NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 4/20/23

		California	Virginia	Colorado	Utah	Connecticut	Iowa	Indiana	Montana*	Tennessee*
Enforcement and Controller Requirements	**Private Right Action**	Yes (§ 1798.150(c))	No (§ 59.1-579 (C))	No (§6-1-1310)	No	No	No	No (Chapter 8 Section 4)	No	No
	Right to Cure?	No (§1798.150(b))	Yes (30 days) (§ 59.1-579(B))	Yes (60 days). Sunsets on January 1, 2025. (§ 6-1-1311(d))	Yes (30 days) (§ 13-61-402 (3)).	Yes (60 days) (§ 11(b)). Right to cure is granted at Attorney General's discretion.	Yes (90 days) (§ 715D.8(4))	Yes (30 days) (Chapter 10 Section 3.(a))	Yes (60 days) Sunsets April 1, 2026 (§ 12).	Yes (60 days) Does not sunset (§ 47-18-3212(b)).
	Universal Opt-Out Mechanisms/Opt-out Preference Signals	Yes (GPC treated as "Do Not Sell" request) (Cal. Code Regs. tit. 11 § 999.315(a))	No	Yes (6-1-1306(a)) See Finalized Regs. Rule Part 5 for more information on implementing universal opt-out mechanism	No	Yes (§ 5)	No	No	Yes -- consumer may designate an authorized agent by way of technology, including a browswer setting (§ 6)	No
	Definition of Sale	(ad) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration. (2) For purposes of this title, a business does not sell personal information when: (A) A consumer uses or directs the business to intentionally : (i) disclose personal information; (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information. (C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. . . (1798.140(ad))	"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include: 1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller; 2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; 3. The disclosure or transfer of personal data to an affiliate of the controller; 4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or 5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets. (§ 59.1-575)	"sale", "sell", or "sold" means the exchange of personal data for monetary or othervaluable consideration by a controller to a third party. "sale", "sell" or "sold" does not include: (I) the dislcosure of personal data to a processor that processes the personal data on behalf of the controller; (II) The disclosure of personal data to a third party for the purpose of providing a product or service requested by a consumer; (III) the disclosure or transfer of personal data to an affiliate of the controller; (IV) disclosure or transfer as part of merger/bankruptcy, etc.; (V) the discosure of personal data: (A) that a consumer directs the controller to disclose or itentionally discloses by using the controller to interact with a third party; or (B) Intentionally made avaialble by a consumer to the general public (6-1-1303(23)).	"Sale," "sell," or "sold" means the exchange of personal data for monetary consideration by a controller to a third party. (b) "Sale," "sell," or "sold" does not include: (i) a controller's disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) a controller's disclosure of personal data to an affiliate of the controller; (iii) considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations; (iv) the disclosure or transfer of personal data when a consumer directs a controller to: (A) disclose the personal data; or (B) interact with one or more third parties; (v) a consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of child; (vi) the disclosure of information that the consumer: (A) intentionally makes available to the general public via a channel of mass media; and (B) does not restrict to a specific audience; or (vii) a controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, an acquisition, or a bankruptcy in which the third party assumes control of all or part of the controller's assets. (13-61-101(31))	"Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets. (1(26))	"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include: a. The disclosure of personal data to a processor that processes the personal data on behalf of the controller. b. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer or a parent of a child. c. The disclosure or transfer of personal data to an affiliate of the controller. d. The disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience. e. The disclosure or transfer of personal data when a consumer uses or directs a controller to intentionally disclose personal data or intentionally interact with one or more third parties. f. The disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party. (715D.1(25))	"Sale of personal data" means the exchange of personal data for monetary consideration by a controller to a third party. The term does not include: (1) the disclosure of personal data to a processor that processes the personal data on behalf of the controller; (2) the disclosure of personal data to a third party for purposes of providing a product or service requested by: (A) the consumer; or (B) the parent of a child; to whom the personal data pertains; (3) the disclosure or transfer of personal data to an affiliate of the controller; (4) the disclosure of information that the consumer: (A) intentionally made available to the general public via a channel of mass media; and (B) did not restrict to a specific audience; or (5) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets (Chapter 2, Sec. 27)	