National Reverse Mortgage Lenders Association

Annual Meeting & Expo

November 18-20, 2019 Nashville, TN

A Sea Change in Privacy Protections: What California and Other States Are Requiring

November 19, 2019

Panelists:

Soroush Shahin — Weiner Brodsky Kider PC

Jay Wright — Bradley Arant Boult Cummings LLP

Agenda

- Background
- Scope & Exceptions
- Enforcement & Private Right of Action
- Privacy Rights
- CCPA Amendments
- CCPA 2.0 – Ballot Initiative
- CCPA Regulations
  - Disclosures and Do Not Sell
  - Privacy Policy
  - Verified Consumer Requests, Verification, & Authorized Agent
  - Training, Record Keeping, & Financial Incentive
  - Service Providers
  - Miscellaneous
- Other State Laws

Background

- On June 28, 2018, California enacted the **California Consumer Privacy Act (CCPA)**
  - Goes into effect on **January 1, 2020**
- Broadest and most comprehensive privacy law in US to date
  - "**GDPR-like**" consumer privacy rights
- CA legislature passed CCPA quickly to **avert a proposed ballot initiative** that sought to impose even more stringent requirements
  - **Rush to pass** ➡ ambiguity & uncertainty
- Recent amendments and proposed regulations clarified some issues, but there is **still a lot of work that needs to be done**

Background

- CA Constitution states right of privacy is an "**inalienable**" right
- Builds on **other CA privacy laws**
  - Online Privacy Protection Act
  - Shine the Light Law
  - Privacy Rights for California Minors in the Digital World Act
- CA legislature stated the **need for enhanced consumer privacy rights**
  - Law has **not kept pace with technological developments** and privacy implications surrounding collection, use, and protection of personal information
- Specifically cites to March 2018 **disclosure and misuse** of personal data by data mining firm (Cambridge Analytica)
  - Also references **congressional hearings** that followed which highlighted the fact that personal information shared on the internet can be subject to misuse

Scope – Key Terms

Three **key definitions**:

- Business
- Consumer
- Personal Information

Scope – Key Terms

- "**Business**" is defined as any for-profit entity that (i) does business in California, (ii) collects PI of consumers, (iii) determines on its own or jointly with others the purpose and means of processing that information, and (iv) meets **one** of the following criteria:
  - Has annual gross revenues **in excess of $25 million**, adjusted for inflation
  - Annually buys, receives for a commercial purpose, sells, or shares for commercial purpose PI of **50,000 or more** consumers, households or devices
  - **Derives 50%** or more of its annual revenue from selling consumers' PI
- Also includes any entity that "**controls**" or is "**controlled**" by a "business" and that "**shares common branding**" with the "business"

Scope – Key Terms

- "**Consumer**" means a natural person who is a California "**resident**," as defined under the California tax provisions
  - Includes:
    - Every individual who is in California for other than a temporary or transitory purpose
    - Every individual who is domiciled in California but is outside California for a **temporary or transitory purpose**
  - Whether or not a purpose is considered "**temporary or transitory**" will **depend on facts and circumstances** of each particular case

Scope – Key Terms

- "**Personal information**" means info that identifies, relates to, describes, is *reasonably* capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
- "**Personal information**" includes:
  - Identifiers such as name, address, personal identifier, IP address, email address, account name, SSN, driver's license number, or passport number
  - Commercial info, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies
  - Geolocation data
  - Biometric info
  - Internet or other electronic network activity info, including browsing history, search history & info regarding consumer's interaction with a website, application or advertisement

Scope – Key Terms

"**Personal information**" includes (cont'd):

- Any categories of PI described in Cal. Civ. Code § 1798.80(e) (e.g., signatures, telephone numbers, bank account numbers, credit/debit card numbers)
- Audio, electronic, visual, thermal, olfactory or similar info
- Professional or employment-related info
- Education info, defined as info that is not publicly available personally identifiable info as defined in the Family Educational Rights and Privacy Act
- Characteristics of protected classifications under California or federal law
- Inferences drawn from any of the above info to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes

Scope – Key Terms

"**Personal information**" does **not** include:

- **Publicly available information**
  - Info lawfully available from federal, state, or local government records
- **Aggregate consumer information**
  - Info that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device
- **Deidentified information**
  - Info that cannot reasonably identify, relate to, describe, be capable of being associated with or be linked to a particular consumer, provided that business makes no attempt to reidentify info and has implemented: (i) technical safeguards that prohibit reidentification of consumers, and (ii) business processes: (A) to prevent inadvertent release of deidentified info, and (B) that specifically prohibit reidentification of the info

Exceptions

- Obligations imposed by CCPA do **not** restrict a business' ability to:
  - Comply with federal, state, or local laws
  - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities
  - Cooperate with law enforcement agencies concerning conduct or activity that entity reasonably believes may violate federal, state, or local law
  - Exercise or defend legal claims
  - Collect or sell a consumer's PI ***if every aspect of that commercial conduct takes place wholly outside of CA***
    - If business collected info while consumer was outside of CA, no part of sale of consumer's PI occurred in CA, and no PI collected while consumer was in CA is sold

Exceptions

- Does **not** apply to PI collected, processed, sold, or disclosed pursuant to:
  - California Financial Information Privacy Act (CFIPA)
  - Gramm-Leach-Bliley Act (GLBA)
- CCPA also provides a Fair Credit Reporting Act (FCRA) exemption
  - Expanded by recent amendments

- ***Still subject to CCPA's data breach provisions***

Enforcement

California Attorney General

- Not allowed to bring enforcement action until 6 months after publishing ***final*** regulations or July 1, 2020, whichever is sooner
- 30-day notice and cure period
- Injunction
- Civil penalties
  - $2,500 for each unintentional violation
  - $7,500 for each intentional violation
- Consumer Privacy Fund
  - Offset costs incurred by courts and AG
- Can seek AG opinion for guidance on how to comply with CCPA

Private Right of Action

Data Breaches

- Goes into effect on January 1, 2020
- Injunctive or declaratory relief
- Statutory damages
  - $100 to $750 per consumer per "**incident**," or actual damages (whichever is greater)
  - Consumer's nonencrypted and nonredacted ***personal information*** was subject to unauthorized access and exfiltration, theft or disclosure as a result from the business' ***failure to implement and maintain reasonable security procedures and practices*** appropriate to the nature of that information
- Slightly narrower definition of "**personal information**"
  - Now also includes biometric data, tax ID numbers, passport numbers, military ID numbers, and unique identification numbers issued on government documents
- Must give written notice (30 days) before filing action for statutory damages
  - No notice required if consumer **suffered actual pecuniary damages**

Privacy Rights

- **Right to Know (Disclosure and Access)**
  - The right to know what PI is collected, used, disclosed or sold (and to whom)
- **Right to Delete**
  - The right to delete PI that has been collected
- **Right to Opt Out**
  - The right to opt out of the sale of their PI to third parties
- **Right to Nondiscrimination**
  - The right to equal service and price, whether or not rights under CCPA are exercised

Right to Disclosure

- **At or before the point of collection**, must disclose categories of PI to be collected and purposes for which categories of PI will be used
  - Must not collect additional categories of PI or use PI for other purposes without notice

- **Privacy Policy**
  - A description of:
    - Designated methods for consumers to submit requests
    - Consumers' rights under CCPA
  - Must generally disclose:
    - Categories of PI collected and sold
    - Categories of sources from which PI is collected
    - Categories of PI business has disclosed for a business purpose
    - Categories of third parties with whom business shares PI
    - Business or commercial purposes for collecting or selling PI
  - Link to "Do Not Sell My Personal Information"
  - Update once every 12 months

Right to Access

- Upon receiving a **verifiable consumer request (VCR)**, must generally disclose **(free of charge)**:
  - Specific pieces of PI business has collected
  - Categories of PI it has collected or sold
  - Categories of sources from which PI was collected
  - Categories of PI disclosed for business purpose
  - Categories of third parties to whom the PI was sold or shared
  - Business or commercial purpose for collecting or selling PI

- **Response Time**
  - Within 45 days of VCR (can be extended for additional 45 days upon notice)
- **12-Month Period**
  - Response must cover 12-month period preceding consumer's request
  - Not required to comply with consumer's request more than twice in 12-month period
- **Delivery Method**
  - Consumer's account, mail or electronically (**portable** and in a readily usable format)

