	NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 3/30/23						
	CPRA	Virginia	Colorado	Utah	Connecticut	Iowa	
Private Right Action	Yes (§ 1798.150(c))	No (§ 59.1-579 (C))	No (§6-1-1310)	No	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))	
User Enabled Browser Control	Yes (GPC treated as "Do Not Sell" request) (Cal. Code Regs. tit. 11 § 999.315(a))	No	No	No	Yes (§ 5)	No	
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. (§ 57.1-571)	-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))	
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))	- No requirements to re-identify pseudonymous data or keep data in identifiable form. (§ 59.1-577 (B)), - Consumer rights do not apply to pseudonymous data where controller can prove info used to identify the consumer is kept separately and is subject to effective organizational controls to prevent the controller from accessing the info. (§ 59.1-577 (D)). - Controllers disclosing de-identified or pseudonymous data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous or de-dentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments. (§ 59.1-577 (E)).	- 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 pseudonymous data (§ 13-61-303 (1)(a)) -No requirement to maintain pseudonymous 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 pseudonymous data (§ 9(b)(1)) - No requirement to maintain pseudonymous 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))	

	NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 3/30/23						
	CPRA	Virginia	Colorado	Utah	Connecticut	Iowa	
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 category of personal data that includes: 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; 3. The personal data collected from a known child; or 4. Precise geolocation data." (§ 59.1-571)	"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))	"(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)	
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).	Statute does not explicitly define "infer" or "reveal" but defintion of "sensitive data" includes the "personal data that *reveals*" a protected category. "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or *predict personal aspects* related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. (§ 59.1-171).	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.	

	NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 3/30/23						
	CPRA	Virginia	Colorado	Utah	Connecticut	Iowa	
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))	- Sale or sharing of PI (§ 59.1-573(A)(5)) - Right to know and access data (§ 59.1-573(A)(1)) - Right to delete data (§ 59.1-573(A)(3)) - Right to correct (§ 59.1-573(A)(2)) - Right to appeal process. (§ 59.1-573 (C) - Right to data portability (§ 59.1-573(A)(4))	- 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))	
Opt in for Sale	Age 13-16: opt in. (§ 1798.120(d))	Opt in for sensitive PI or children's data (§ 59.1-574(A)(5))	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.	
Opt out of sale for known user	Yes; opt out. (§ 1798.120(a))	Yes; opt out. (§ 59.1-573(A)(5)).	Yes; opt out. (§ 6-1-1306(1)(a)(I)(B))	Yes; opt-out (§ 13-61-201(4).	Yes; opt out (§ 4(a)(5)).	Yes; opt-out (§ 715D.3(d))	
Opt out of sale for pseudonymous or inferences data	Included in sale. (§ 1798.120)	No. (§ 59.1-577(D))	No. (§ 6-1-1307(3))	Yes. Limits on consumer rights for pseudonymous data **do not** apply to right to opt out. (§13-61-303(2)).	Yes. Limits on consumer rights for pseudonymous data **do not** apply to right to opt out. (§ 9(d)).	No	
Seperate Opt out for Targeted Advertising	Included in sale. (§ 1798.120)	Separate from sale. (§ 59.1-573(A)(5)).	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)	
Seperate Opt out of Profiling	Included in sharing. (§ 1798.140(ah)(1))	Separate from sale. (§ 59.1.573(A)(5))	Separate from sale. (§ 6-1-1306(1)(a)(I)(C))	No. No right to opt-out of profiling at all (§ 13-61-201(4)).	Separate from sale. (§ 4(a)(5)(C)).		
Opt out for use of Sensitive Information	Yes (§ 1798.135)	No	No	Yes (§ 13-61-101(32)).	No	Yes - § 715D.4(2)	
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	
Access Right (Specific Pieces of Information)	Yes (§ 1798.110)	Yes (§ 59.1-573(A)(1))	Yes (§ 6-1-1306(1)(b))	Yes (§ 13-61-201(1)(b)).	Yes (§ 4(a)(1)).	Yes (§715D.3(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)	No, categories required in privacy policy (§ 59.1-574(C))	No, categoires required in privacy policy (§ 6-1-1306(1)(a)(IV)(C))	No, categories required in privacy policy (§ 13-61-302 (1)).	No, categories required in privacy policy (§ 6(c)).	Yes (§715D.3(a))	
Deletion Right	Yes (§ 1798.105(b))	Yes (§ 59.1-573 (3))	Yes (§ 6-1-1306(1)(d))	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 - §715D.3(b)	

	NAI State Law Comparison Chart for the Digital Advertising Industry-- Last updated 3/30/23						
	CPRA	Virginia	Colorado	Utah	Connecticut	Iowa	
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))	
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 yo iot out of such processing. (§715D.4(2))	