May 25, 2021

Privacy Legislation and Regulation in the USA State and Federal — in 2021 and Beyond

Reed Freeman
Venable

Chelsea Reckell
Venable

Christopher Oswald
Association of National Advertisers

Maneesha Mithal
Federal Trade Commission

Esther Chavez
Office of the Texas Attorney General

Privacy+ Security Forum

Speakers

Reed Freeman, Jr.
eCommerce, Privacy, Cybersecurity
Advertising & Marketing
Venable LLP

Maneesha Mithal
Bureau of Consumer Protection
Federal Trade Commission

Esther Chavez
Consumer Protection and Public Health Division
Office of Texas Attorney General

Chelsea Reckell
eCommerce, Privacy, Cybersecurity
Venable LLP

Chris Oswald
Government Relations
Association of National Advertisers (ANA)

Privacy+ Security Forum

Agenda

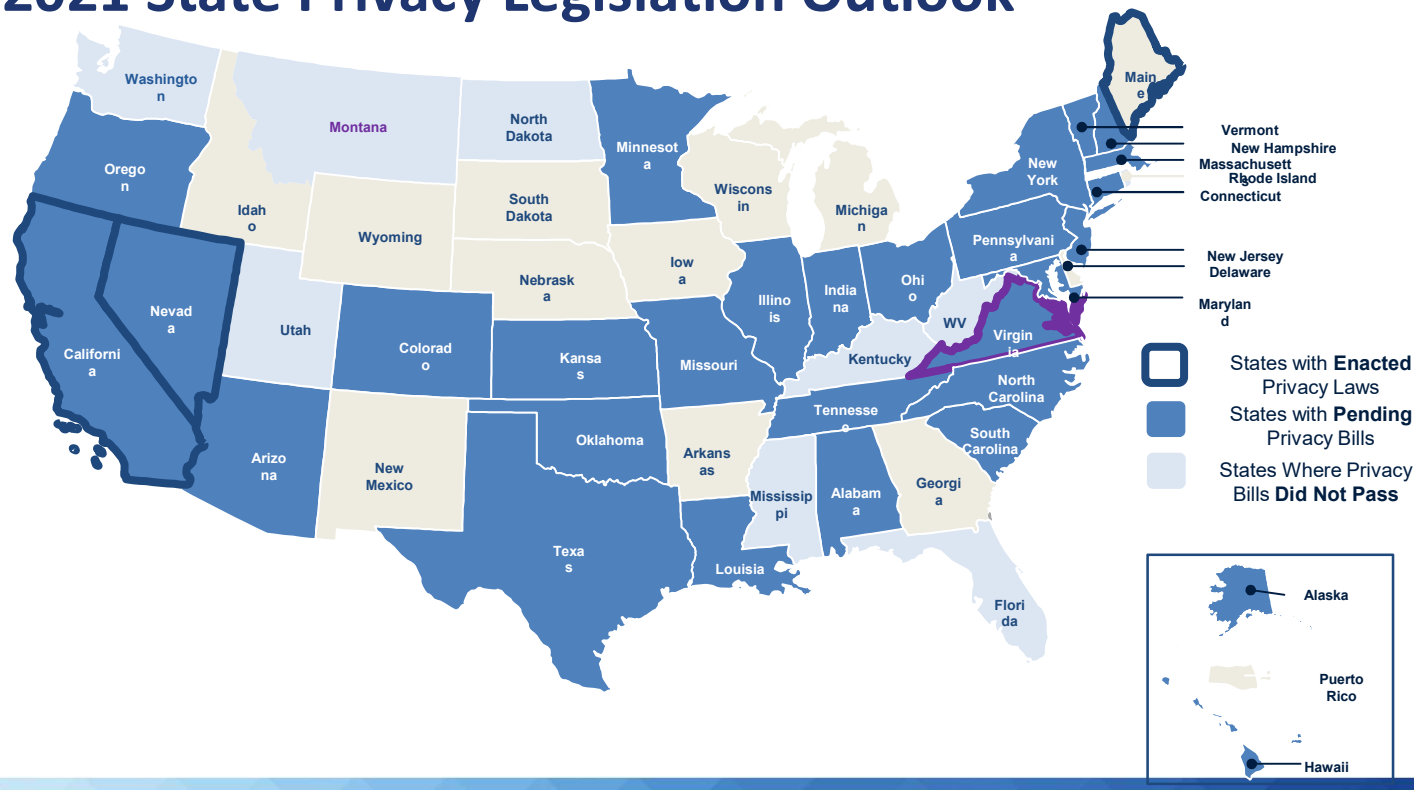
- Introduction
- State Privacy Legislation Outlook
- Virginia Consumer Data Protection Act
- Federal Privacy Legislation Outlook
- FTC Priorities
- State Enforcement

