Sources and Legend. The following chart compares Vermont S.71 (Draft 3.3, May 8, 2026) against the Connecticut Data Privacy Act ("CTDPA"), as enacted by Public Act 22-15 (SB 6, 2022) and subsequently amended by Public Act 23-56 (SB 3, 2023) and Public Act 25-113 (SB 1295, 2025). The "Issue" column summarizes the baseline principles reflected in national consensus comprehensive privacy law framework. ❌ identifies provisions that diverge from that baseline, while ✅ identifies provisions that align with it. Italicized and bolded phrases highlight notable outlier provisions.

#	ISSUE	VT S.71 (Draft 3.3)	The Connecticut Data Privacy Act (CTDPA)
DEFINITIONS			
1	"Biometric data" is defined as data generated from automatic measurements of biological characteristics used to identify a specific individual.	❌ — defined as data generated from the ***"technological processing"*** of a consumer's unique biological, physical, or physiological characteristics that ***"allow or confirm"*** unique identification, such as iris/retina scans, fingerprints, ***facial/hand mapping or geometry or templates, vein patterns, voice prints or vocal biomarkers, and gait.*** • Will create an overbroad definition that will affect services like makeup or glasses virtual try-ons and confuse consumers about what is truly biometric data and what is not.	✅ — defined as data generated from "automatic measurements" of an individual's biological characteristics used to identify a specific individual, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics.

2	“Collect” is addressed through the definition of “process” or “processing,” rather than as a standalone defined term.	❌ — Defines “collect” ***as a standalone term*** which includes buying, renting, gathering, obtaining, receiving, or accessing personal data by any means, and expressly including ***active or passive receipt and observation*** of the consumer’s behavior. • Businesses will face uncertainty about whether routine analytics, session recordings, or A/B testing constitute “collection” triggering separate notice obligations. • Consumers will be overwhelmed with disclosures about ordinary website interactions they do not perceive as data collection.	✅ — “Collect” is subsumed within “process”/ “processing,” which includes the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.
3	“Consent” is defined as a clear affirmative act signifying freely given, specific, informed, and unambiguous agreement.	❌ — Defined as an agreement for a ***“narrowly defined particular purpose,”*** and prescribes specific methodologies for obtaining consent, including requirements that consent mechanisms ***be easy to understand and execute, provide symmetry in choice, avoid confusing language or interactive elements, and not use choice architecture that***	✅ — Defined as a clear affirmative act signifying freely given, specific, informed, and unambiguous agreement and excludes acceptance of general terms of use, hovering/muting/pausing/closing content, and dark patterns.

		impairs consumer decision-making. ● Not defined this way in any state comprehensive law. ● Will result in confusing and longer disclosures to consumers when consent is required.	
4	"Identified or identifiable individual" is defined as an individual who can be readily identified, directly or indirectly.	❌ — Expands the definition by enumerating specific identifiers, ***including precise geolocation data, online identifiers, and device identifiers.*** ● Sweeps in advertising IDs, IP addresses, and cookie identifiers that other states regulate only when linked to an individual. ● Expands the scope of data subject to the statute and imposes compliance obligations on routine digital operations that consumers would not expect to implicate their privacy.	✅ — Defined as an individual who can be readily identified, directly or indirectly.

5	“De-identified data” is defined as data that cannot reasonably be linked to an identified or identifiable individual and is subject to safeguards designed to prevent re-identification and restrict downstream use.	❌ — Expands definition to include data not reasonably linkable to ***a household*** and ties “reasonable measures” ***to the deidentification requirements set forth under HIPPA (45 C.F.R § 164.514).*** • The definition is an outlier among other state comprehensive laws. • Tying the standard to HIPAA’s de-identification methodology imposes health-care-grade compliance costs on non-healthcare businesses and may discourage the use of de-identified data for beneficial purposes like product improvement and safety research.	✅ — Defined as data as not reasonably linkable to an identified or identifiable individual, or a device linked to such individual, if the controller (A) takes reasonable measures, (B) publicly commits to process only in de-identified form and not attempt re-identification, and (C) contractually obligates recipients.
6	“Derived data” is addressed through the definition of personal data when linked or reasonably linkable to an identified or identifiable individual.	❌ — Defines “derived data” as ***a standalone term*** and expressly incorporates it into the scope of personal data. • Businesses could face the impossible task of tracing and deleting algorithmic outputs throughout their systems, while consumers will see bloated privacy disclosures listing	✅ — Does not separately define “derived data”; treatment depends on whether the information is linked or reasonably linkable to an identified or identifiable individual.

