NEW DATA PRIVACY LAWS: UNDERSTANDING VIRGINIA, COLORADO, AND UTAH'S PRIVACY LAWS

By Danica P. Baird, Esq.

Dentons Durham Jones Pinegar

danica.baird@dentons.com

OBJECTIVES

- Understand applicability and key components of data privacy laws in Virginia, Colorado and Utah, which all go into effect in 2023.
- Compare these new laws with other significant data privacy laws
- Developing steps and strategies to ensure compliance with ever shifting climate

WHY IT MATTERS?

- Hotel Company $25.8 million in fines due to inadequate privacy policies and procedures
- Clothing company: $35.5 million euro
- Reputational harm and consumer outcry

BASE DEFINITIONS:

- **Personal Data:** any information that is linked or reasonably linkable to an identified or identifiable person
  - Does not include de-identified or publicly available information
- **Consumer:** a natural person who is a resident of a state acting in an individual or household context
  - Doesn't include people acting in a commercial (B2B) or employment context
- **Controller:** person or entity controlling how data is collected, processed, or used
- **Processor:** person or entity processes information on behalf of controller

SENSITIVE DATA

- Consent to process sensitive data
  - Affirmative act
  - Freely given
  - Specific
  - Informed
  - Unambiguous
- Sensitive Data:
  - Racial or ethnic data, religious beliefs, mental or physical health information, sexual orientation, citizenship or immigration status, biometric data, precise geolocation data

PATCHWORK OF LAWS

- Comprehensive data privacy laws passed
  - California (CCPA 2018, CPRA 2020)
  - Virginia (Virginia Consumer Data Privacy Act, 2021)
  - Colorado (Colorado Privacy Act 2021)
  - Utah (Utah Consumer Data Privacy Act 2022)

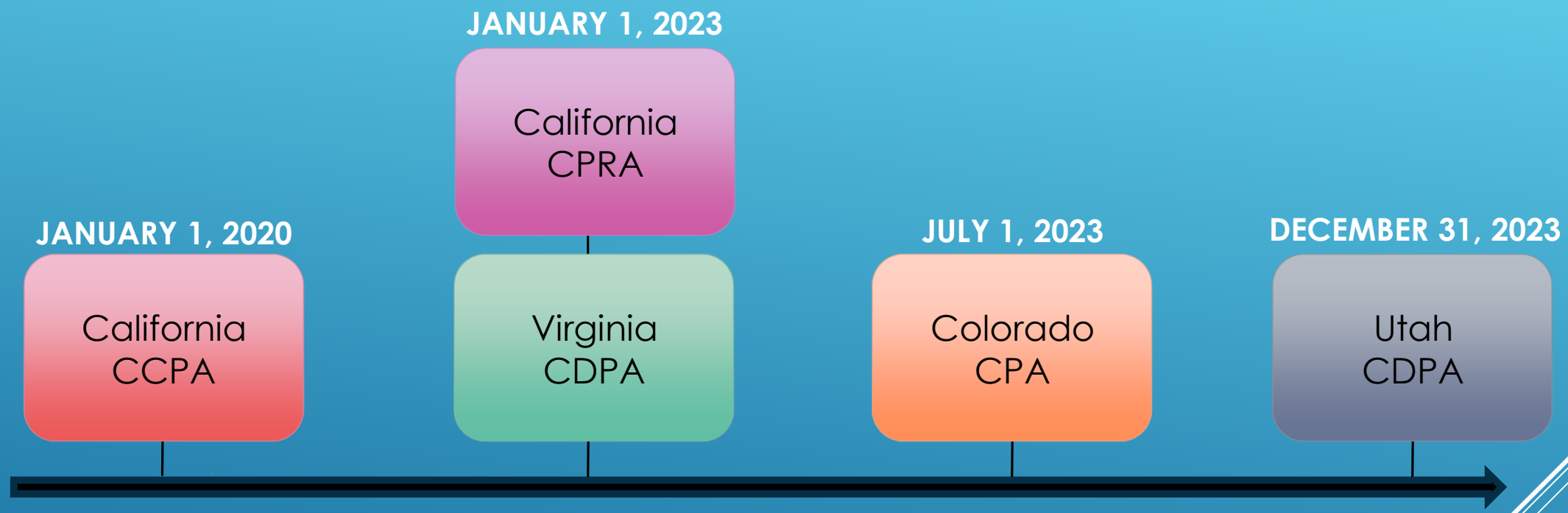
PATCHWORK OF LAWS

- Introduced:
  - 15 states have introduced comprehensive consumer data privacy legislation in 2022 (e.g., Arizona, Connecticut, Florida, Minnesota, Mississippi, and Washington)
  - 38 states introduced more than 160 privacy related bills in 2021
  - 30 states introduced bills in 2020
  - New SEC cybersecurity disclosure rules
  - Changes to Canada's PIPEDA currently pending
  - Changes to California's privacy laws have been proposed
  - Talk of federal law
- No sign of stopping or slowing down

VIRGINIA V. CALIFORNIA

- Divide amongst states as to approach in data privacy laws with Virginia and California being debated as models to follow.
- The two states that have successfully passed comprehensive data privacy laws have opted to follow Virginia
  - Virginia and Utah rejected California as not pro-business enough
- Major differences between Virginia and California:
  - No private right of action

EFFECTIVE DATES



APPLICABILITY

CALIFORNIA

- For-profit business doing business in state
- Collects personal information AND either
  - Has an annual gross revenue of at least $25 million **or**
  - Shares for a commercial purpose or sells information of at least 50,000 California residents, households, or devices
    - Note: CPRA it's 100,000 residents **or**
  - Derives 50% or more of annual revenue from selling personal information of California residents.

