Nonprofit Organization Data Privacy and Security

March 16, 2023

Kelly DeMarchis Bastide
Partner & Co-Chair, Privacy and Data Security Group | 202.344.4722 | KABastide@Venable.com

John Banghart
Senior Director for Cybersecurity Services, Technology and Innovation Group | 202.344.4803 | JFBanghart@Venable.com

Nana-Kwabena Abrefah
Associate, Privacy and Data Security Group | 202.344.4161 | NAAbrefah@Venable.com

VENABLE LLP

Agenda

- Cybersecurity Policy Trends
- State Privacy Laws and Nonprofit Organizations
- Litigation Risks Arising from New Applications of Old Privacy Laws (the Video Privacy Protection Act ("VPPA"), Wiretapping Laws, and Illinois's Biometrics Information Privacy Act (BIPA))
- Takeaways

VENABLE LLP

Cybersecurity Policy Trends

VENABLE LLP

The Cyber Threat Landscape

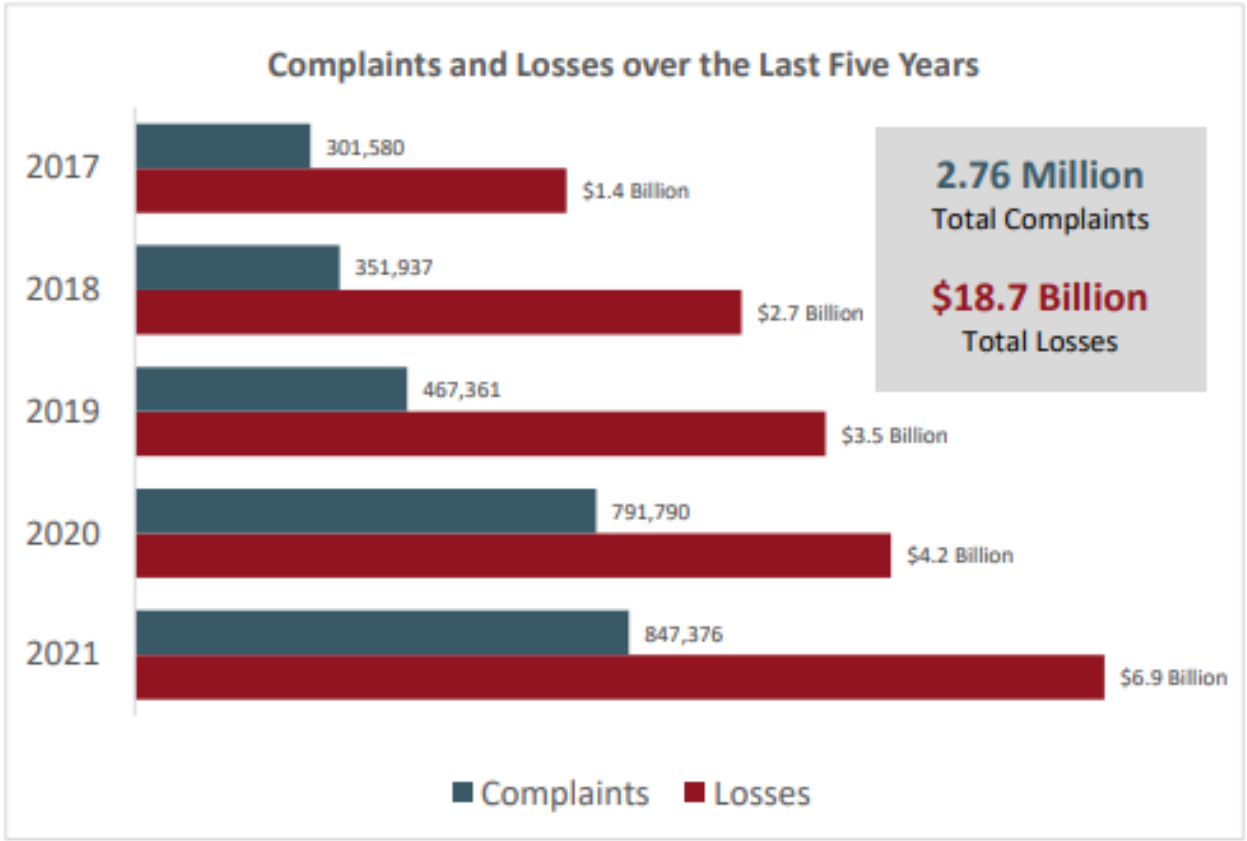
- **The cyber threat landscape continues to increase in size and sophistication**
  - More devices, more data, more adversaries

- **The impact of cyberattacks has become more severe**
  - **Colonial Pipeline (2021)** – Critical infrastructure, public panic, national economic disruption
  - **Kaseya VSA (2021)** – Supply chain attack, 1000+ organizations impacted
  - **Health Service Executive (2021)** – Critical infrastructure, patient care negatively impacted for an extended period, over $83 million in damages and remediation costs reported
  - **Costa Rican Government (2022)** – State of emergency declared, disruption to government services and foreign trade reported