State Privacy Legislation Outlook

Privacy+ Security Forum

Privacy+ Security Forum

2021 State Privacy Legislation Outlook



Costs of Patchwork of State Privacy Laws

- The total cost of initial compliance with the CCPA, which constitutes the vast majority of compliance efforts, is approximately $55 billion. This is equivalent to approximately 1.8% of California Gross State Product in 2018.
- A preliminary estimate of direct compliance costs is estimated to be $467-$16,454 million over the next decade (2020-30), depending on the number of California businesses coming into compliance.

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

Florida TaxWatch

Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations

Table 1. Total Cost of Initial Compliance

Employees	Number of Firms	Cost per Firm	Total Cost of Initial Compliance
<20	409,941	$50,000	**$20.49 Billion**
20-99	31,289	$100,000	**$3.12 Billion**
100-499	7,167	$450,000	**$3.22 Billion**
500+	4,821	$2,000,000	**$9.64 Billion**
		Total	**$36.50 Billion**

Pending State Privacy Laws

- Select overviews of pending state laws:
  - New York S2886, A405, A680, and several more:
    - The New York proposals offer a wide range of approaches, including rights-based bills, consent for the transfer of data, the creation of a "data fiduciary" requirement that includes duties of care, loyalty, and confidentiality, and requirements to secure data against privacy risks.
  - Texas HB 3741:
    - Rights-based bill, with different requirements for different "categories" of information, *i.e.*, a flat prohibition on transfers of "category two information" to third parties and processing "category three information."

Pending State Privacy Laws

- Select overviews of pending state laws:
  - Colorado SB 21-190:
    - Rights-based bill with a general opt-out of processing, a requirement to send rights requests to third parties to which data was disclosed. There is a limited exception for pseudonymized data and no private right of action.
  - Connecticut SB 893:
    - Rights-based bill with a general opt-out of processing, a requirement to send rights requests to third parties to which data was disclosed. There is a limited exception for pseudonymized data and no private right of action.

- Various additional bills ranging from selective privacy rights, geolocation data, employee privacy, data brokers registration, student privacy, social media, and more across 20+ jurisdictions.

Failed State Bills

- Bills that died in session:
  1. Florida:
     - HB 969 and SB 1734 failed to pass the legislature.
     - The bill was rights-based bill, with 2-year data retention restrictions, a 2-day opt-out requirement, explicit notice requirements, and a broad private right of action
  2. Washington:
     1. SB 5062 failed to pass due to disagreements between the House and Senate.
        1. A rights-based bill, like VA. Passage failed due to disagreement over a private right of action.
  3. Other state bills that failed to pass:
     KY, MS, MT, ND, UT, WV