Right to Delete

- Upon receiving VCR, business **must delete PI and direct service providers to delete PI**
- **Response Time**
  - Within 45 days of VCR (can be extended for additional 45 days upon notice)
- **Exceptions** (not required to delete PI if necessary to):
  - Complete transaction, provide good or service, or otherwise perform contract with consumer
  - Detect security incidents
  - Debug and identify/repair errors that impair functionality
  - Comply with California Electronic Communications Privacy Act
  - Exercise free speech or exercise another right
  - Engage in certain public or peer-reviewed scientific, historical, or statistical research
  - Enable internal uses that are reasonably aligned with consumer's expectations
  - Comply with a legal obligation
  - Otherwise use PI, internally, in lawful manner compatible with context in which info was given

Right to Opt Out

- Consumers have right to **opt out** of a business's sale of their PI to third parties

- **Authorized Agent**
  - Consumer may authorize an agent to opt out of sale of PI on their behalf
- **Notice**
  - Clear and conspicuous link ("Do Not Sell My Personal Information") on Internet homepage, privacy policy, & any California-specific description of consumers' privacy rights
- **Training**
  - Individuals responsible for handling privacy inquiries or CCPA compliance must know CCPA requirements, including opt-out right, and how to direct consumers to exercise their rights
- **Requesting New Consent**
  - Cannot request authorization from consumer to sell PI for at least 12 months
- **Minors**
  - Stricter requirements (must opt in)

Right to Nondiscrimination

- Businesses are **prohibited from discriminating** against consumers who have exercised their rights under CCPA
- **Examples**
  - Denying goods or services
  - Charging different prices or rates
  - Imposing penalties
  - Providing different level/quality of goods or services
- **Exceptions**
  - May charge different price, or provide different level/quality of goods or services, or ***offer financial incentives*** if reasonably related to value provided to business by consumer's data
  - Must not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature

CCPA Amendments

- CA enacted several bills that amend CCPA the day after AG released proposed regulations

- **Partial exemption for employees and B2B communications/transactions**
  - PI collected from natural person acting as an employee, job applicant, owner, director, officer, or contractor of the business to the extent that the PI is collected and used solely within the context of that person's role or former role
    - Includes PI collected for emergency contact info and benefit administration
    - Not exempt from certain notice requirements (e.g., notice at or before collecting PI)
  - PI reflecting a communication or a transaction between business and consumer who is acting as an employee, owner, director, officer, or contractor of a company and whose communication or transaction with business occur solely within context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company
    - Not exempt from right to opt out of sale of PI
  - Still subject to data breach requirements
  - ***One-year sunset provision (expires January 1, 2021)***

CCPA Amendments

- **Expanded FCRA exemption**
  - Exempts activity involving collection, maintenance, disclosure, sale, communication, or use of PI bearing on consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by CRA, furnisher, and user of credit report
  - Only applies to the extent that such activity or use of PI is subject to regulation under FCRA, and PI is not used, communicated, disclosed, or sold except as authorized by FCRA
  - Still subject to data breach provisions
- **Revised requirements for consumer requests**
  - Business that operates exclusively online and has direct relationship with consumer is permitted to provide only an email address for consumer requests
  - May require authentication of consumer that is reasonable in light of the nature of PI requested, and if consumer maintains an account with business, require consumer to submit request through that account
- **Also fixed (some) drafting errors**

CCPA 2.0 – Ballot Initiative

- Would create **California Privacy Rights and Enforcement Act (CPREA)**
  - CCPA 2.0
  - Concerned recent amendments have "weakened" CCPA
  - 623,212 signatures needed

- **Some key changes**:
  - Establishes new agency – California Privacy Protection Agency
  - Adds new category of "sensitive personal information" (e.g., SSN, government ID number, financial info, geo location) that would be subject to additional requirements
  - Grants consumers a right to correct inaccurate PI (similar to GDPR)
  - Revises definition of "business" to mitigate burden on small businesses
    - Proposed: Annually buys or sell PI of **100,000** or more consumers or households
    - Current: Annually buys, ***receives for a commercial purpose***, sells or ***shares for commercial purpose*** PI of ***50,000*** or more consumers, households ***or devices***
  - Includes partial exemption for employees and B2B communications/transactions

CCPA Regulations

Disclosures and Do Not Sell 01

Privacy Policy 02

Verified Consumer Requests, Verification and Authorized Agent 03

Training, Record Keeping, Financial Incentive 04

Service Providers 05

Miscellaneous 06

Disclosures

Notice and Disclosure At Point of Collection

- Notice at point of collection must:

  - **Be easy to read**
  - **Use plain, straightforward language**
  - **Use a format that draws attention to notice and makes it readable on smaller screens**
  - **Be available in languages used in the ordinary course of business to provide contracts, notices, etc.**
  - **Be ADA accessible (at a min. provide information on how disabled can access in alternative format).**

- Business cannot collect or use any PI unless the PI and all uses were disclosed at the point of collection

Notice and Disclosure At Point of Collection

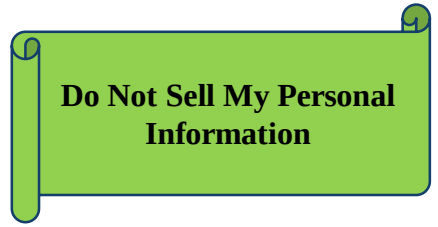
- Notice must include:
  - List of categories of PI collected. Each category must provide consumers "a meaningful understanding" of the information being collected
  - Business or commercial purpose and use of each category of PI
  - "Do Not Sell My Personal Information [Info]" link
  - Link to business's privacy policy (or website address)
- Notice must be provided offline if PI collected outside of website (*i.e.* in-person retail, call center, etc.)
- Pop-up to (or direct reference to) link to notice requirements (*i.e.* specific section within privacy policy) allowed

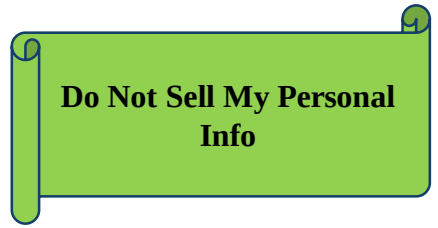
Do Not Sell

Do Not Sell—Opt-Out Notice

- Notice of opt-out of current or future selling; must:

  - **Be easy to read**
  - **Use plain, straightforward language**
  - **Use a format that draws attention to notice and makes it readable on smaller screens**
  - **Be available in languages used in the ordinary course of business to provide contracts, notices, etc.**
  - **Be ADA accessible (at a min. provide information on how disabled can access in alternative format).**





- Opt-Out notice must be provided at point of offline collection of personal information (e.g. printing the notice on paper forms that collect PI, providing consumer with paper version of notice, or posting signage directing consumer to website).

Do Not Sell—Opt-Out Notice

- Opt-Out Notice must include:
  - Description of consumer's right to opt-out
  - The interactive webform by which a consumer can submit their request to opt-out online (or offline method if no website maintained)
  - Instructions for any other method of opt-out submission
  - Any proof required when a consumer uses an authorized agent to exercise their right to opt-out
  - A link to the business's privacy policy
- Exempt Business
  - Does not *and* **will not** sell personal information collected during the time period during which notice of opt-out is not posted; and
  - Privacy policy states that business does not and will not sell personal information.

Do Not Sell—Opt-Out Notice

- Two or more designated request forms—one must be link, other is flexible.
- Business must treat user-enabled privacy controls (such as privacy setting) as a communication or signal of the consumer's choice to opt-out of sale

This can be read to require a business to constantly monitor for plug-ins that purport to "communicate or signal the consumer's choice to opt-out." It is imposing the requirement on businesses with no standardized framework to send and process these signals.

Do Not Sell—Opt-Out Notice

- Business may present consumer with choice to opt-out of certain categories as long as global option also available
- Opt-out request must be completed within 15 days
- Business must notify all third parties to whom it sold information in the last 90 days and instruct not to further sell—***business must notify consumer when completed***
  - Is this required to be in a contract?
  - Companies must keep track of all information sold going back 90 days?
  - What if you sell multiple pieces of consumer information at different time periods?

Opting In After Opting Out

- Opt-in requires a two step process
  - Request opt-in
  - Confirm choice to opt-in
- Business may inform a consumer who has opted-out when a transaction requires the sale of personal information as a condition of completing the transaction

Practical Application – No Direct Consumer Contact

- Question: I receive leads from another business (*i.e.*, I do not collect information directly from the consumer), do I need to provide the opt-out notice before I can sell (share for consideration)?
- Answer: Yes, unless you do one of the following:

  1. You contact the consumer directly to provide the opt-out notice and provide the opportunity to opt-out

  OR

  2. You confirm the source provided an opt-out notice at collection AND obtain signed attestations form the source describing how the source gave the opt-out notice AND attach a copy of the notice.