VENABLE LLP

Non-state Threat Actors

- **Cybercrime continues to be a lucrative criminal enterprise**
- **Top cybercrime types include ransomware and Business Email Compromise (BEC)**
- **Other non-state actors include Hacktivist / Patriotic Hackers whose motivations may lay outside of financial gain**
- **Non-state actors have shown willingness to target critical infrastructure sectors**



Source: FBI IC3 Report 2021

VENABLE LLP

Nation-state Threat Actors

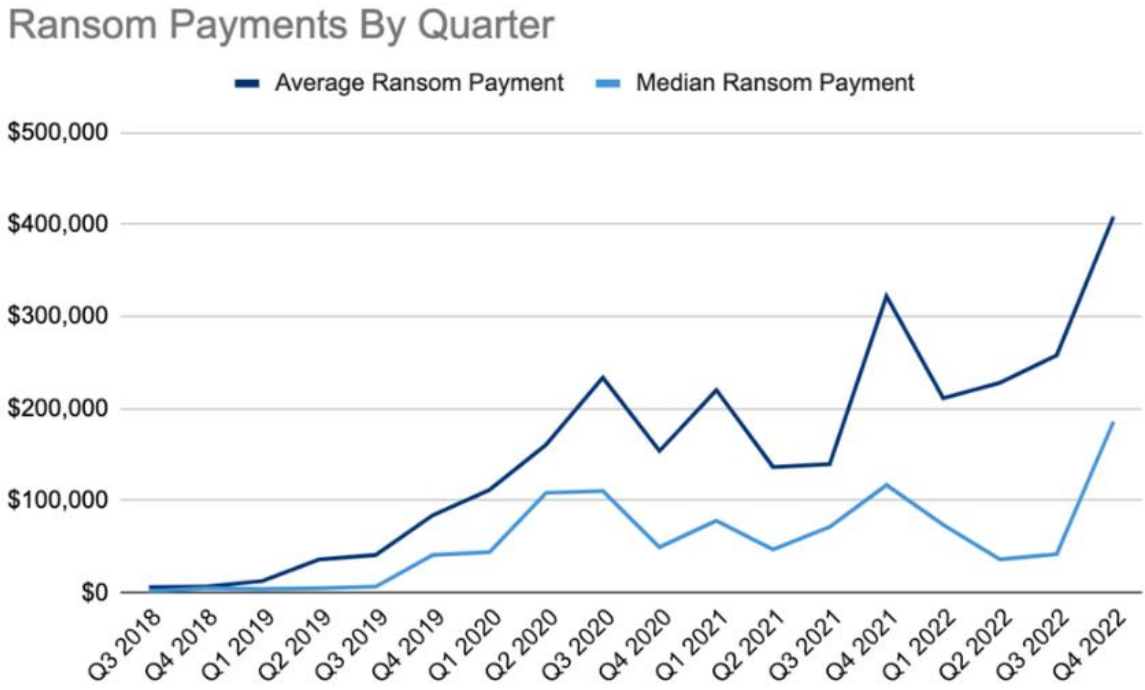
- **Nation-state threat actors continue to use cyber capabilities to further national strategic interests**
  - Military and economic research and development
  - Profit
  - Espionage and sabotage
  - Disinformation operations

- **Russia** – Extensive offensive cyber operations targeting Ukraine's government and civilian infrastructure
- **Iran** – Accused of extensive cyberattacks on Albania leading to severed diplomatic relations
- **China** – Continuous espionage and intellectual property (IP) theft activities
- **North Korea** – Estimated to have engaged in cybercrime activities worth between $630M and $1B in 2022

VENABLE LLP

Ransomware

- **Fewer victims are paying**
  - 85% Q1 2019 -> 37% Q4 2022
- **However, average and median ransom payments have continued to trend upward**
  - Q4 2022 Average: $408,644 (+58% over Q3)
  - Q4 2022 Median: $185,972 (+342% over Q3)
- **Cybercriminals continue to rapidly adapt ransomware tools and strategies**
  - RaaS
  - Various extortion methods to maximize profit (double extortion, triple extortion, re-extortion)



Source: Coveware

VENABLE LLP

Government Policies

- **What are governments championing and what should they be championing?**
  - Secure Software Development / Secure by Design Principles
    - e.g. NIST SSDF
  - Vulnerability Disclosure
    - Coordinated responsible disclosures
  - Cybersecurity Metrics
  - Expanding and improving Information Sharing
  - International Standards and Regulatory Harmonization

VENABLE LLP

Incident Reporting and Compliance Challenges

- **Incident Reporting Gains Global Traction**
  - CISA: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
  - SEC: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

- **Requirements**
  - Covered entities that suffer a covered cyber incident must report to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours after the entity "reasonably believes that the covered cyber incident has occurred."
  - Covered entities that make a ransom payment as the result of a ransomware attack must report the payment to CISA within 24 hours
  - Covered entities may be required to submit supplemental reports depending on evolving circumstances
  - CISA is tasked with developing CIRCIA regulations through an extensive rulemaking process