Virginia Consumer Data Protection Act

Privacy+ Security Forum

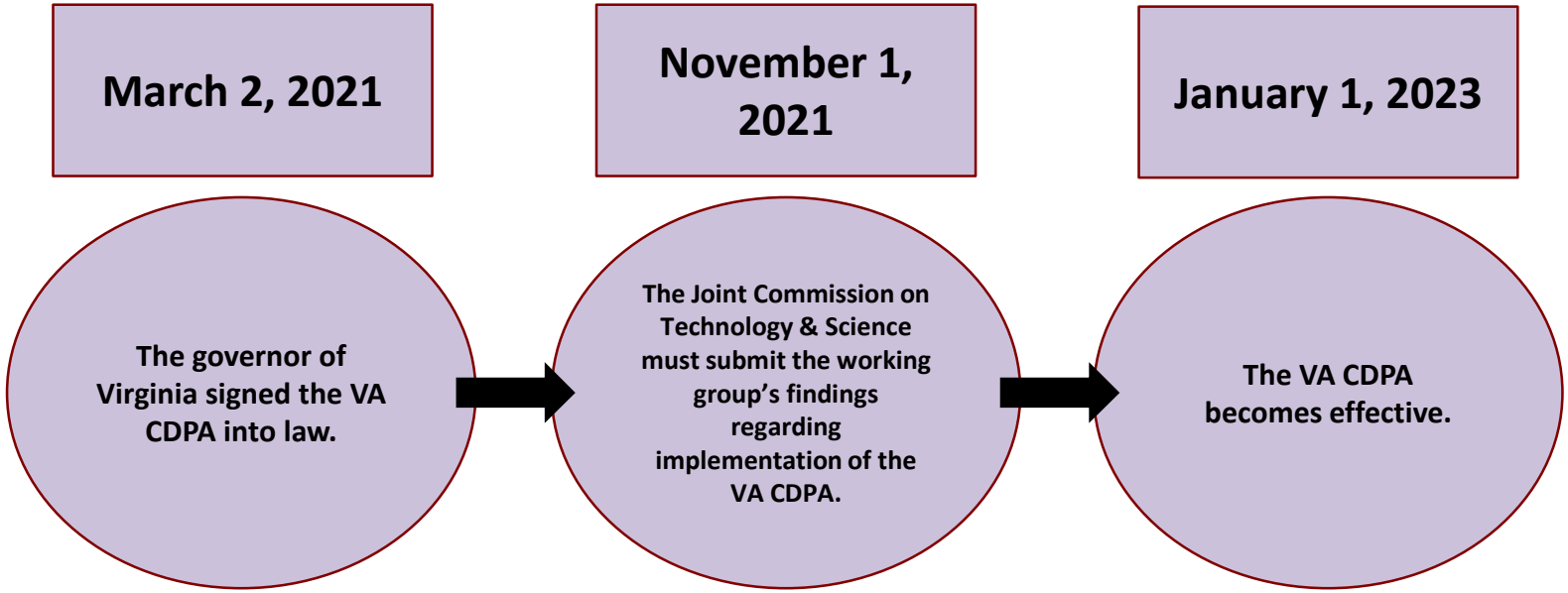
Overview of the Virginia Consumer Data Protection Act

- The Virginia Consumer Data Protection Act (VA CDPA) was signed into law on March 2, 2021, making Virginia the second state after California to pass a comprehensive state privacy law.
  - Nevada and Maine have also enacted more limited privacy laws in recent years.
- The VA CDPA includes concepts similar to those of the California Consumer Privacy Act of 2018 (CCPA), the California Privacy Rights Act of 2020 (CPRA), and the European Union's General Data Protection Regulation (GDPR).
  - The VA CDPA is a rights-based law, offering consumers specific rights with respect to personal data collected about them.
- Enforcement is limited to the Virginia attorney general (no private right of action, unlike the CCPA/CPRA).
  - Controllers and processors accused of a violation will have a 30-day period to cure alleged violations, after which the Virginia attorney general can seek damages of up to $7,500 per violation.

Report on Implementation of the VA CDPA

- The VA CDPA mandates the chairman of the Joint Commission on Technology and Science (JCOTS) to create a working group consisting of:
  - the Virginia Secretary of Commerce and Trade;
  - the Virginia Secretary of Administration;
  - the Virginia Attorney General;
  - the Virginia Chairman of the Senate Committee on Transportation;
  - Representatives of businesses that control or process personal data of at least 100,000 persons; and
  - Consumer rights advocates.

VA CDPA Timeline: Key Dates



Threshold Issues: Scope of the VA CDPA

The VA CDPA applies to any person or entity that:

- Conducts business in Virginia; or
- Produces products or services that are targeted to residents of Virginia and that either:
  - Controls or processes personal data of at least 100,000 consumers annually, or
  - Controls or processes personal data of at least 25,000 consumers and derives over 50% of its gross revenue from sales of personal data.
    - Note that unlike the CCPA and CPRA, Virginia does not set a pure gross revenue threshold ($25 million in CA) that brings a business within the law's scope; the revenue threshold under the VA CDPA is combined with a requirement to process personal data of at least 25,000 Virginia consumers.