(a) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party." The term does not include: (i) the disclosure of personal data to a processor that processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party for the purposes of providing a product or service requested by the consumer; (iii) the disclosure or transfer of personal data to an affiliate of the controller; (iv) the disclosure of personal data in which the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; (v) the disclosure of personal data that the consumer: (A) intentionally made available to the public via a channel of mass media; and (B) did not restrict to a specific audience; or (vi) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets. (§ 2(23))	"Sale of personal information": (A) Means the exchange of personal information for monetary or other valuable consideration by the controller to a third party; and (B) Does not include: (i) The disclosure of personal information to a processor that processes the personal information on behalf of the controller; (ii) The disclosure of personal information to a third party for purposes of providing a product or service requested by the consumer; (iii) The disclosure or transfer of personal information to an affiliate of the controller; (iv) The disclosure of information that the consumer: (a) Intentionally made available to the general public via a channel of mass media; and (b) Did not restrict to a specific audience; (v) The disclosure or transfer of personal information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets; or (vi) The disclosure of personal information to a third party at the direction, and with the consent, of the consumer; (§ 47-18-3201(24))
	Defintion or references to of Pseudonymous Data	-Personal information -No connection to specific consumer without additional information -Must be kept separate -Subject to additional technical and organizational measures. (§ 1798.140 (r))		-Personal information -No connection to specific consumer without additional information -Must be kept separate -Subject to additional technical and organizational measures. (§ 6-1-1303 (22))	-Personal information -No connection to specific consumer without additional information -Must be kept separate -Subject to additional technical and organizational measures. (§ 13-61-101(28)).	-Personal information -No connection to specific consumer without additional information -Must be kept separate -Subject to additional technical and organizational measures. (§ 1(24)).	- Personal data - cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately - subject to appropriate technical and organizational measures (§ 715D.1(c)(23))	- Personal data - cannot be attributed to a specific individual because additional information that would allow the data to be attributed to a specific individual is: (1) kept separately; and (2) subject to appropriate technical and organizational measures; to ensure that the personal data is not attributed to an identified or identifiable individual. (Chapter 1 Section 25)	- personal data - cannot be attributed to a specific individual without the use of additional information provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. (§2(21))	- personal data - cannot be attributed to a specific natural person without the use of additional informaiton, so long as the additional information is kept separately and is subject to appropriate safeguards to ensure that personal information not attributed to an identified or identifiable person. (§47-18-3201(22))

NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 4/20/23

		California	Virginia	Colorado	Utah	Connecticut	Iowa	Indiana	Montana*	Tennessee*
Definitions and Exceptions	**Pseudonymous Data Exceptions**	-No requirement to respond to request to delete deidentified data (Cal. Code Regs. tit. 11 § 999.323(f)) -No requirement to respond to a request to provide deidentified data (Cal. Code Regs. tit. 11 § 999.323(f)) -No requirement to re-identify deidentified data (Cal. Code Regs. tit. 11 § 999.323(f)) -Obligations imposed on businesses by this title don't restrict a business' ability to collect, use, retain, sell or disclose consumer information that is deidentified (Cal. Civ. Code tit. 1.81.5 § 1798.145(a)(6))	1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;	- No requirement to respond to respond to request to delete pseudonymous data. - No requirement to respond to request to provide deidentified data. - No requirement to re-identify deidentified data - No requirement to pseudonymous data portable. - No requirement to correct pseudonymous data. Section 6-1-1307 (3)	-No requirement to reidentify pseudonynmous data (§ 13-61-303 (1)(a)) -No requirement to maintain pseudonynmous data in identifiable form or obtain, retain, or access any data or technology (§ 13-61-303(1)(b)) -No requirement to comply with a consumer request to exercise a right in § 13-61-202(1)-(3) if the controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome to do so, the controller does not use the personal data to recognize or respond to the consumer, or associate the personal data with other personal data about the consumer, and does not sell or otherwise disclose the personal data to any third party other than a processor, except as permitted (§ 