VENABLE LLP

SEC: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

- **Proposed Requirements**
  - SEC registrants would need to report material cybersecurity incidents on Form 8-K
  - SEC registrants would need to make periodic disclosures regarding:
    - Policies and procedures to identify and manage cybersecurity risks
    - Management's role in implementing cybersecurity policies and procedures
    - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk
    - Updates about previously reported material cybersecurity incidents

VENABLE LLP

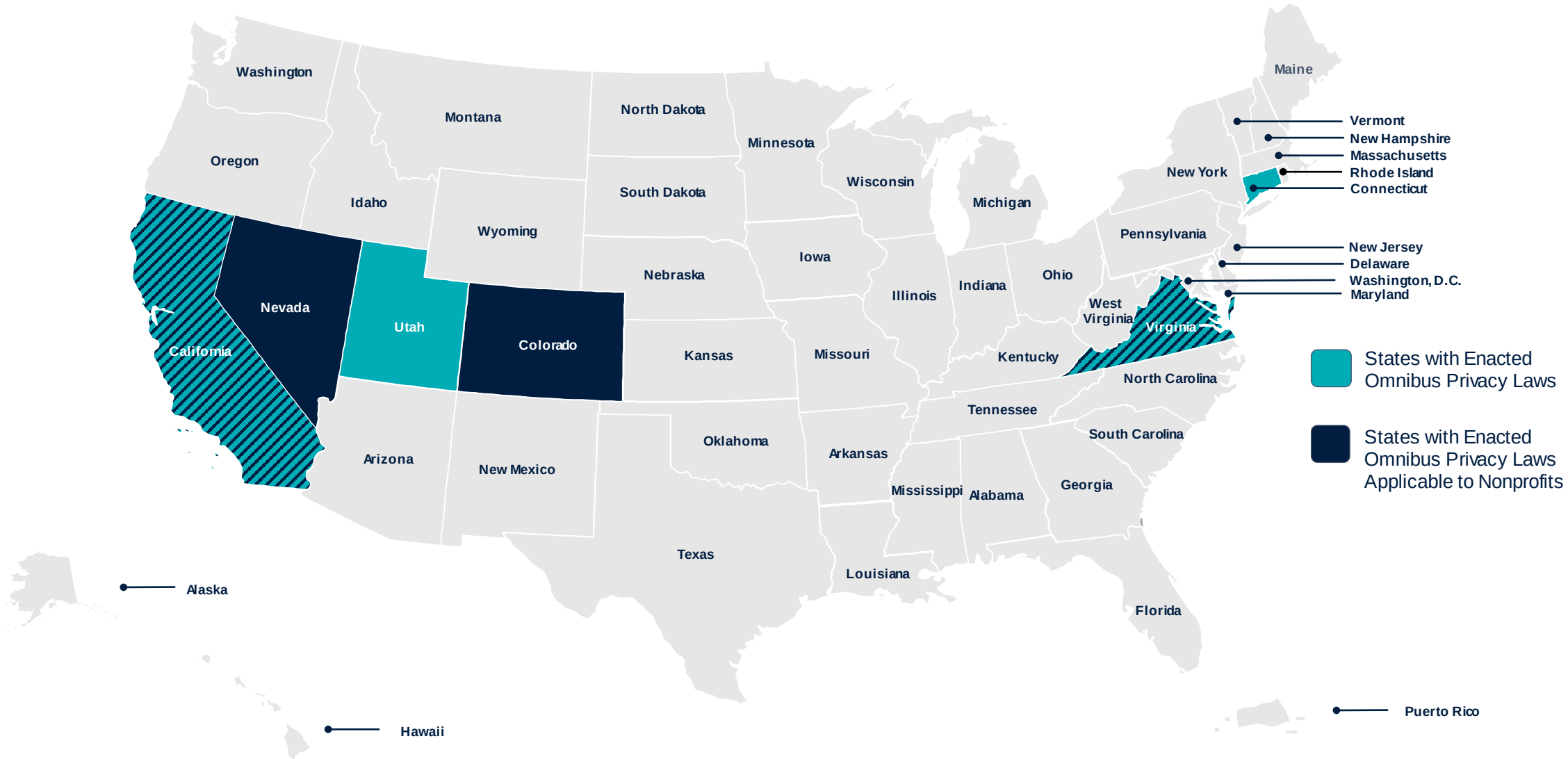
State Privacy Laws: Overview

VENABLE LLP

Timeline
Laws Effective

VENABLE LLP

State Privacy Laws



VENABLE LLP

State Laws That Exempt Nonprofits

- **Connecticut:** The Connecticut Data Privacy Act (CTDPA)
  - "The provisions . . . of this act do not apply to any . . . nonprofit organization" defined as "any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time." 2022 Conn. Acts 22-15 §§ 1(17), 3(a)(2).
- **Utah:** The Utah Consumer Privacy Act (UCPA)
  - "This chapter does not apply to . . . a nonprofit corporation" defined as an entity that (1) is not a foreign nonprofit corporation and is incorporated under Utah's Revised Nonprofit Corporation Act (Utah Code Ann. § 16-6a); or (2) is incorporated under law other than Utah's laws and would be a nonprofit corporation if formed under Utah's laws. Utah Code Ann. §§ 13-61-101(23), 13-61-102(2)(d).