		“derived” data categories they do not understand.	
8	“Precise geolocation data” includes information derived from technology that directly identifies the specific location of an individual within a defined geographic radius, with limited exclusions for communications content and utility infrastructure data.	❌ — Defined to information ***revealing the past or present physical location*** of a consumer or linked device ***within a 1,850-foot radius.*** Includes an additional exclusion for ***photograph, video, and associated metadata that cannot be linked to an individual.*** • Businesses operating consumer apps may need to treat vacation photos and restaurant check-ins as precise geolocation data subject to opt-in consent, creating unnecessary friction for consumers who expect to share location-tagged content freely and diluting the purpose of classifying precise location data as sensitive. • ***Not in any other comprehensive privacy law definition.***	✅ — Defined as information derived from technology that directly identifies the specific location of an individual within a radius of 1,750 feet. Excludes the content of communications and data generated by or connected to advanced utility metering infrastructure systems or equipment used by a utility.

9	“Processing” is defined as operations performed on personal data, whether by manual or automated means, including the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.	❌ — Expands the enumerated list of operations to include ***“otherwise handling”*** personal data. • This catch-all language eliminates any limiting principle and departs from the standard definition found in all other state frameworks. •	✅ — Includes collection, use, storage, disclosure, analysis, deletion, and modification of personal data performed by manual or automated means.
10	“Processor” is defined as a person that processes personal data on behalf of a controller.	❌ — Expands the definition to include persons that ***“collect”*** personal data and persons acting on behalf of ***“another processor.”*** • Businesses will likely need renegotiate existing processor agreements to account for sub-processor liability just for VT, increasing contracting costs and timelines. • Consumers experience no benefit from this expanded definition but will bear the costs through delayed product deployments and reduced service options as businesses consolidate vendor	✅ — Defined as a person that processes personal data on behalf of a controller.

		relationships to minimize liability.	
11	“Sale of personal data” excludes disclosures directed by the consumer and intentional consumer interactions with third parties.	❌ — Limits the exclusion to disclosures made ***“with the consumer’s consent”*** where the consumer directs the controller to disclose personal data or intentionally uses the controller to interact with a third party. • No other state adopts this formulation. The purpose of the exception is to avoid requiring additional consent where a consumer affirmatively directs the controller to interact with a third party. The added language undermines that purpose and significantly narrows the exception. • Businesses will be forced to build redundant consent flows for disclosures consumers have already directed (e.g., when a consumer uses a platform to connect with a third-party service provider) adding unnecessary friction and	✅ — Excludes disclosures where the consumer directs the controller to disclose personal data or intentionally uses the controller to interact with a third party.

		confusing consumers who already made the affirmative choice to share their data.	
12	"Personal data" is defined as information linked or reasonably linkable to an identified or identifiable individual, excluding de-identified data and publicly available information.	❌ — Expands the definition to expressly include ***derived data, unique identifiers,*** and information linked or reasonably linkable to a device associated with ***one or more individuals in a household.*** ● Including household data opens up significant unintended consequences when talking about data rights such as access, deletion, etc. ● Should a consumer be able to access personal data on their roommate? ● Should a domestic violence abuser be able to access the victim's precise geolocation information?	✅ — Defined as information linked or reasonably linkable to an identified or identifiable individual and excludes de-identified data and publicly available information.

13	“Publicly available information” is defined as information lawfully made available through government records or to the public, with limited exclusions.	❌ — Adopts a broader set of exclusions, including ***collated consumer profiles made publicly available, information offered for sale, inferences derived from such information, personal data created through combinations with publicly available information, restricted-audience content, nonconsensual intimate images, and genetic data unless publicly disclosed by the consumer.*** • Many of these novel provisions create First Amendment questions.	✅ — Defined as information lawfully made available from government records or lawfully made available to the general public, and excludes biometric data associated with a specific consumer that was collected without the consumer’s consent.