13-61-303(1)(c)(i)-(iii)) -Consumer rights in § 13-61-201(1)-(3) do not apply to pseudonymous data where the information necessary to identify a consumer is kept separately and is subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual (§ 13-61-303(2)(a)-(b))	-No requirement to reidentify pseudonynmous data (§ 9(b)(1)) -No requirement to maintain pseudonynmous data in identifiable form or obtain, retain, or access any data or technology (§ 9(b)(2)) -No requirement to comply with a consumer rights request if the controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome to do so, the controller does not use the personal data to recognize or respond to the consumer, or associate the personal data with other personal data about the same consumer, and does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as permitted (§ 9(c)(1)-(3)) -Consumer rights in § 4(a)(1)-(4) do not apply to pseudonymous data where the controller can demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information (§ 9(d))	- no requirement for a controller or processor to re-identify de-identified pseudonymous data (§ 715D.6(1)(a)) - Consumer rights contained in section 715D.3 and 715D.4 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. (§ 715D.6(3))	No requirement to: (1) re-identify de-identified data or pseudonymous data; (2) maintain data in identifiable form; or (3) collect, obtain, retain, or access any data or technology; (Chapter 7 Section (b)(1-3) rights of a consumer set forth in IC 24-15-3-1(b)(1) through IC 24-15-3-1(b)(4); and (2) responsibilities of a controller under IC 24-15-4-1(1) through IC 24-15-4-1(5); do not apply to pseudonymous data in any case in which the controller is able to demonstrate that any informationnecessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information. (Chapter 6 Section 5)	- no requirement to re-ID deidentified or pseudonymous data or maintain data in an identifiable form (§10 (1)(c)) - consumer right to opt-out of processing for purposes of targeted advertising, the sale of consumer data, and profiling in furtherance of automated decisioins that produce legal or similarly significant effects concerning the consumer apply to pseudonymous information as well (§10(4)). - A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments. (§10(5)).	- no requirement to re-ID de-identified or pseudonymous data or maintain in an identifiable form - consumer rights in 47-18-3203-04 do not apply to pseudonymous data in cases where the controller can show that the information needed to re-ID the information is kept sepaprately and subject to appropriate safeguards. (§47-18-3207(c))
	Sensitive Data Defintion	Sensitive Personal Information means "(1) Personal information that reveals: (A) A consumer's social security, driver's license, state identification card, or passport number. (B) A consumer's 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. (C) A consumer's precise geolocation. (D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership. (E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication. (F) A consumer's genetic data. (2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer. (B) Personal information collected and analyzed concerning a consumer's health. (C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation. (3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information. (§ 1798.140(ae))		"Sensitive Data means: (a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status. (b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or (c) personal data of a known child." (§ 6-1-1303(24)) See Finalized Regs. Rule 6.10 for more information on duty regarding sensitive data	"(a) 'Sensitive data' means: (i) personal data that reveals: (A) an individual's racial or ethnic origin; (B) an individual's religious beliefs; (C) an individual's sexual orientation; (D) an individual's citizenship or immigration status; or (E) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional; (ii) the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or (iii) specific geolocation data. (b) "Sensitive data" does not include personal data that reveals an individual's: (i) racial or ethnic origin, if the personal data are processed by a video communication service; or (ii) if the personal data are processed by a person licensed to provide health care under Title 26, Chapter 21, Health Care Facility Licensing and Inspection Act, or Title 58, Occupations and Professions, information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional." (13-61-101(32))	(27) "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data. (§ 1(27)).	"Sensitive data" means a category of personal data that includes the following: a. Racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law. b. Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person. c. The personal data collected from a known child. d. Precise geolocation data. (§715D.1(26)(a-d)	"Sensitive data" means a category of personal data that includes any of the following: (1) Personal data revealing racial or ethnic origin, religious beliefs, a mental orphysicalhealthdiagnosis made by a health care provider, sexual orientation, or citizenship or immigration status. (2)Genetic or biometric data thatis processedfor the purpose of uniquely identifying a specific individual. (3) Personal data collected from a known child. (4) Precise geolocation data. (Chapter 1 Section 28)	"Sensitive data" means personal data that includes: (a) data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (c) personal data collected from a known child; or (d) precise geolocation data. (§2 (24)).	"Sensitive data" means a category of personal information that includes: (A) Personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (B) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (C) The personal information collected from a known child; or (D) Precise geolocation data; (§47-18-2301(25))