State Laws That May Apply to Nonprofits

- **Colorado**: The Colorado Privacy Act (CPA)
  - No express nonprofit exemption.
  - A nonprofit may **conduct business** in Colorado by registering in the state (among other actions).
  - **Processing** personal data includes a wide range of data practices, such as **collection.**
  - A **"consumer"** is an individual who is a Colorado resident acting in an individual or household capacity. In determining the number of consumers by state, a nonprofit may consider, for example, the following: (1) number of unique website visitors per year from Colorado; (2) number of Colorado donors per year; or (3) number of Colorado residents on mailing lists.
- **Virginia**: The Virginia Consumer Data Protection Act (VCDPA)
  - As Virginia and Colorado share similar definitions of conducting business, processing, and a consumer, the above examples likely apply to determining Virginia's thresholds, too.
  - VCDPA exempts nonprofits organized under Virginia law, 501(c)(3), (6), and (12) organizations, political organizations, and subsidiaries or affiliates of utility providers.
  - However, the VCDPA **does *not* exempt all 501(c)(4) organizations** (certain insurers providing information to authorized law enforcement are exempt).

VENABLE LLP

State Laws That May Apply to Nonprofits (cont'd)

- **California:** The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA)
  - The CPRA directly regulates "**businesses**." While a nonprofit generally does not qualify as a business, one may **if another business "controls" the nonprofit and the two entities share personal information and "common branding."** For example, if a corporation has a nonprofit arm or foundation, that nonprofit arm may qualify as a business under California law. *See* Cal. Civ. Code § 1798.140(d).
  - A nonprofit may also qualify as a "**service provider**," "**contractor**," or "**third party**" under the CPRA and be subject to certain contractual requirements or other requirements to assist a business in its compliance with the law.
- **Nevada**: The Privacy of Information Collected on the Internet from Consumers Act (NPA)
  - The NPA applies to **"operators,"** organizations that: (1) own or operate a website or online service for commercial purposes; (2) collect data from Nevada residents; and (3) direct activities toward Nevada, transact with Nevada, or otherwise establish connection with Nevada

VENABLE LLP

Statutory Thresholds

If a nonprofit meets the following thresholds, it may be subject to the respective state's consumer privacy law.

Threshold Category	California	Colorado	Nevada	Virginia
1. Operating in the state	Do business in CA	Conduct business or target CO residents with products/services	Fulfill 3 criteria to qualify as an "operator."	Conduct business or target VA residents with products/services
2. Gross annual revenue	$25 million	N/A	N/A	N/A
3. Buys, sells, or shares the personal information of some number of consumers or households	100,000 consumers	N/A	N/A	N/A
4. Controls or processes the personal information of some number of consumers or households per calendar year	N/A	100,000 consumers	N/A	100,000 consumers
5. Percentage of revenue from selling or sharing (for targeted advertising) consumers' personal information	50% or more	N/A	N/A	N/A
6. Controls or processes consumer information plus percentage revenue from selling personal data	N/A	25,000 consumers + any revenue or discount from selling personal data	N/A	25,000 consumers + more than 50%
Analysis	If 1 and any of 2-6 above are met, the law applies	If 1 and either 4 or 6 is met, the law applies	If 1 is met, the law applies	If 1 and either 4 or 6 is met, the law applies

VENABLE LLP

The Colorado Privacy Act (CPA) and Virginia Consumer Data Protection Act (VCDPA)

VENABLE LLP

How Does the VCDPA or CPA Apply to Organizations?

Colorado

- The CPA applies to more types of nonprofit organizations than does the VCDPA.
- If a nonprofit directs or controls the processing of personal data, the organization may be a **controller** and be directly regulated by the CPA.
- If a nonprofit instead processes personal data on behalf of another entity, the organization may be a **processor** subject to the CPA and largely regulated through contractual terms.
- The CPA does not apply to employment records, job applicants, or business-to-business contacts.
- Date Effective: **July 1, 2023**

Virginia

- The same standards define whether an organization qualifies as a controller or processor under the VCDPA.
- The VCDPA also does not apply to employment records, job applicants, or business-to-business contacts.
- Date Effective: **January 1, 2023**

VENABLE LLP

Consumer Rights and Personal Data

- Colorado and Virginia generally take similar approaches to consumer rights and personal data.
- Both laws are **rights-based** and give Coloradans and Virginians the **rights to access**, **correct**, **delete, and opt-out of processing of** personal data.
- **Personal data** is information that is linked or linkable to an identified or identifiable individual. Personal data does ***not*** include de-identified or publicly available information.
- Controllers will have primary responsibilities for responding to consumer rights requests. Processors will be required to assist in responding to certain requests, providing information to respond, or otherwise providing information to show compliance with the statute.
- If a controller **cannot authenticate** that a requester is the individual in question using commercially reasonable means, the CPA and VCDPA do not require the controller to respond to consumer rights requests.
    - Colorado residents may also appoint an **authorized agent** to submit requests on their behalf. Controllers must be able to authenticate the agent's authorization; otherwise, controllers are not required to respond to these requests.

