decide on geographic scope** – Determine whether your organization will apply changes nationwide, and where to take a different approach based on state laws.
  - Look for opportunities to **keep practices uniform where possible**. The laws are all different but have common elements.

Analysis and Assessment

- **During gap analysis, identify items requiring engineering and development work** – Your organization may need **new technical tools** to comply with the state laws, and this takes time.
  - The **CPRA** requires **new website links** to allow consumers to exercise their rights, including one titled "Do Not Sell or Share My Personal Information."
  - **Colorado's law** will require **adherence to opt-out signals** communicated by global privacy controls.
- **Conduct data protection assessments where required** – Some of the new state laws will 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.

Policies and Contracts

- **Start with compliance steps that are externally visible and take time.**
- **Review your contracts –** The new state laws all establish **contractual requirements** related to "service providers" or "processors."
  - Assess what updates to existing contracts and templates are needed and consider preparing contracting checklists to comply with these new requirements.
- **Prepare to update your privacy notices –** Each new state law will require "controllers" or "businesses" to include **specific information in a privacy policy**.
  - At minimum, your organization's privacy policy will likely require changes to describe the new rights available to consumers.

VENABLE LLP

Data Restrictions

- **Prepare for sensitive personal data requirements** – The new state laws all place restrictions on processing sensitive personal data **but differ on which data types are considered "sensitive"** and whether opt-in consent or opt-out choice is required before processing can occur.
  - Evaluate the sensitive personal data your organization is collecting, if any, to get consent and offer choices where required.
- **Inventory your California personnel and business contact data** – The CPRA will apply to personal data about business contacts and personnel in the same manner in which it applies to consumer data.
  - Prepare for these new obligations by taking an inventory of existing personnel and business contact data, planning for requests from these parties, and minimizing the collection of unnecessary data.

Consumer Rights Requests

- **Prepare to execute new consumer rights in new states** – Several of the new laws will require companies to allow individuals to request correction of inaccurate personal data maintained by the company.
  - All of the new state laws **provide consumers in those states with rights of access and deletion** similar to those in the CCPA.
  - Your organization should consider **how new rights requests may fit into existing procedures** and address any gaps.
- **Prepare for targeted advertising opt-out requirements** – The new state laws give consumers the right to opt out of targeted advertising.
  - Your organization should **get mechanisms in place to handle such requests**.
  - For California, the opt-out right is specific to "sharing" for targeted advertising, while the other four states require an opt-out right for all processing for targeted advertising.

Next Steps

- **Stay up to date on state law developments** – The basic contours of the new state laws are unlikely to change, but **important updates will come from a variety of sources**—from state agency regulations to attorney general opinions.
  - For example, **California and Colorado have not finalized** regulations implementing the new laws.
  - Staying abreast of state privacy news will help your organization evolve with this changing landscape.

VENABLE LLP

Enforcement at the State Level

VENABLE LLP

State Enforcement

- **California**
  - **Currently**, the **California attorney general** is tasked with enforcement. **Beginning on July 1, 2023**, the **California Privacy Protection Agency** (CPPA) will also be tasked with enforcement and is currently drafting implementing regulations.
  - State attorney general enforcement is subject to **a 30-day cure period**; the CPPA will have a **discretionary 30-day cure period**.
  - 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**
  - Enforceable by the **Virginia attorney general**; a **30-day cure period** is available to controllers.
- **Colorado**
  - 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.
  - Delegates authority to the **Colorado attorney general to issue regulations** as necessary to further the purposes of the title.

State Enforcement

- **Connecticut**
  - Enforceable solely by the **Connecticut attorney general**; violations **will constitute an unfair trade practice** for purposes of Connecticut's UDAP statute.
  - **A 60-day cure period** is available to controllers **until December 31, 2024**, if a cure is "deemed possible"; **beginning on January 1, 2025**, the cure period is discretionary.
- **Utah**
  - Tasks the **Utah Division of Consumer Protection with investigating** violations and **referring them to the Utah attorney general** for enforcement; a **30-day cure period** is available.
- **Nevada**
  - Enforceable by the **Nevada attorney general**; a one-time **30-day cure period** is available for certain violations.

Enforcement in California

- Currently, the California attorney general is tasked with enforcement of the CCPA.
- On August 24, 2022, the California attorney general announced a **settlement with Sephora USA**, Inc., under the California Consumer Privacy Act. As part of the settlement, Sephora agreed to pay **a $1.2 million fine** and comply with particular provisions in the CCPA.
  - The attorney general alleged that following an **enforcement sweep of online retailers**, it found that Sephora and its analytics provider had **engaged in "commercial surveillance,"** involving the **"sale" of Californian's data to the analytics provider**, **without** CCPA-prescribed **notice or the ability to opt out**, including via global privacy controls.
- While the **CPPA will largely take over enforcement** of the CPRA in 2023, the Sephora complaint and settlement make clear that the attorney general:
  - Interprets the CCPA and its obligations on businesses broadly; and
  - Is focused on adequate disclosures and on consumers' ability to opt-out.