Key VA CDPA Definitions

- **"Controller"** is defined as "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."

- **"Processor"** is defined as "a natural or legal entity that processes personal data on behalf of a controller."

- **"Personal data"** is defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." It does not include de-identified or publicly available information.

Consumer Rights

Under the VA CDPA, consumers have the right to:

1. **Access** personal data that a controller collects about them;
2. **Correct inaccuracies** in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's data;
3. **Delete** personal data provided by or obtained about the consumer;
4. **Obtain a portable copy** of the consumer's personal data to transmit to another controller (right to portability); and
5. **Opt out of the processing of personal data** for the purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

VA CDPA Opt-Out Right

- Under the VA CDPA, consumers have the right to opt out of the processing of personal data for the purposes of:
  1. **Targeted advertising**, which is defined to mean "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests."
  2. **Sales** of personal data; or
  3. **Profiling** in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. "Profiling" is defined to mean any form of automated processing performed on personal data to evaluate, analyze, to predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

Pseudonymous Data Exemption for Most Consumer Rights

- **Pseudonymous data is exempt from the consumer rights under the VA CDPA except for the right to opt out**, so long as any information necessary to identify the consumer is kept separate from the pseudonymous data and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

- The VA CDPA defines **"pseudonymous data"** as personal data that cannot be attributed to a specific person without additional information, provided that such additional information is kept separate and is subject to appropriate measures to ensure that the personal data is not attributed to an identifiable person.

Opt-In Consent Required for Processing Sensitive Data

- The VA CDPA is an opt-out regime, except for **"sensitive data," which requires consent for processing**. Controllers may not process sensitive data absent opt-in consent from a Virginia consumer.

- **"Sensitive data"** under the VA CDPA includes (1) personal data revealing race or ethnicity, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship/immigration status; (2) processing of genetic or biometric data for the purpose of identifying a natural person; (3) personal data collected from a known child; and (4) precise geolocation data.

Appeals Process Required

- The VA CDPA requires controllers to establish a process for consumers to **appeal** the controller's decision not to take action on a consumer rights request.
  - The appeal process must be conspicuously available and similar to the process for submitting rights requests.
  - A controller must respond in writing within **60 days** of receiving an appeal informing the consumer of any action taken or not taken and explaining the reasons for its decisions.
  - If the appeal is denied, the controller must also provide the consumer with a **method of submitting a complaint to the Virginia attorney general.**

Data Protection Assessments Required

- The VA CDPA requires controllers to conduct **data protection assessments** (DPAs) for certain processing activities, such as:
  - Processing involving **targeted advertising**;
  - **Sales of personal data**;
  - Profiling that could lead to a **risk of harm to the consumer**;
  - Processing **sensitive data**; and
  - Any other processing that could lead to a **heightened risk of harm to consumers**.

- Controllers must maintain these DPAs. The Virginia attorney general may request such DPAs if they are relevant to an ongoing investigation by the Virginia attorney general. In the event of such a request, controllers must turn their DPAs over to the AG.

VA CDPA Privacy Notice Requirements

- Requires privacy notices that include:
  1. The categories of personal data processed;
  2. The purpose(s) for processing personal data;
  3. How consumers can exercise their rights and how to appeal a controller's decision not to act on a rights request;
  4. The categories of personal data the controller shares with third parties; and
  5. The categories of third parties with whom the controller shares personal data.

- If applicable, the VA CDPA requires controllers to disclose how they sell or process personal data for targeted advertising and the manner in which a consumer can opt out of targeted advertising.