VENABLE LLP

Access, Correct, and Delete

Colorado

- For an authenticated **access request**, a controller must provide the personal data about the consumer that the nonprofit processes or maintains.
    - **Portability.** In Colorado, to the extent technically feasible, an organization must provide the consumer with data the organization processes about the consumer in a format that could be transferred to and readily used by another entity.
- For an authenticated **correction request**, a controller must correct inaccurate information about the individual.
    - Proposed regulations would allow a controller to request information relating to the accuracy of the information in dispute.
- For an authenticated **deletion request**, a controller must delete personal data about the requester, subject to certain exempted purposes for retaining the data.

Virginia

- Similarly, a controller must provide personal data in response to an access request.
    - In providing "portable" data, a controller need only provide **data the consumer provided** (possibly narrower than all data processed).
- For correction, a controller again must correct inaccurate information
    - Virginia has not provided further detail on processes to interrogate the accuracy of data in dispute.
- A controller responds to a deletion request as in Colorado.

VENABLE LLP

Opt-Outs of Processing

Colorado

- The CPA gives consumers **the right to opt out of the processing** of their personal data for the purposes of (A) targeted advertising, (B) the sale of personal data, or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.
- "**Targeted advertising**" means **displaying to a consumer an advertisement** that is **selected based on personal data** obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests.
- "**Sale**" means exchanging personal data **for monetary or other valuable consideration**.
- "**Profiling**" means 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.
- The CPA requires businesses to provide a "clear and conspicuous" method to consumers to exercise the right to opt out of the sale of personal data or targeted advertising.

Virginia

- The VCDPA grants consumers a similar opt-out right.
  - Targeted advertising and profiling have the same meaning.
  - However, Virginia **defines "sale" more narrowly** as exchanges for monetary consideration.
- Although not specific to the opt-out right, the VCDPA requires methods to exercise consumer rights to appear in a privacy policy.

VENABLE LLP

Opt-Outs: Universal Opt-Out Mechanisms (*Colorado only*)

- From July 1, 2023 until July 1, 2024, controllers that process personal data for targeted advertising or sales **may** allow Colorado consumers to opt out of such processing through a user-selected universal opt-out mechanism. Effective **July 1, 2024**, controllers are **required** to honor browser/device signals from Colorado residents.
- The CPA charges the Colorado attorney general with issuing **technical specifications** governing the opt-out mechanism. The most recent version of proposed regulations to implement the CPA includes terms on technical specifications, such as the ability to communicate more than one opt-out right without unfairly disadvantaging any controller. The attorney general is required to **issue the regulations by July 1, 2023**.
- The proposed regulations to implement the Colorado Privacy Act set forth a process whereby the Colorado attorney general would maintain a **public list of AG-recognized universal opt-out mechanisms**.

Appeal

Colorado

- If an organization **denies or refuses to act** on a consumer's rights request, the CPA requires the organization to explain the denial and provide **instructions for how to appeal** the decision.
- Upon receiving an appeal, an organization has **45 days to reply with a possible 60-day extension** where reasonably necessary.
- A response to an appeal must **explain the decision** to approve, partially approve, or deny the appeal.
- For all appeals regardless of disposition, the response must **notify the appellant of their ability to contact the Colorado attorney general** with concerns.

Virginia

- The VCDPA similarly requires instructions to appeal upon denying or refusing to act on a request.
- The Virginia law grants an organization **60 days to respond** to appeals **with no express mention of a possible extension**.
- Responses also must include an explanation.
- An organization must provide an appellant with an **online contact mechanism for the Virginia attorney general** to submit a complaint **only if an appeal is denied**.

VENABLE LLP

Sensitive Data

- Colorado and Virginia impose the same consent obligations on entities that would process "sensitive data" but differ in their definitions of "sensitive data."
- **Opt-in consent.** A nonprofit must not process a consumer's "sensitive data" without first obtaining the consumer's consent.
- "**Consent**" means a **clear, affirmative act** signifying a consumer's freely given, specific, informed, and unambiguous agreement.
    - The CPA **expressly excludes** the following from satisfying effective consent:
        - acceptance of a general term or broad terms of use or a similar document that contains descriptions of personal data processing along with other, unrelated information;
        - hovering over, muting, pausing, or closing a given piece of content; and
        - agreement obtained through dark patterns.