California Privacy Protection Agency

- The CPRA **created a new agency** to issue and implement regulations called the **California Privacy Protection Agency (CPPA)**.
  - The CPPA is **responsible for rulemaking** under the CCPA and CPRA, **enforcement**, and **privacy education** in California.
- The CPPA board is made up of **five members**.
  - The current members include a law school professor, an assistant AG, an SVP for LA28, a law firm counsel/law school professor, and an attorney for the Greenlining Institute.

Developments at the Federal Trade Commission

VENABLE LLP

FTC's Historic Role in Privacy Enforcement

- FTC **enforces Section 5 of the FTC Act,** along with other **sector-specific laws and rules** (Children's Online Privacy Protection Act, Health Breach Notification Rule, Gramm-Leach-Bliley Act, enforcing data security standards, etc.). Using this authority, the **FTC has brought hundreds of privacy and data security** cases.
- Section 5 of the FTC Act prohibits "**unfair or deceptive acts or practices in or affecting commerce**."
- Engaging in practices that the FTC deems to be unfair or deceptive can **result in a large-scale investigation** of the company.

VENABLE LLP

Penalties

- In a unanimous opinion on April 22, 2021, the **United States Supreme Court** held in *AMG Capital Management, LLC v. Federal Trade Commission* that **Congress did not authorize the FTC to obtain equitable monetary relief** pursuant to its authority under Section 13(b) of the FTC Act to obtain an injunction.
- Notably, this **change does not affect the FTC's ability to seek monetary penalties** for violations of:
  - Prior **cease-and-desist orders** or **consent orders**;
  - **Trade Regulation Rules** issued under Section 18(a)(1)(B) of the FTC Act defining unfair and deceptive practices; or
  - Through the **process authorized by Section 19** of the FTC Act.

FTC's Focus on Privacy

- The Commission is in a **transformational period**. FTC Chair Lina Khan has signaled a specific focus on privacy, including:
  - Advocating for a **new, comprehensive privacy rule**;
  - Announcing a "**holistic" approach** to identifying consumer harms that considers data collection practices; and
  - **Analyzing competition** with privacy in mind.
- The Commission has also taken to issuing "**Notice of Penalty Offense**" letters outlining practices determined to be unfair or deceptive.
  - This practice **allows the Commission to immediately seek relief** in federal District Court as companies that receive the letters are presumed to have "actual knowledge" of prohibited conduct.

Commercial Surveillance ANPR

- On August 11, 2022, the FTC published an **Advance Notice of Proposed Rulemaking** on **"commercial surveillance" and data security**.
  - "Commercial surveillance" is defined as "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."
- **The FTC can seek monetary relief for alleged violations of rules** made pursuant to Section 18.
- The comment period has been extended to November 21.

What if the FTC Is Interested in Your Company?

- The FTC has various tools at its disposal to investigate companies and collect information.
  - Initial wrongdoing does not have to be alleged.
  - Inquiries to learn about a company or an industry ("sweeps") are common.
- If you receive a civil investigative demand (CID) from the FTC:
  - Take it seriously.
  - Institute a litigation hold.
  - Retain counsel and schedule a "meet and confer" with FTC staff.
  - Begin your internal investigation into the activities targeted by the CID.
  - Be prepared for a (potentially) lengthy process.

EU-U.S. Data Privacy Framework

VENABLE LLP

EU-U.S. Data Privacy Framework

- In **March 2022**, President Biden and European Commission President Ursula von der Leyen announced an **agreement in principle** to **reestablish a framework** governing data transfer from the EU to the U.S.
- On October 7, 2022, President Biden signed an executive order, "**Enhancing Safeguards for United States Signals Intelligence Activities,**" that outlines the steps the U.S. will take to **implement U.S. commitments under the EU-U.S. Data Privacy Framework**. Notably, the executive order:
  - Adds **further safeguards for U.S. signals intelligence activities**, including outlining permissible national security objectives;
  - **Mandates handing requirements for personal information** collected through signals intelligence activities;
  - Extends the **responsibilities of legal, oversight, and compliance officials** to ensure actions are taken to remediate incidents of noncompliance; and
  - Creates a **multilayer mechanism for individuals** from qualifying states and regional economic integration organizations to **obtain independent and binding review and redress**.

Questions?

VENABLE LLP

VENABLE LLP