14	“Sensitive data” includes standard categories (e.g., racial/ethnic origin, religious beliefs, health, sex life/sexual orientation, citizenship/immigration status, genetic/biometric data, children's data, crime victim status, geolocation).	❌ — Expands the enumerated categories to include ***philosophical beliefs, pregnancy status, income level and indebtedness, tax returns, consumer health-data analytics used for non-identification purposes, driving behavior***, and personal data collected from a consumer the controller ***“knew or should have known”*** is a minor. • These novel elements create significant redundancies (e.g., “pregnancy status” is already included in definition of “consumer health data”). • The “knew or should have known” standard for minors effectively requires age-gating or age-estimation mechanisms across all digital services, imposing significant implementation costs on businesses and creating friction-heavy experiences for all consumers, including adults, who will need to verify their age to	✅ — Includes standard categories of sensitive personal information, including racial or ethnic origin, religious beliefs, health data, sex life or sexual orientation, citizenship, or immigration status, genetic or biometric data, children’s data, crime-victim status, and precise geolocation data.

		access ordinary services.	
15	“Targeted advertising” excludes advertisements based on activities within the controller’s own websites or online applications.	❌ — Expands the exclusion to advertisements based on activities within the controller’s own ***“commonly branded”*** websites or online applications. ● This language does not exist anywhere in any other state privacy law. ● The qualifier introduces ambiguity about which affiliated properties qualify. As a result, businesses must conduct legal analysis of every co-branded partnership and family of sites. ● Consumers will experience inconsistent ad experiences where first-party advertising works on some affiliated sites but not others within the same brand family.	✅ — Excludes advertisements based on activities within the controller’s own websites or online applications.
APPLICABILITY			

16	Conflicts among privacy laws are resolved through ordinary rules of statutory construction.	❌ — Adopts a ***"greatest protection to privacy"*** standard requiring the law providing the greatest privacy protection to control in the event of a conflict. • This will create significant confusion in terms of which statute is actually governing personal data, as we have seen in CA with its inclusion of this language. What is "the greatest privacy protection" is completely subjective. • This phrase threatens to undermine the entire statute.	✅ — Relies on ordinary rules of statutory construction.
EXEMPTIONS			
17	HIPAA exemption applies to covered entities and business associates.	❌ — Exempts only a ***"covered entity that is not a hybrid entity,"*** the ***"health care component of a hybrid entity,"*** or a business associate.	✅ — Exempts a covered entity or business associate, as defined in 45 CFR 160.103.
18	Public-health-activities data exemption applies to information used for public health purposes as authorized by HIPAA.	❌ — Limits the exemption to information used for public health, community health, or population health activities ***"when provided by or to a covered entity or when provided by or to a business associate in accordance with the***	✅ — Exempts information used for public health activities and purposes "as authorized by HIPAA," community health activities, and population health activities.

		business associate agreement with a covered entity."	
19	Limited data sets are exempt when used, disclosed, and maintained in the manner specified by HIPAA.	❌ — No separate exemption for limited data sets.	✅ — Expressly exempts information included in a limited data set, as described in 45 CFR 164.514(e), to the extent such information is used, disclosed, and maintained in the manner specified therein.
20	Information originating from and intermingled with exempt health-care-related information maintained by a covered entity or business associate is exempt.	❌ — No intermingled-data exemption.	✅ — Exempts information originating from and intermingled to be indistinguishable with, or treated in the same manner as, exempt health-care information maintained by a covered entity, business associate, or qualified service organization.
21	Third-party administrators are not exempt.	❌ — Expressly exempts third-party administrators, as defined in the Third-Party Administrator Rule adopted pursuant to 18 V.S.A. § 9417.	✅ — Does not list third-party administrators as a separately enumerated exempt entity.
22	The de-identification exemption for health-related information applies to information de-identified in accordance with HIPAA requirements.	❌ — Limits the exemption to information de-identified in accordance with 45 C.F.R. § 164.514 that is derived from ***"individually identifiable health information"*** as described in HIPAA.	✅ — Applies the exemption to information de-identified in accordance with HIPAA requirements that is derived from enumerated categories of health care-related information, including HIPAA-regulated information, health records, Part 2 information, research data, public-health information, and clinical-trial data.