VENABLE LLP

Sensitive Data (cont'd)

Colorado

- "Sensitive data" means
  - Personal data revealing:
    - Racial or ethnic origin
    - Religious beliefs
    - A mental or physical health **condition or diagnosis**
    - **Sex life** or sexual orientation
    - Citizenship or citizenship status
  - Genetic or biometric data that may be processed to uniquely identify an individual
  - Personal data from a known child
  - **Sensitive data inferences**, e.g., sensitive information inferred from
    - Precise geolocation data (like presence at a religious building)
    - Web browsing data, alone or in combination

Virginia

- "Sensitive data" means
  - Personal data revealing:
    - Racial or ethnic origin
    - Religious beliefs
    - A mental or physical health diagnosis
    - Sexual orientation
    - Citizenship or citizenship status
  - Processing genetic or biometric data to uniquely identify an individual
  - Personal data from a known child
  - **Precise geolocation data**

VENABLE LLP

Transparency Requirements

- The CPA and VCDPA require certain notices, which may appear in an organization's **privacy policy** and include the following information:
  - Categories of personal data collected or processed
  - Categories of third-party recipients of personal data
  - Purposes for processing
  - How and where consumers may exercise their rights
  - If applicable, the fact that an organization sells personal data or processes it for targeted advertising plus how a consumer can opt out.

Data Protection Assessments

Colorado

- The Colorado Privacy Act requires a controller to conduct a **data protection assessment** in the following instances:
  - Processing personal data for **targeted advertising**;
  - **Selling** personal data;
  - Processing personal data for **profiling with a reasonably expected risk of substantial injury** (including, unfair or deceptive treatment; unlawful disparate impact; financial, physical, or reputational injury; or a reasonably offensive privacy invasion)
  - Processing sensitive data; and/or
  - Processing that otherwise presents a heightened risk of harm to individuals.
- Assessment goals: (1) weigh benefits and risks of processing, (2) identify safeguards, and (3) demonstrate that the benefits outweigh the risks offset by the safeguards.
- **At their discretion**, the Colorado attorney general may request an organization produce an assessment.

Virginia

- The Virginia law sets the same requirements for when a data protection assessment must occur and what it should accomplish.
- The Virginia attorney general may request an assessment **only if relevant to an investigation** the Virginia attorney general is conducting.

VENABLE LLP

Who Enforces?

Colorado

- **The Colorado attorney general and state district attorneys** will enforce the CPA.
- There is a **60-day cure period** that **sunsets on January 1, 2025**.
- The law grants the **Colorado attorney general rulemaking authority.** The third and most recent version of proposed regulations to implement the CPA was published on January 27, 2023.
- The statute does not provide explicit fines for noncompliance. However, violations of the CPA are **considered deceptive trade practices** as defined by the Colorado Consumer Protection Act. Noncompliant entities then can be **fined up to $20,000 per violation**.
- The CPA does **not include a private right of action**.

Virginia

- The **Virginia attorney general will have exclusive enforcement authority** for the VCDPA.
- A **30-day cure period** exists and does not sunset.
- The Virginia law does not grant rulemaking authority.
- Violations of the law may incur civil penalties of **up to $7,500 per violation**.
- The VCDPA also does **not include a private right of action**.

VENABLE LLP

California Privacy Rights Act (CPRA)

VENABLE LLP

California
CCPA *vs.* CPRA At-a-Glance

Requirement	CCPA	CPRA
Right to Know and Access	✓	✓
Right of Deletion	✓	✓
Right to Opt-Out of the *Sale* of Personal Information	✓	✓
Right to Opt-Out of the *Sharing* of Personal Information		✓
Right to Correct Inaccurate Personal Information		✓
Rights Pertaining to Sensitive Personal Information		✓
Risk Assessment Requirements		✓
Opt-out Preference Signal/Global Privacy Controls Requirement	✓	✓
Private Right of Action (Limited)	✓	✓
30-Day Cure Period	✓	✓ - Private Actions ✓ - Civil Actions by AG **Discretionary** – Administrative Enforcement Actions by California Privacy Protection Agency ("CPPA")
Enforcement	AG	AG & CPPA

VENABLE LLP

California Privacy Rights Act Overview

- The CPRA amends the CCPA, including by expanding consumer rights:
  - A right to **know and access** personal information;
  - A right to **correct** inaccurate personal information;
  - A right to **delete** personal information;
  - A right to **opt out of "sales"** of personal information
  - A right to **opt-out of "sharing"** of personal information for "**cross context behavioral advertising**"; and
  - A right to **limit the use and disclosure** of "**sensitive personal information**."
- The CPRA primarily regulates "businesses" as well as "service providers," "contractors," and "third parties."
- Effective Date : **January 1, 2023**
- Date When Civil and Administrative Enforcement May Begin: **July 1, 2023**

VENABLE LLP

“Sharing” Personal Information

- Under CPRA, consumers may opt out of business “sales” of personal information ***and*** **limit the business’s “sharing” of personal information.**
  - “**Sharing**” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information by the business to a third party for **cross-context behavioral advertising**, **whether or not for monetary or other valuable consideration**.
- “**Cross-context behavioral advertising**” is defined as “the **targeting of advertising** to a consumer based on the consumer’s personal **information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services**, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.”

Transparency and Consumer Rights

- The CPRA requires certain privacy policy disclosures to align with its statutory text e.g., descriptions of categories of personal information collected or disclosed.
- If an organization sells or shares personal information or processes sensitive personal information for purposes other than those permitted by the statute, California's law also requires certain links to be posted: "**Do Not Sell or Share My Personal Information**," "**Limit the Use of My Sensitive Personal Information**," and/or an alternative opt-out link (combining the functionality of the prior two) "**Your Privacy Choices**" or "**Your California Privacy Choices**."
- Proposed regulations to implement the CPRA also **require businesses to honor opt-out preference signals** sent on behalf of consumers and to treat these signals as valid requests to opt out of the sale and sharing of personal information.
    - The statute requires the California Privacy Protection Agency (CPPA) to provide certain specifications and guardrails for these signals that may be the subject of continued rulemaking or discussion processes at the CPPA.