	Definition or references to Inferences	"**Infer**" or "**inference**" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data. (§ 1798.140(m)) Sensitive personal information that is collected with the purpose of inferring chracteristics about a consumer is subject to a consumer's right to limit use and disclosure. (§ 1798.121).	2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;	Statute does not explicitly define "infer" or "reveal" but definition of senitive data includes "personal data *revealing*" a protected category. § 6-1-1303(24)(a). The implementing regulations also define "sensitive inference" -- "Sensitive Data Inference" or "Sensitive Data Inferences" means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status. ""Revealing" as referred to in C.R.S. § 6-1-1303(24)(a) includes Sensitive Data Inferences … While precise geolocation information at a high level may not be considered Sensitive Data … precise geolocation data which is used to indicate an individual visited a reproductive health clinic and is used to indicate an individual's health condition or sex life is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a)." Regs. (1/27 version) Rule 2.02	Statute does not explicitly define "infer" or "reveal" but defintion of sensitive data includes the words "personal information that reveals" a protected category. (§ 13-61-101 (32)(a)(i), Targeted Advertising is displaying an advertisement to a consumer that is selected based on personal data obtained or inferred over time from the consumer's activities. § 13-61-101(34)(a).	Statute does not explicitly define "infer" or "reveal" but defintion of sensitive data includes "data revealing" a protected category. § 1 (27). Targeted advertising is displaying an advertisement to a consumer that is selected based on personal data obtained or inferred over time from that consumer's activities. § 1(28).	Statute does not explicitly define "infer" or "reveal" and the definitioon of sensitive data does not contain this lanague either, as opposed to other states.	Statute does not explicitly define "infer" or "reveal" but definition of sensitive data includes "personal data revealing" a protected category.	Statute does not explicitly define "infer" or "reveal" but definition of senitive data includes "personal data revealing" a protected category.	Statute does not explicitly define "infer" or "reveal" but definition of senitive data includes "personal data revealing" a protected category.

NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 4/20/23

		California	Virginia	Colorado	Utah	Connecticut	Iowa	Indiana	Montana*	Tennessee*
	Service Provider Contract Requirements?	A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that: (1) Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes. (2) Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title. (3) Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title. (4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title. (5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. (1798.100(d)). Contract required by CCPA must: - prohibit service provider or contractor from selling or sharin personal information it collects pursuant to written contract - identify specific business purposes for which service provider or contractor is processing personal information pursuant to the contract - prohibit service provider or contractor from retaining, using, or disclosing the personal information it collected for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations -prohibit service provider or contractor from retaining, using, or disclosing the personal information it collected with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. - Require service provider or contractor to comply with all relevant sections of the CCPA - Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. - Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations. - Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. - Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request. (Regs. S.7051(a))	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall: 1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; 2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; 3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter; 4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and 5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data. (59.1-579(B))	Processing by a processor must be governed by a contract that sets out: - processing instructions, including nature and purpose - type of data processed and the duration - requirements imposed by subsections 3-5 - the following requirements: (I) processor shall delete or return all personal