23	Government contractors processing consumer health data on behalf of a government entity are exempt.	❌ — No exemption for government contractors processing consumer health data; only the government entity itself is exempt in the ordinary course of its operation.	✅ — Exempts any person who has entered a contract with a body, authority, board, bureau, commission, district, or agency of the state "while such person is processing consumer health data on behalf of such body . . . pursuant to such contract."
24	Protected health information under HIPAA is exempt.	❌ — Exempts "health care records" (as defined in 18 V.S.A. § 9419) only ***"if the information is held by an entity that is a covered entity or business associate under HIPAA."***	✅ — Exempts "protected health information under HIPAA" as a standalone data-level exemption.
25	Human-subjects research exemptions encompass information collected pursuant to federal research and clinical-trial standards.	❌ — Research-data exemptions are provided only through the Federal Policy for the Protection of Human Subjects (45 C.F.R. Part 46) and FDA regulations (21 C.F.R. Parts 50 and 56).	✅ — Separately exempts identifiable private information collected as part of human-subjects research conducted pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use.
26	Nonprofit organizations are exempt.	❌ — Only exempts specific categories of nonprofits (e.g., insurance-fraud-detection nonprofits, postsecondary enrollment-reporting nonprofits, and victim services organizations).	✅ — Provides an entity-level exemption for any "nonprofit organization" (defined as any organization exempt under IRC § 501(c)(3), (c)(4), (c)(6), or (c)(12)).
27	Political committees and candidate committees are exempt.	❌ — Does not separately exempt political committees or candidate committees.	✅ — Exempts candidate committees, national committees, party committees, and political committees.

28	Institutions of higher education are exempt.	❌ — Provides a limited exemption stating that the act shall not require an independent school (as defined in 16 V.S.A. § 11(a)(8)) or a private institution of higher education (as defined in 20 U.S.C. § 1001 et seq.) to delete personal data or opt out of processing of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.	✅ — Provides an entity level exemption for any institution of higher education.
29	Agents, broker-dealers, investment advisers, and investment adviser agents regulated by state banking regulators, or the Securities and Exchange Commission are exempt.	❌ — Does not provide an entity-level exemption for securities professionals regulated by state banking regulators or the SEC.	✅ — Exempts any agent, broker-dealer, investment adviser, or investment adviser agent regulated by the Department of Banking or the Securities and Exchange Commission.
30	Security and fraud-prevention exemption preserve activities necessary to prevent, detect, investigate, or respond to security incidents, fraud, and illegal activity.	❌ — Expands the carveout to expressly include illegal activity “targeted at or involving the controller or processor or its services.” • No other state restricts the fraud prevention provisions in this way, and companies should be free to protect their own data and their	✅ — Preserves controllers’ and processors’ ability to prevent, detect, protect against, or respond to security incidents, fraud, harassment, malicious or deceptive activities, and illegal activity, preserve system integrity and security, and investigate, report, or prosecute such activity.

		consumers in the ways they deem best. • Could prevent businesses from taking necessary steps to protect themselves against known threats prior to actually being targeted.	
CONSUMER PERSONAL DATA RIGHTS			
31	Authorized agents may exercise specified opt-out rights on a consumer's behalf.	❌ — Permits an authorized agent to exercise all consumer rights, including opt-out rights. • No other state extends authorized agent authority beyond sale of personal data, targeted advertising, and profiling opt-outs. • Extending agent authority to access, correction, and deletion requests creates massive consumer identity theft risks. • A bad actor posing as an "authorized agent" could obtain a consumer's full data profile, modify personal records, or delete account information entirely, with no meaningful	✅ — Permits designation of an authorized agent to exercise opt-out rights related to targeted advertising, the sale of personal data, and profiling in furtherance of automated decisions producing legal or similarly significant effects.

		safeguard preventing abuse.	
32	Consumer-rights provisions address dark patterns through the consent standard.	❌ — Separately prohibits conditioning the exercise of consumer rights through false, fictitious, fraudulent, or materially misleading statements or representations, or the employment of dark patterns.	✅ — Addresses dark patterns through the definition of consent and does not separately prohibit conditioning the exercise of rights through misrepresentations or dark patterns in the consumer-rights section.
33	Deletion requests for personal data obtained from third parties may be satisfied through alternative compliance pathways.	❌ — Provides a single deemed-compliance pathway allowing a controller to retain a record of the deletion request and the minimum data necessary to ensure the consumer's data remains deleted and is not used for any other purpose. • Deviates from solution negotiated with consumer advocates in 2023 and since replicated with no controversy in other state comprehensive laws. • Limiting controllers to a single compliance pathway eliminates the flexibility to opt consumers out of processing as an alternative. • As a result, this removes a compliance option	✅ — Permits either: (1) retaining a record of the deletion request and the minimum data necessary to ensure the consumer's data remains deleted and is not used for any other purpose; or (2) opting the consumer out of the processing of such personal data for any purpose other than those exempted by statute.