VIRGINIA, COLORADO, AND UTAH

- VA and Colorado:
  - For-profit business doing business in state
  - Controls or processes the personal data of at least 100,000 residents **or**
  - Controls or processes the personal data of at least 25,000 residents ***and*** derives over 50% of gross revenue from the sale of personal data
- Utah: Revenue of over $25 million in revenue and meets one of the obligations above (for-profit business)

EXEMPTIONS

- Many types of business fall outside coverage (non-profit, HIPAA organizations, Gramm-Leach Bliley Act, etc.)
- Consumer data (not B2B or employee data)

DATA SUBJECT RIGHTS

- Access
  - Confirmation company is processing the consumer's personal data
- Rectification/Correction
- Cancellation, Erasure, or Deletion
- Portability
- Opt-out of having PI sold, targeted advertising, and automated decision making.
- Anti-discrimination
- GDPR: right to be informed, access, rectification, deletion, restrict processing, data portability, object to processing, automated processing

DATA SUBJECT RIGHT: ACCESS

- Colorado: Consumer right to confirm whether their information is being processed and to access the data.
- Virginia, California and Utah: Right to obtain copy of personal data
  - Generally, 45 days to respond to request; extensions allowable in certain situations
  - May charge consumer a reasonable fee:
    - VA: request is "manifestly unfounded, excessive, or repetitive"
    - Colorado: second request in a 12-month period
    - Utah: Both VA and Colorado rules and if the company believes the primary purpose is for something other than exercising their consumer right.

DATA RIGHT: RECTIFICATION/CORRECTION

NO	YES

California CCPA
Utah
	► California CPRA
	  ► Consumer may request that information be corrected.
	► Virginia and Colorado
	  ► Consumer may correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing.

DATA RIGHT: CANCELLATION, ERASURE, DELETION

NO	YES
Utah (very limited)	► California ► Virginia ► Colorado Typically have 45 days to respond subject to certain extensions Verification standards allowed

Business must provide the information requested in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance.

DATA SUBJECT RIGHT: PORTABILITY

AUTOMATED DECISION MAKING/PROFILING

- California CCPA
  - Consumers are entitled to know how information will be used.
- California CPRA
  - Consumers are entitled to know how information will be used, right to limit processing in certain cases.
- Virginia
  - Consumers have right to limit processing of profiling activities (including automated processing).
    - Additional guidance may be forthcoming.
- Colorado
  - Consumers have the right to opt-out of the processing of personal data for profiling, meaning any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
- Utah
  - Consumers have the right to opt out of targeted advertising or the sale of personal data.

PRIVATE RIGHT OF ACTION

NO	YES
Colorado Virginia Utah	► California CCPA and CPRA ► Limited to instances where certain PI is subject to a data breach resulting from the business failing to maintain "reasonable" security around that data.

ENFORCEMENT

- California- Statutory damage of $750 per consumer; enforcement action $2,500-$7,500 per violation
- VA: AG may seek up to $7,500 per violation
- Colorado: up to $2,000 per violation but not to exceed $500,000
- Utah: up to $7,500 in statutory damages plus action damages to consumer

OTHER CONSIDERATIONS

- Data Mapping
- Data Retention
- Incident Response and Breach reporting and notifications
- Meeting security measures imposed by each states
- VA and CPRA require privacy impact assessments
- Handling of children data
- Confidentiality requirements for processors and employers (contractual obligations processors)

CONTRACTS BETWEEN PROCESSORS AND CONTROLLERS

- Contract must include:
  - Instructions for processing data
  - Nature and purpose of processing
  - Type of data subject to processing
  - Duration of processing
  - Rights and obligations of both parties
  - Duty of confidentiality
  - Deletion/Return of information
  - Subcontracting
  - Security

PRIVACY POLICIES

- What you collect? What types of data?
- How you collect?
- Why you collect it? (the purpose)
- How to exercise privacy rights?
- What you do with data?
- How long you retain it?
- Who do you share it with? What type of data is shared?
- How you secure it?
- Cookies?
- Third-party use?

PRIVACY POLICY PITFALLS

- Not having one (even if B2B, you should post one)
- Not having effective date
- Way too specific
- Not having opt out of cookies information
- Not having state-specific information
- Not updating frequently enough
  - Not monitoring monetary and residential thresholds closely enough
- (Collecting too much data)

PRIVACY PITFALLS

- "We don't collect any data, nothing to secure"
- Collecting too much data
- Way too complicated of incident response programs and internal policies and procedures
- Not following privacy policies and procedures
- Cultures where people are afraid to report incidents
- Not seeking legal counsel on reporting obligations
- Not training employees on importance of privacy and security regularly
- No contracts between controllers and processors

PSEUDONYMOUS AND DE-IDENTIFIED DATA

- Pseudonymous data is still personal data
  - Data that can be traced back to an individual
    - Reduces privacy risk and some requirements but it does not eliminate data privacy risk
  - De-identified/anonymized data is required for HIPAA, GDPR, CCPA, and Virginia's law
    - Can never be re-identified

DEALING WITH THE PATCHWORK

- Transparency
- Minimization of Data Collection and Use
- Security
- Accountability
- Determine whether you want to take on most restrictive obligations and have one policy or have specific state carve outs
  - Closely monitoring required if you take it state by state.

QUESTIONS?