data to to the controller at the request of the controller and (II) processort shall make available all necessary information to demonstrate compliance, and shall allow for all reasonable audits and inspections (6-1-305(5))	Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that: (a) clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations; (b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and (c) requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data. (13-61-301(2))	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of this act; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of this act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request. (S 7(b))	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and duties of both parties. The contract shall also include requirements that the processor shall do all of the following: a. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data. b. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law. c. Upon the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this chapter. d. Engage any subcontractor or agent pursuant to a written contract in accordance with this section that requires the subcontractor to meet the duties of the processor with respect to the personal data. (715D.5(2))	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor do the following: (1) Ensure that each individual processing personal data is subject to a duty of confidentiality with respect to the data. (2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision ofservices,unless retentionofthepersonaldata is requiredby law. (3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance withthe obligations in this chapter. (4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the processor's obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of any such assessment to the controller upon request. (5) Subject to subsection (b), engage any subcontractor pursuantto awrittencontractthat requiresthe subcontractor to meet the obligations of the processor with respect to the personal data (Chapter 5, Sec. 2)	A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also require that the processor: (a) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the personal data; (b) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (c) on the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in [sections 1 through 12]; (d) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (e) allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under [sections 1 through 12] using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request. (§ 8 (2))	A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this part. . . A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract is binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor shall: (1) Ensure that each person processing personal information is subject to a duty of confidentiality with respect to the data; (2) At the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law; (3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this part; (4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of each assessment to the controller upon request; and (5) Engage a subcontractor pursuant to a written contract in accordance with subdivision (b)(3) that requires the subcontractor to meet the obligations of the processor with respect to the personal information. (47-18-3205(b))

NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 4/20/23

		California	Virginia	Colorado	Utah	Connecticut	Iowa	Indiana	Montana*	Tennessee*
Proccessor/Service Provider Obligations	**Service Provider / Processor Obligations with Consumer Rights Flowing from Businesses / Controllers**	-Limit use and disclosure of sensitive PI (§ 1798.121(c)) -Right to know and access data -Right to delete data (§ 1798.105(c)(3)) -Right to correct (proposed Cal. Code Reg. tit. 11 § 7023(c)) -Right to data portability (§ 1798.130 (a)(3)(B)(iii))	3. The disclosure or transfer of personal data to an affiliate of the controller;	- Right to opt out of sale or sharing of data (§ 6-1-1306 (1) (a)). - Right to know and access data. (§ 6-1-1306 (1) (b)). - Right to delete data. (§ 6-1-1306 (1) (d)). - Right to correct data. (§ 6-1-1306 (1) (c)). - Right to appeal process (6-1-1306 (3)). - Right to withdraw consent (6-1-1306 (1) (a) (IV) (C). - Right to data portability. (§ 6-1-1306 (1) (e)).	-Sale or sharing of PI (§ 13-61-302 (1)(b)) - Right to know and access data (§ 13-61-201(1)(a)-(b)) -Right to delete data (§ 13-61-201 (2)) -No right to correct -No right to appeal process -No right to withdraw consent -Right to data portability (§ 13-61-201(3)(a)-(c)) -Mitigate risk to consumer data (§ 13-61-302(2)(a)(i)-(ii)) -Limit use and disclosure of sensitive PI (§ 13-61-302(3)(a)-(b))	-Sale or sharing of PI (§ 6(e)(2)) -Right to know and access data (§ 4 (a)(1)) -Right to delete data (§ 4(a)(3)) -Right to correct (§ 4(a)(2)) -Right to appeal process (§ 4(c)-(d)) -Right to withdraw consent ((§ 6(a)(6)) -Right to data portability (§ 4(a)(4)) -Limit use and disclosure of sensitive PI (§ 6(a)(4)) (§ 7 implies that all of the obligations of a controller pass through to a processor).	