		that other states recognize as equally protective of consumer interests and reduces consumer choice.	
DUTIES OF CONTROLLERS			
34	Data minimization provisions require controllers to limit the collection of personal data to what is reasonably necessary and proportionate to disclosed purposes, while separately regulating secondary uses that are incompatible with those disclosed purposes.	❌ — Applies the "reasonably necessary and proportionate" standard to both collection and ***processing*** and permits processing for another disclosed purpose that is ***"compatible with the context"*** in which the data was collected. Separately defines "reasonable expectations of the consumer" through detailed statutory factors, including ***the source and method of collection, the specificity and prominence of disclosures, and whether processor and third-party involvement is apparent to the consumer.***	✅ — Separately limits collection to what is reasonably necessary and proportionate to disclosed purposes and prohibits processing for a "material new purpose" that is neither reasonably necessary to nor compatible with those disclosed purposes unless the controller obtains consumer consent. Compatibility is evaluated through enumerated factors, including consumer expectations, the relationship between the original and new purposes, consumer impact, contextual relationship, and additional safeguards.

35	Controllers must obtain consumer consent before processing personal data for purposes that are incompatible with the purposes originally disclosed to the consumer.	❌ — Requires consent before processing personal data for any purpose that does not satisfy the statute's "reasonably necessary and proportionate" or "compatible with the context" standards. Separately prescribes detailed requirements governing how consent must be obtained, including symmetry of choice, avoidance of confusing language or interfaces, restrictions on choice architecture, and ease of execution. • These prescriptive consent mechanics go well beyond the national standard and will require businesses to redesign user interfaces across all digital touchpoints at significant cost. • The subjective nature of "symmetry of choice" and "confusing" interface elements will produce inconsistent compliance interpretations. • Consumers will face longer and more complex consent interactions that impede their ability	✅ — Requires consent only before processing personal data for a material new purpose that is neither reasonably necessary to nor compatible with the purposes originally disclosed to the consumer.

		to quickly access the services they want.	
36	Processing of sensitive data is generally permitted with the consumer's consent (or, for known children, in accordance with COPPA).	❌ — Prohibits the collection or processing of sensitive data unless the processing is ***"strictly necessary"*** to provide or maintain a specific product or service requested by the consumer. • The "strictly necessary" standard is far more restrictive than the consent-based approach used in every other state. • It will prevent businesses from offering consumers personalized services that rely on sensitive data (e.g., health and wellness recommendations, financial planning tools) even where the consumer affirmatively wants those services and would freely consent. • ***Prevents consumers from exercising control over their sensitive data.***	✅ — Permits processing of sensitive data where the processing is reasonably necessary in relation to the disclosed purposes and the controller obtains the consumer's consent, or, for known children, processes the data in accordance with COPPA.

37	Controllers may not process personal data for targeted advertising or sell personal data where the controller has actual knowledge, or wilfully disregards, that the consumer is a minor.	❌ — Prohibits targeted advertising to minors and the sale of minors' personal data but creates an exception for certain "covered businesses" and "covered minors" that comply with separate statutory requirements under Vermont law. • The exception for "covered businesses" and "covered minors" under separate Vermont-specific definitions creates a two-track compliance regime. • Businesses must determine whether they qualify under Vermont-specific classifications and apply different rules depending on the outcome, adding compliance complexity that does not exist in any other state. • This creates confusion for parents about what protections apply to their children.	✅ — Prohibits processing personal data for targeted advertising or selling personal data where the controller has actual knowledge, or wilfully disregards, that the consumer is at least thirteen years of age but younger than eighteen years of age.

38	Sale of sensitive data generally is permitted only with the consumer's consent.	❌ — Prohibits the sale of sensitive data outright. ● An outright ban, rather than permitting sale with consumer consent, eliminates consumer choice entirely. ● Prevents consumers from voluntarily participating in data-sharing programs they may affirmatively want (e.g., health research initiatives, financial wellness platforms that rely on sensitive data sharing in exchange for direct consumer value.) ● Prevents advertising based on race/sexual orientation, reducing access to products and services for those populations.	✅ — Permits the sale of sensitive data only where the controller obtains the consumer's consent.