Sensitive Personal Information

- The CPRA defines "**sensitive personal information**" and gives Californians the right to **limit a business's use and disclosure** of this type of information to certain limited uses.
- The right to limit a business's use and disclosure of sensitive personal information **applies only to sensitive personal information that is collected or processed with the "purpose of inferring characteristics about a consumer.**"
- Businesses must provide a "**Limit the Use of My Sensitive Personal Information**" **link** on their Internet homepages to allow consumers to submit a request to effectuate the right to limit the use or disclosure of this information

- Sensitive personal information includes:
  - Personal information that reveals:
    - Social Security, driver's license, state identification card, or passport number;
    - account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
    - precise geolocation;
    - race, ethnicity, religious or philosophical beliefs, or union membership;
    - contents of mail, email, or text messages; or
    - genetic data;
  - Processing biometric information to uniquely identify a consumer;
  - Health information; and
  - Information regarding sex life or sexual orientation.

VENABLE LLP

The California Privacy Protection Agency and Enforcement

- The CPPA may investigate possible violations of the CPRA upon the sworn complaint of any person or on its own initiative. The California attorney general also has enforcement authority for the CPRA.
- Enforcement is subject to a **discretionary 30-day cure period**.
- **The CPRA provides the CPPA with the regulatory authority to issue rules** to "further the purposes of [the] title," as well as rules addressing a non-exhaustive list of specific issue areas including regulations to define or add additional color to specific terms and technical specifications for an opt-out preference signal. This grant removes the attorney general's rulemaking authority.
- On February 15, 2023, the CPPA submitted a finalized packet of regulations to California's Office of Administrative Law. These regulations will likely come into effect, at latest, **by July 1, 2023**.
- While the CPPA seeks to finalize its first round of rulemaking, the agency has announced a second round of rulemaking on cybersecurity audits, risk assessments, and automated decision-making.
- The CPRA **alters the CCPA's limited private right of action** for data breaches. It maintains the CCPA's 30-day cure period but states that implementation and maintenance of reasonable security procedures following a breach do not constitute a cure with respect to that breach.

Nevada Privacy of Information Collected on the Internet from Consumers Act (NPA)

VENABLE LLP

When Is an Organization Subject to the NPA?

- Nevada passed its privacy law in 2019 and amended the law in 2021. The NPA is much narrower in scope than the Colorado law (and other state privacy laws). **The Nevada law applies to "operators" and does not exempt nonprofits.**
- The NPA addresses **"covered information,"** which means any of the following, alone or in combination, if collected online and maintained in an accessible form: (1) first and last name; (2) home or physical address; (3) e-mail address; (4) phone number; (5) Social Security number; (6) an identifier; or (7) any other information combined with an identifier, making the information personally identifiable.
- **The Nevada attorney general is permitted to bring enforcement actions for violations**. The Nevada law has **no private right of action**.
- Date Effective: **October 1, 2021**

VENABLE LLP

Transparency and Limited Consumer Rights

- **The NPA does not provide consumers with rights to access, correct, or delete their personal information.** It emphasizes transparency in data collection.
- **Operators subject to the Nevada law that collect covered information must provide a privacy policy** that includes disclosures such as the categories of covered information collected and whether a third-party may collect covered information about an individual consumer's online activities. Operators who fail to do so have a **30-day cure period** to remedy said failure.
- The Nevada law gives consumers the ability to **opt-out of sales of covered information**. **"Sale"** is defined as exchanging covered information for monetary consideration.
- The law was amended in May of 2021 and expanded consumers' ability to opt-out of sales of covered information held by **"data brokers."**

VENABLE LLP

Litigation Risks Arising from New Applications of Old Privacy Laws (VPPA, Wiretapping Laws, and BIPA)

VENABLE LLP

When Does the VPPA Apply to an Organization?

- Congress enacted the Video Privacy Protection Act (VPPA) in 1988 to afford consumers a narrow privacy right to control who could obtain their video viewing records from a video rental or retail store. The law **does not exempt nonprofit organizations.**
- The VPPA **prohibits the knowing disclosure of "personally identifiable information" (PII)** of a consumer **by a video tape service provider (VTSP)** to any person, subject to limited exceptions.
- VTSPs include anyone engaged in the business of renting, selling, or delivering prerecorded video cassette tapes or similar audio-visual materials. Courts have interpreted this term to **include video streaming services and other video content providers on the Internet.**
- PII means information that **identifies a person as requesting or obtaining specific video materials from a VTSP**. Courts have held that PII includes items like an individual's full name with a video title and generally agree that any information that would allow an ordinary person to identify a specific person as having watched a video would constitute PII.
    - Courts have generally found that a device identifier alone with a video title does not count as PII but could if combined with additional data elements (e.g., precise location information).