- Assist controller in duties required under Iowa bill (§715D.5(1)) - Right to delete or return data (§715D.5(2)(b) - Right to make avaialble to the controller all information to ensure compliance (§715D.5(2)(c))	A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include the following: 1. Assisting the controller in meeting the controller's obligation to respond to consumer requests under IC 24-15-3 byappropriate technical andorganizationalmeasures, insofar as this is reasonably practicable, and taking into account the nature of processing and the information available to the processor. 2. Taking into account the nature of processing and the informationavailable totheprocessor, assisting the controller in meeting the controller's obligations in relation to: (A) the security of processing the personal data; and (B) the notification of a breach of security of the system of the processor under IC 24-4.9; in order to meet the controller's obligations 3. Providing necessary information to enable the controller to conduct and document data protection impact assessments under IC 24-15-6 (Chapter 5 Section 1)	Processor must adhere to instructions of controller and assist in helping controlling fulfill obligations, including: - assistance with fulfilling consumer rights requests - assistance with meeting security obligations - providing necessary information for DPAs (8(1))	Processors must adhere to hte instructions of a controller and assist controller in meeting obligations, including: - assisting in fulfilling consumer rights requests - providing necessary information to enable the controller to conduct DPAs - contracting (see above) (47-18-3205)
Consumer Rights	**Opt in for Sale**	Age 13-16: opt in. (§ 1798.120(d))		Opt in for secondary use (§ 6-1-1308(4)) and for sensitive data (§ 6-1-1308(7)).	Opt-in for for "known children" (Age < 13) in accordance with COPPA requirements. (§ 13-61-302 (3)(b)).	Opt in for sensitive data (§ 6)	No opt-in for sale, but requires entities to follow COPPA.	Required before the sale of children's data (Chapter 4 Section 1 (5))	opt-in required before the sale of the data of a known child (under 13) (§ 7(2)(b))	opt-in required for sale of data of a known child (under 13) (47-18-3201(25); (47-18-3204 (6))
	Opt out of sale for known user	Yes; opt out. (§ 1798.120(a)) See Regs. S.7013 for more information on the right to opt-out of sale and sharing	4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or	Yes; opt out. (§ 6-1-1306(1)(a)(I)(B)) See Finalized Regs. as of 5/23 Rule 4.03 for more information on how to comply with opt-out right	Yes; opt-out (§ 13-61-201(4).	Yes; opt out (§ 4(a)(5)).	Yes; opt-out (§ 715D.3(d))	Yes; opt-out (Chapter 3 Section 1 (b)(5)	Yes; opt-out (§ 5(1)(e)).	Yes; opt out (47-18-3203(a)(2)(F))
	Opt out of sale for pseudonymous or inferences data	Pseudon. Included in right to opt out of sale. (§ 1798.120)	Pseudon. Included in right to opt out of sale. (§ 59.1-581(D))	Pseudon. Included in right to opt out of Sale. (§ 6-1-1307(3))	Pseudon. included in right to opt out of sale (§13-61-303(2)).	Pseudon. included in right to opt out of sale (§ 9(d)).	Pseudon. not included in the right to opt out of sale (715D.6 (3))	Pseudon. Included in the Right to opt of sale	Pseudon. Included in the right to opt out of sale (§10(4))	No; consumer rights do not apply to pseudonymous data (47-18-3207(c))
	Seperate Opt out for Targeted Advertising	Included in sale. (§ 1798.120)	5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.	Separate from sale. (§ 6-1-1306(1)(a)(I)(A))	Yes; opt-out for targeted advertising separate from the opt-out for sale (§ 13-61-201 (4))	Separate from sale. (§ 4(a)(5)(A)).	Yes - § 715D.4(6)	Yes - Chapter 3 Section (1)(b)(A)	Yes (§5(1)(e)(i))	No -- included in sale (47-18-3203(a)(2))
	Seperate Opt out of Profiling	No (§ 1798.140(ah)(1))	Yes, right to opt out from profiling Separate from sale. (§ 59.1.573(A)(5))	Yes, right to opt out of profiling Separate from sale. (§ 6-1-1306(1)(a)(I)(C))	No. No right to opt-out of profiling at all/profiling not contemplated by statute (§ 13-61-201(4)).	Yes, right to opt out of profiling Separate from sale.(§ 4(a)(5)(C)).	No. No Right to opt-out of profiling at all/profiling not contemplated by the statute.	Yes, right to opt out of profiling Separate from sale. - Chapter 3 Section (1)(b)(C)	Yes, right to opt out of profiling Separate from sale. (§5(1)(e)(iii))	No, included in sale of personal data
	Opt in for use of Sensitive Information	No	Yes (§ 59.1-574(A)(5))	Yes (§ 6-1-1308(7))	No (§ 13-61-101(32)).	Yes (§ 6(a)(4)).	No	Yes - (Chapter 4 Section 1 (5))	Yes (§7(2)(b))	Yes (47-18320(a)(6))
	Access Right (Specific Pieces of Information)	Yes (§ 1798.110) See Regs. S.7011(2) for more information on complying with consumer rights requests	Yes (§ 59.1-577(A)(1))	Yes (§ 6-1-1306(1)(b)) Note -- Per finlized regs as of 5/23, data rights request methods do not need to be specific to CO (Rule 4.02(C)) See Regs. Rule 4.04 for more information on right of access requirements See Regs. Rule 4.08 for more informaiton on authenticating users for purposes of data rights requests	Yes (§ 13-61-201(1)(b)).	Yes (§ 4(a)(1)).	Yes (§715D.3(a))	Yes (Chapter 3 Section 1(b))	Yes (§5(1)(a))	Yes (47-18-3203(a)(2)(A))