39	Controllers may process personal data for targeted advertising subject to consumer opt-out rights and heightened protections for sensitive data.	❌ — Expressly authorizes controllers to process or ***"transfer"*** personal data collected pursuant to the statute's data minimization standard for targeted advertising ***unless the data constitutes sensitive data*** or the consumer has opted out of targeted advertising. ● ***No other comprehensive state law contains this kind of outright prohibition.*** ● Introducing "transfer" as an undefined, distinct concept alongside processing expands the scope of restrictions on data movement in ways not defined elsewhere in the statute or in other states. ● Businesses face uncertainty about whether routine data-sharing arrangements such as cloud hosting or analytics integrations constitute "transfers" subject to separate restrictions. ● Consumers may lose access to ad-supported free services as businesses limit data	✅ — Permits targeted advertising subject to a consumer opt-out right; sensitive data may be processed for targeted advertising only with consumer consent.

		flows to avoid compliance risk.	
40	Anti-discrimination provisions generally prohibit discriminatory treatment in connection with the processing of personal data and the exercise of consumer privacy rights.	❌ — Prohibits processing personal data in a manner that discriminates against individuals or denies equal enjoyment of goods or services based on protected characteristics, while also prohibiting processing personal data in violation of state or federal anti-discrimination laws. Includes specified exceptions for private establishments, anti-bias testing, and diversity-related processing.	✅ — Prohibits controllers from processing personal data in violation of state or federal anti-discrimination laws.
41	Controllers must establish, implement, and maintain reasonable administrative, technical, and physical safeguards appropriate to the volume and nature of the personal data.	❌ — Requires controllers to maintain reasonable security practices and separately mandates compliance, for sensitive-data processing, with specified National Institute of Standards and Technology (“NIST”) Privacy and Cybersecurity Frameworks and requires disposal of personal data pursuant to a retention schedule when the data must be deleted by law or is no longer necessary for the disclosed purpose. • Mandating specific NIST frameworks locks businesses into a particular compliance	✅ — Requires controllers to establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.

		methodology that may not align with their existing security infrastructure, forces costly re-engineering of systems, and does not account for industry-specific frameworks that may provide equal or greater protection to consumers. • Will imposed untold costs on small and medium-sized businesses.	
42	Privacy notices must disclose categories of personal data processed, processing purposes, consumer-rights mechanisms, categories of data sold, categories of third parties receiving the data, large-language-model training disclosures, and the date of the most recent update.	❌ — Requires a separate list of categories of sensitive data processed and requires the categories of personal data collected and processed to be described in a level of detail that provides consumers a "meaningful understanding" of the data collected and processed. Also requires disclosure of categories of third parties with which personal data is ***"shared."*** • Disclosing categories of third parties with which data is "shared, "a term not otherwise defined in the statute, creates ambiguity and potential liability for businesses that cannot determine	✅ — Requires disclosure of categories of personal data processed, categories of personal data sold, categories of third parties to which personal data is sold, and clear and conspicuous disclosures regarding targeted advertising activities.

		with certainty which relationships trigger disclosure.	
PROCESSORS' DUTIES; CONTRACTS BETWEEN CONTROLLERS AND PROCESSORS			
43	Controller-processor contracts govern processing procedures performed on behalf of the controller.	❌ — Requires processors to adhere to the controller's instructions and limits processors to processing and transferring personal data only to the extent necessary to provide the contracted service requested by the controller. ● Limiting processors to activities "necessary to provide the contracted service" goes beyond the national standard, which requires that processors follow controller instructions. ● Prevents processors from engaging in quality assurance, product improvement, or security testing that benefits the controller's consumers unless each activity is specifically enumerated in the contract.	✅ — Requires a contract governing the processor's data processing procedures with respect to processing performed on behalf of the controller.