Privacy Policy

“Purpose of privacy policy is to provide consumer with comprehensive description of business’s online and offline practices”

Privacy Policy

- Privacy policy must include:
  - "Right to Know"
  - Right to Request Deletion
  - Right to Opt-Out of Sale
  - Right to Non Discrimination
  - Authorized Agent
  - Contact for More Information
  - Date of last update
  - Metrics under section 999.317(g)(1) (if applicable)

Practical Questions for Privacy Policy

- Privacy Policy must include this information:
  - What process will business use to verify the consumer request, including any information the consumer must provide?
    - How does the business avoid ID theft by providing road-map here?
    - Will business use challenge questions that need to be obtained at the point of data collection?
  - How can a consumer designate an authorized agent to make a request under CCPA on the consumer's behalf?
    - What mechanism will business use to allow designation of authorized agent?
    - How will company verify the authorized agent?

Verified Consumer Requests

Verified Consumer Request

- Requirement Overview
  - Request to Know: 2 or more designated request methods, including: (1) "Interactive" webform on website and (2) toll-free telephone number;
  - Request to Delete: 2 or more designated request methods, including: toll-free telephone number; online form; email address; in person; or mail-in form;
- Business should consider how it typically interacts with consumers when determining best methods
- VCR for deletion requires two step process (1) request and (2) separate confirmation of deletion
- If consumer submits a VCR that is NOT one of the business' designated methods, the business MUST: (1) treat it as a valid VCR; or (2) provide specific directions on how to submit the request or remedy any deficiencies with the request.

Verified Consumer Request--Responding

- Business shall confirm receipt of VCR **within 10 days**
  - Response must:
    - Provide information about how the business will process the request;
    - Describe business's verification process; and
    - When the consumer should expect a response.
- If "Right to Know" request (re:) specific categories of information is denied because of inability to verify consumer, business shall still provide categories of information collected.
- Business MUST NOT disclose: SSN, DL# (or government issued ID), financial account number, health insurance or medical ID#, account password, or security questions/answers.

Verified Consumer Request--Responding

- If business denies the request to know specific pieces of personal information due to conflict with state/federal law, or exception to CCPA, the business must inform the requestor and explain the basis for denial.
  - If request is denied in part, the business must disclose the other information sought by consumer
- Business must use reasonable security measures when transmitting personal information to consumer
- 12-month period runs from the time the consumer submitted the request, regardless of how long it takes to comply
- In responding to consumer's request for categories—business shall provide an individualized response and cannot point consumer to general privacy policy (unless response would be the same for all consumers).

Verified Consumer Request--Responding

- Business must provide response for each identified category of PI it has collected on consumer:
  - Categories of sources from which PI collected
  - Business/Commercial purpose of collection
  - Categories of third parties sold or disclosed to
  - Business/Commercial purpose for selling or disclosure
- If unable to verify consumer for deletion request—MUST treat as a request to opt-out of sale
- Deletion can include:
  - Permanently and completely erasing (except archive/backups*)
  - De-identifying personal information; or
  - Aggregating the personal information.

*Note: AG regulations require deletion when archive or backups are “next accessed or used”

Verified Consumer Request--Responding

- Business must provide method of deletion used in response to consumer
- Business must disclose that it will maintain a record of the request
- If request is denied, business must:
  - Describe basis for denial, including any statutory and regulatory exception therefor;
  - Delete any information not subject to exception;
  - Not use the consumer's personal information retained for any other purpose than provided for in that exception.
- Business may provide consumer with option to delete select portions of their personal information ONLY if a global option to delete is also offered.