Privacy+ Security Forum

VA CDPA vs. CCPA (CA) vs. CPRA (CA) vs. General Data Protection Regulation (GDPR) At-a-Glance

Requirement	VA CDPA	CCPA	CPRA	GDPR
Right of Access	X	X	X	X
Right of Rectification	X		X	X
Right of Deletion	X	X	X	X
Rights Pertaining to Sensitive Information (opt-in or limitation on use right)	X		X	X
Right of Portability	X	X	X	X
Right to Opt-Out	X	X	X	X
Right to Appeal	X			X
Right Against Automated Decision-Making	X			X
Private Right of Action		X	X	X
Opt-In Age Requirement	13	16	16	13-16
Notice/Transparency Requirement	X	X	X	X
Risk Assessments	X		X	X
Prohibition on Discrimination/Retaliation	X	X	X	
Purpose/Processing Limitation	X	X	X	X
Legal Basis and/or General Consent				X

Virginia & California: Differences

- Thresholds for each law's applicability are slightly different
  - No pure revenue threshold imposing obligations under VA CDPA
- Slight, but important, differences in consumer rights
- Varying approaches to treatment of sensitive data
- Different enforcement mechanisms and regulatory authority

Federal Privacy Legislation Outlook

Privacy+ Security Forum

Proposed Federal Legislation

- Information Transparency and Personal Data Control Act (HR 1816 DelBene D-WA):

  A comprehensive privacy bill that does not include individual rights, but that would provide a broad opt-out of data collection, use, and transfer, the right to opt-in for sensitive data, and FTC and state AG enforcement. The bill provides for preemption and no private right of action.

- Online Consumer Protection Act (Schakowsky D-IL & Castor D-FL):

  Would enact a large overhaul of Section 230

- Data Care Act (S 919 Schatz D-HI):

  A bill to create a duty of care and loyalty for online service providers. Enforcement by the FTC & state AGs. No preemption of state laws.

Proposed Federal Legislation

- Children and Teens' Online Privacy Protection Act (Markey D-MA 7 Cassidy (R-LA):

  The bill would amend the Children's Online Privacy Protection Act (COPPA) to require consent from consumers that are 13 to 15 years old for data collection and prohibit targeted advertising "directed at children."

- Promoting Digital Privacy Technologies Act (S 224 Cortez Masto D-NV/HR 847 Stevens D-MI):

  Supports research on privacy enhancing technologies and promote responsible data use.

- Fourth Amendment Is Not For Sale Act (S 1265 Wyden D-OR/HR 2738 Nadler D-NY).

  Prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers.

One National Privacy Standard:

- Privacy for America is an industry coalition that supports enactment of federal legislation that would clearly define prohibited data practices that make personal data vulnerable to breach or misuse, while preserving the benefits that come from responsible use of data.
- P4A's proposal would create reasonable and unreasonable uses of consumer data, while also giving the FTC increased funding for enforcement and regulation.
- www.PrivacyforAmerica.com

FTC Priorities – 2021 and beyond

Privacy+ Security Forum

Key Areas of Focus

- Privacy issues raised by the pandemic
- Privacy and racial equity
- Creating incentives for good privacy practices/remedies

State Enforcement

Privacy+ Security Forum

Multistate Announcements:

- Anthem
- Community Health Systems
- Retrieval Masters Creditors Bureau
- The Home Depot
- Sabre
- CaféPress
- 44 AGs to Facebook: Abandon Instagram for Kids

State Enforcement Cases Cont.

- New York – “Dunkin to Fill Holes…”
- Washington – MapleMedia LLC (“We Heart It”)
- California – Glow, Inc.
- CT/DC – PreMom
- Texas – HB 4390 implementation
- Indiana – Equifax restitution under way

Predictions/Trends

Litigation

- Equifax
  - 3 states sued: Massachusetts, West Virginia, and Indiana
- Facebook
  - *District of Columbia v. Facebook*
  - *Massachusetts v. Facebook*
- *New Mexico v. Google* (COPPA)
- *Vermont v. Clearview*

Settlement Terms

- Injunctive terms
- Consumer redress

Privacy+ Security Forum

Questions?

Questions + Contact

Reed Freeman
RFreeman@venable.com

Maneesha Mithal
MMITHAL@ftc.gov

Esther Chavez
esther.chavez@oag.texas.gov

Christopher Oswald
coswald@ana.net

Chelsea Reckell
CBReckell@venable.com