VENABLE LLP

VPPA Enforcement and Tracking Tools

- The VPPA is enforced exclusively through private litigation. With the growth in online video streaming services, the law has seen a resurgence in interest.
- The VPPA does **not generally exempt disclosures to service providers** and otherwise includes limited exceptions—e.g., to the consumer, to third parties with informed written consent that meets specific requirements, or in the "ordinary course of business" as narrowly defined by the VPPA.
- Consumers can bring **class action lawsuits for $2,500 per violation for violations of the VPPA**, which can easily cause costs to balloon when considering online audience sizes.
- The law generally does not apply to, and is not enforced against, recipients of PII.
- Additionally, lawsuits are beginning to **extend the VPPA websites' tracking of online video viewing behavior.**
- For example, if an organization's website embeds video content or services and uses tracking technologies—like session replay or even cookies and pixels—those technologies may collect identifiers combined with video information and share that information with third parties. Recent lawsuits allege that this collected information constitutes PII and that the sharing violates the VPPA.

How Do Wiretapping Laws Apply to Online Tracking?

- All 50 states and the federal government have laws relating to wiretapping or surveilling communications.
- Taking the federal Electronic Communications Privacy Act (or "Wiretap Act") as an example, these laws **may apply to nonprofits** since they govern "persons" generally.
- The federal Wiretap Act refers to and regulates "**intercepting**" a communication, which is acquiring the contents of any wire, electronic, or oral communication via any electronic, mechanical, or other device.
- There is a split between two-party consent and one-party consent jurisdictions, referring to the necessary number of parties to a communication to legally justify a recording or interception. **One-party is the majority rule** among states, and the federal Wiretap Act also follows this rule.

VENABLE LLP

Enforcing Wiretapping Laws and Session Replay

- **Session-replay tools** allow a website operator to **record a user's interactions with the website**, including clicks, keystrokes, and search information.
- Recent **class-action lawsuits under wiretapping laws** have alleged that use of session-replay technology constitutes wiretapping and a violation of the relevant statute.
- Wiretap statutes, like the federal Wiretap Act, California Information Privacy Act (CIPA), and Florida Security of Communications Act (FSCA), may provide for **statutory damages**, raising the risk of costly litigation.
- These allegations pose a problem in two-party consent states where the operator's consent to the session-replay technology alone will not suffice if the technology is deemed to be wiretapping.
- In 2022, cases in the Third and Ninth Circuits raised but did not definitively answer the issue of **whether notice in a privacy policy would be sufficient** to avoid liability under wiretapping statutes. These cases also inspired dozens of plaintiffs' suits.

What Does BIPA Cover?

- The Illinois Biometric Information Privacy Act ("BIPA") **requires "private entities" to obtain consent prior to processing a consumer's "biometric information**," among other restrictions.
- The law defines a "**private entity**" to be any individual, partnership, corporation, limited liability company, association, or other group, however organized. Therefore, **BIPA applies to nonprofits**.
- "**Biometric information**" means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier (i.e., retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) used to identify an individual."

VENABLE LLP

BIPA Enforcement and Litigation

- BIPA grants a private right of action for alleged violations. Damages may be up to the greater of
  - Liquidated damages of $1,000 or actual damages per negligent violation; or
  - Liquidated damages of $5,000 or actual damages per intentional or reckless violation.
- After the law went into effect in 2008, the first jury verdict under Illinois's BIPA was issued in 2022. That verdict resulted in a **$228 million judgment** against the Defendant.
- In February 2023, the Illinois Supreme Court ruled that **a separate claim accrues under BIPA each time an entity scans or transmits an individual's biometric identifier or biometric information**. *See Cothron v. White Castle Systems*, Inc., 2023 IL 128004 (Feb. 17, 2023).

VENABLE LLP

Takeaways

VENABLE LLP

Threat Mitigation Strategies

- **Best Practices and Innovative Mitigation Strategies**
  - Cybersecurity risk is organizational risk – starts with the Board/C-suite
  - Embrace an information sharing and shared defense mindset
    - ISACs/ISAOs
  - Make use of cloud services where it makes sense
    - Cloud shared responsibility models for security – You still have to do you part!
  - Supply-chain
    - Implement contractual third-party cybersecurity baselines
    - Figure cybersecurity and technical support lifetimes into product acquisition

Privacy Law Preparation and Risk Mitigation

- Assess applicability of state laws (consider a data map of your organization)
- Update privacy policies, especially regarding consumer rights explanations and ways to exercise these rights
- Keep abreast of regulatory processes and developments in California and Colorado
- If using tracking tools (session replay but also cookies, pixels, and the like), review disclosures to consumers and, with legal counsel, consider including specific disclosures in a privacy notice or establishing other consent processes.

Questions?

Kelly DeMarchis Bastide

KABastide@Venable.com

John Banghart

JFBanghart@Venable.com

Nana-Kwabena Abrefah

NAAbrefah@Venable.com

VENABLE LLP

VENABLE LLP