Verification

Verification

- Methodology:
  - Match “identifying information” provided by the consumer to the PI of consumer maintained by business, or use a third-party verification service that complies with this section.
  - Avoid collecting SSN, DL# (or government issued ID), financial account number, or medical information as part of verification process
  - Sliding scale of verification necessary depending on sensitivity of data
  - Consider risk of harm by unauthorized access/deletion and likelihood that fraudulent or malicious actors would seek personal information
  - Verification must be sufficiently robust to protect against fraudulent activities
  - Consider manner of interaction with consumer and availability of technology for verification

Verification

- Business must implement reasonable security measures to detect fraudulent identity verification activity
  - Including requests made through existing accounts
- Verification can be made through existing account
- "Reasonable Degree of Certainty" required to disclose categories of personal information
  - "reasonable" may include matching at least **two *reliable*** data points provided by consumer and maintained by business
- Example:
  - Business maintains consumer's name and credit card information
    - Could require consumer to provide CVV and most recent purchase information (reasonable degree of certainty)

Verification

- "High Degree of Certainty" required to disclose specific pieces of personal information
  - "high degree" may include matching at least **three *reliable*** data points provided by consumer and maintained by business **together with a signed declaration** under penalty of perjury that requestor is consumer whose personal information is subject to request
- Deletion may require reasonable or high degree of certainty based on information requested for deletion
- **Fact based verification process may be required** if business maintains personal information in a manner that is not associated with a named actual person
- Verification methodology must be evaluated on a yearly basis

Authorized Agent

Authorized Agent

- For deletion by authorized agent, business may require:
  - Consumer to provide written permission to authorized agent;
  - Consumer to verify their identity directly with the business

- If authorized agent has a power of attorney, then the above does not apply

- Authorized agent can be required to submit proof of authorization

Training, Record Keeping and Household Information

Training, Record Keeping, and Household Information

- Establish training policy
  - Training required
- Must maintain records of VCRs and how business responded for 24 months
- Metrics for large data collection required
- VCR request may pertain to household PI
  - May require verification of all members of household

Financial Incentive—
"program, benefit, or other offering, including payments to consumers as compensation for the disclosure, deletion, or sale of personal information"

Financial Incentive

- Notice of financial incentive must:

  - **Be easy to read**
  - **Use plain, straightforward language**
  - **Use a format that makes it readable on smaller screens**
  - **Available in languages used in the ordinary course of business to provide contracts, notices, etc.**
  - **Be ADA accessible (at a min. provide information on how disabled can access in alternative format)**
  - **Be available online or at physical location where consumers will see it before opting into the financial incentive**

Financial Incentive

- Notice of financial incentive must include:
  - Summary of financial incentive or price/service difference offered
  - Description of material terms of financial incentive or price/service difference (including categories of PI implicated)
  - How consumer can opt-in to the financial incentive
  - Notification of consumer's right to withdraw opt-in and how consumer may exercise right
  - ***An explanation of why financial incentive is permitted under CCPA,*** including: (a) good faith estimate of value of consumer's data; and (b) description of the method the business used to calculate the value of consumer's data

Service Providers

Service Providers

- Company can be a service provider under CCPA to a non-profit or entity that does not meet definition of business under CCPA
- A service provider can combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to detect data security incidents or protect against fraud or illegal activity
- Service provider shall direct consumer to submit VCR requests to business and provide contact information for the business
- Service provider can be business for PI it collects, maintains, or sells outside of role as a service provider

Miscellaneous

Other Requirements

- Minors
  - Opt-in requirement for minors under 13 years of age
  - Requirements for minors 13-16
  - Notices to minors under 16
- Non-Discrimination
- Calculating the Value of Consumer Data

Will Other States Follow California?

State Laws — Passed

- Maine Act to Protect the Privacy of Online Consumer Information
  - Prohibits broadband Internet access service providers from using, selling, distributing or permitting access to customer personal information for purposes other than providing services
    - Unless the customer expressly consents to that use, disclosure, sale, or access
  - Effective July 1, 2020
- Nevada (SB 220/Chapter 603A)
  - Requires sellers of consumer personal information to provide consumers with an option to opt-out of the sale of their information
  - Contains significant carve-outs
  - Effective October 1, 2019

State Laws — Pending

- Hawaii (SB 418)
- Illinois Data Transparency and Privacy Act (HB 3358)
- Louisiana Internet and Social Media Privacy and Protection Act (HB 465)
- Maryland Online Consumer Protection Act (SB 613)
- Massachusetts (SD 341/S 120)
- Minnesota (HF 2917/SF 2912)
- New Jersey (S2834)
- New York (SB S5642)
- Pennsylvania Consumer Data Privacy Act (HB 1049)
- Rhode Island Consumer Privacy Protection Act (S0234)
- Texas Consumer Privacy Act (HB 4518)
- Washington Privacy Act (SB 5376)