44	Controller-processor contracts specify processing instructions, purposes, duration, and the parties' respective rights and obligations.	❌ — Separately prohibits processors, absent consumer consent, from combining personal data received from a controller with personal data received from or on behalf of another controller or collected directly from the consumer. • Presents a false choice because consumers do not interact with processors. • This data-combination prohibition will impede legitimate aggregation activities like fraud detection, security threat analysis, and benchmarking services that rely on cross-client data patterns. • It will ultimately weaken the security protections and service quality available to consumers while forcing businesses to build siloed and duplicative data infrastructure at significant cost.	✅ — Requires controller-processor contracts to clearly set forth processing instructions, the nature and purpose of processing, the type of data processed, the duration of processing, and the rights and obligations of both parties.
DATA PROTECTION AND IMPACT ASSESSMENTS; DISCLOSURE TO ATTORNEY GENERAL			

45	Data protection assessments generally must be reviewed and updated to account for changes in processing activities and associated risks.	❌ — Requires controllers to update data protection assessments throughout the processing lifecycle as often as appropriate based on the type, amount, and sensitivity of the data and the level of risk presented by the processing. Also requires ongoing monitoring for harm, adjustment of safeguards over time, and retention of all data protection and impact assessments for at least three years. ● The perpetual reassessment obligation, without clear triggers specifying what constitutes a material change, diverts resources from actual privacy protection to continuous documentation maintenance, disproportionately burdening smaller businesses that lack dedicated privacy teams. ● This this increases costs for all businesses without a corresponding improvement in consumer protection.	✅ — Requires updates to data protection assessments only in connection with children's provisions and only as necessary to account for material changes to the relevant processing operations. Requires retention of assessment documentation for the longer of: (1) three years after the processing operations cease; or (2) as long as the controller offers the relevant online service, product, or feature.

46	Independent assessment and validation requirements generally apply in the context of processor oversight and compliance verification.	❌ — Requires independent review and validation of data protection assessments involving sensitive data, including validation of compliance with the statute's minimum cybersecurity baseline. Mandates written validation reports identifying assessed systems, compliance findings, remediation measures, and remediation timelines, and treats knowing failure to complete a required validation or inclusion of false information as fraud subject to statutory penalties. • ***No state comprehensive law provides this requirement.*** • The fraud-based penalty structure will create a chilling effect on candid internal documentation, as businesses will be disincentivized from identifying risks in writing. • This ultimately harms consumers by discouraging the very self-assessment activities that protect their data. • Will saddle businesses with untold compliance	✅ — Permits controllers to conduct reasonable assessments of processors or to rely on assessments conducted by qualified and independent assessors using accepted control standards or frameworks. Requires processors to cooperate with such assessments and provide assessment reports to controllers upon request.

		costs for no discernible consumer benefit.	
ENFORCEMENT			
47	Enforcement authority rests with the Attorney General.	❌ — Provides exclusive Attorney General enforcement for most violations but authorizes consumers to bring civil claims against entities with annual gross revenues exceeding $1 billion in the previous calendar year. • The private right of action, even limited to billion-dollar companies, will generate class-action litigation that increases legal costs passed through to consumers in the form of higher prices. • The revenue threshold creates an arbitrary compliance cliff that disadvantages companies as they scale and incentivizes creative corporate structuring to remain below the threshold.	✅ — Provides exclusive Attorney General enforcement and expressly states that the statute does not create, and may not serve as the basis for, a private right of action under the statute or any other law. Violations constitute unfair trade practices enforceable solely by the Attorney General.

48	Attorney General enforcement authority does not include rulemaking authority.	❌ — Expressly authorizes the Attorney General to adopt rules implementing the statute. • Granting rulemaking authority allows the regulatory landscape to shift without legislative process, creating ongoing uncertainty for businesses that cannot rely on the statute as enacted and forcing continuous monitoring costs that disproportionately burden smaller companies without in-house regulatory counsel.	✅ — Does not provide rulemaking authority under the statute.
49	Enforcement provisions do not create standalone fraud liability tied to data protection assessment compliance obligations.	❌ — Creates a separate fraud-based enforcement provision for knowingly failing to complete required validation obligations or including false information in a data protection assessment, punishable by civil penalties, treble damages, and investigation and prosecution costs. • Converting privacy compliance into potential fraud liability, with treble damages, is wildly disproportionate to the underlying	✅ — Does not establish a standalone fraud offense or separate fraud-based penalty structure tied to data protection assessment obligations.

		obligation and will deter businesses from conducting candid self-assessments at all. ● Consumers are left worse off because the threat of fraud prosecution discourages the very internal risk-identification processes that protect their data.	