	Access Right (Categories)	Yes; categories of PI; categories of sources of PI; business purpose of collecting, selling, or sharing PI; categories of third parties PI has been disclosed to; specific pieces of PI collected. (§ 1798.110) See Regs. S.7011(2) for more information on complying with consumer rights requests	No, categories required in privacy policy (§ 59.1-578(C))	No, categoires required in privacy policy (§ 6-1-1306(1)(a)(IV)(C)) Note -- Per finlized regs as of 5/23, data rights request methods do not need to be specific to CO (Rule 4.02(C)) See Regs. Rule 4.08 for more informaiton on authenticating users for purposes of data rights requests	No, categories required in privacy policy (§ 13-61-302 (1)).	No, categories required in privacy policy (§ 6(c)).	No, categories required in privacy policy (§715D.4(5)(d))	No, categories required in privacy policy (Chapter 4, Sec. 3 (1))	No, categories required in privacy policy (§7(5)(a))	Yes (47-18-3203(a)(2)(E))
	Deletion Right	Yes (§ 1798.105(b)) See Regs. S.7011(2) for more information on complying with consumer rights requests See Regs. S.7022 for more on Requests to Delete	Yes (§ 59.1-573 (3))	Yes (§ 6-1-1306(1)(d)) Note -- Per finlized regs as of 5/23, data rights request methods do not need to be specific to CO (Rule 4.02(C)) See Regs. Rule 4.06 for more information on complying with deletion requests See Regs. Rule 4.08 for more informaiton on authenticating users for purposes of data rights requests	Yes; the consumer has the right to delete the personal information that they provided to the controller only. (§13-61-201(2)).	Yes (§ 4(a)(3)).	Yes; the consumer has the right to delete the personal information that they provided to the controller only. - §715D.3 (b)	Yes - (Chapter 3 Section 1(b)(3))	Yes (§5(1)(c))	Yes (47-18-3203(a)(2)(C))

NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 4/20/23

		California	Virginia	Colorado	Utah	Connecticut	Iowa	Indiana	Montana*	Tennessee*
	Nondiscrimination / Nonretaliation Right	Yes; additional requirements from CCPA. Business cannot "retaliate[ ] against an employee, applicant for employment, or independent contractor... for exercising their rights under this title." Additionally, "[t]his subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title." (§ 1798.125)	Yes: Controller "shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer." (§ 59.1-574(A)(4)).	No right but controllers have a duty to avoid unlawful discrimination. (§ 6-1-1308 (6)).	Yes; controller may not discriminate against a consumer for excercising a right by denying a good or service to the consumer; charging the consumer a different price or rate for a good or service; or providing the consumer a different price or rated for a good or service. Does not prohibit controller from offerring different price, rate, quality, or selection of good or service for a consumer who has opted-out of targeted advertising, or in connection with loyalty program. (§13-61-302(4)).	Yes. "A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer." (§ 6(a)(7)).	Yes - A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. (§ 715D.4(3))	Yes - A controller shall not discriminate against a consumer for exercising any ofthe consumer rightssetforth in this article, including by denying goods or services to the consumer, charging different prices or rates for goods and services, or providing a different level or quality of goods or servicesto the consumer. (Chapter 4 § 1 (4)(A-B))	Yes -- controller may not discriminate against a consumer for exercising the rights set forth (§7(2)(e))	Yes -- controller may not discrimate against user for exercising rights (47-18-3204 (a)(5))
Health-related	**Treatment of health related data**	Under the definition of sensitive data, data that reveals mental or physical health information requires companies to provide consumers with notice of their ability to opt-out of its processing (§ 1798.140(D))	Under the definition of sensitive data, data that reveals mental or physical health diagnosis requires companies obtain opt-in user consent before processing (§ 59.1-576(A))	Under the definition of sensitive data, data that reveals mental or physical health conditions requires companies obtain opt-in user consent before processing (§ 6-1-1304)	Under the definition of sensitive data, information regarding an individual's medical history, mental or physical health condition or medical treatment or diagnosis by a health care professional requires companies to provide consumers with notice of their ability to opt-out of its processing (13-61-101(32)).	Under the definition of sensitive data, data that reveals mental or physical health conditions or diagnoses requires companies to obtain opt-in user consent before processing. (§ 6 (a)(4)).	Under the definition of sensitive data, data that is a mental or physical health diagnosis requires companies to provide consumers wih clear notice and an opportunity to opt out of such processing. (§715D.4(2))	Under the definition of sensitive data, data that is revealing a "mental or physical health diagnosis made by a health care provider" requires opt in consent before processing. (Chapter 2, § 28)	Under the definition of sensitive data, data revealing "a mental or physical health condition or diagnosis" requires opt in consent. (§2(24))	Under the definition of sensitive data, data revealing "a mental or physical health condition or diagnosis" requires opt in consent. (§47-18-3201 (25))