Response to National Industry Lobbyist Comparison Document: "Vermont S.71 (Draft 3.3) vs. Connecticut Data Privacy Act"

Prepared by Rep. Monique Priestley and submitted 5/15/2026 in her individual capacity, not on behalf of the entire committee.

INTRODUCTION

On May 12, 2026, to the Vermont House Committee on Commerce & Economic Development, regarding S.71 v3.3, a lobbyist representing the State Privacy and Security Coalition (SPSC) submitted a comparison document (attached at the end) framing the 2022 Connecticut Data Privacy Act (CTDPA) as the "national standard" Vermont should match. It isn't. Connecticut's own legislature proved that in May 2026 by passing SB 4, which moves Connecticut closer to Vermont's approach on data brokers, geolocation, and aggregation loopholes. The comparison also ignores Vermont's own enacted law: the Age-Appropriate Design Code (AADC, Act 63) is already on the books, and many of S.71 v3.3's provisions aren't novel additions, they're integrations with a framework Vermont already passed. The following response sets the record straight on 49 industry objections across definitions, applicability, exemptions, consumer rights, controller duties, and enforcement. Most mischaracterize where national law actually stands. **California, Maryland, Oregon, and Minnesota have all enacted stronger provisions than what industry is calling the "baseline".**

The industry's framing rests on two flawed premises.

First, it uses the original 2022 CTDPA as its benchmark, largely ignoring the sweeping 2025 amendments (Public Act 25-113, SB 1295), signed by the Connecticut governor in June 2025 and taking effect July 1, 2026. Those amendments moved Connecticut toward Vermont's approach on multiple dimensions, including applicability thresholds, sensitive data, minors' protections, AG rulemaking authority, and privacy notice requirements.

Second, the document ignores Vermont's own enacted law: the Vermont Age-Appropriate Design Code Act (Act 63, S.69), signed into law June 12, 2025, effective January 1, 2027. The AADC defines obligations for covered businesses, including definitions of "covered minor," "covered business," and data minimization standards, that are directly integrated into S.71 v3.3's structure. The industry comparison treats S.71 v3.3's minor-protective provisions as novel outliers; **in fact, they reflect Vermont law already on the books**.

The document is a thinly-veiled attempt by Big Tech companies and their hired lobbyists to scuttle S.71 and continue preying on Vermonters by using, invading and stealing their privacy rights without their permission. Industry could have submitted this document at the beginning of

the week-long testimony held by this committee, or more aptly, during the working group sessions that they were directly involved in with committee leadership prior to the S.71 v2.3 draft. Instead, using a tried and true tactic, they waited until the last moment to submit this document, hoping to bypass any efforts to thoughtfully rebut their spurious arguments. **This technique has been used before both in this body and in others. Such efforts seek to subvert reasoned debate and protect the industry's well documented failure to protect young users for the damage their products have done since their invention.**

These companies have one goal: profit. Not privacy. Not safety. Profit. These are companies that have spent years lobbying against accountability, and they are now doing the same as A.I. moves from an abstract concern to a real one affecting our constituents today. **The State Privacy and Security Coalition, who produced the comparison document, has a membership roster made up of a who's who of data-dependent industries such as Big Tech, telecom, insurance, retail, and ad-tech.** According to their About Us page, SPSC's membership includes: Adobe, Amazon, AT&T, Capital One, Charter Communications, Cox, DIRECTV, Dropbox, GM, Google, Hims & Hers, H&R Block, Humana, IAB, McKesson, Meta, NetChoice, RELX Group, T-Mobile, Target, Verizon, Walgreens, and Yahoo, among others. **POLITICO profiled the man behind SPSC's national strategy in a 2024 piece titled 'The man quietly rewriting American privacy law.'**

The document should be read with that context in mind.

A NOTE ON THE ACTUAL "NATIONAL STANDARD"

The industry document frames the pre-amendment CTDPA as the "national consensus baseline." That characterization cannot survive a survey of where state law actually stands in May 2026.

California is the largest privacy jurisdiction in the country and the state whose framework many businesses build compliance programs around. California applies data minimization to collection, use, retention, and sharing. The California Privacy Protection Agency's Enforcement Advisory No. 2024-01, issued April 2, 2024, called data minimization "a foundational principle in the CCPA" and stated explicitly that businesses "should apply the principle of data minimization to every purpose for which they collect, use, retain, and share consumers' personal information." The California Consumer Privacy Act (CCPA) standard requires that collection, use, retention, and sharing all be "reasonably necessary and proportionate" to the purpose for which data was collected or processed. This is not a collection-only standard; it applies across the full processing lifecycle. Vermont S.71 v3.3's application of minimization to both collection and processing is fully consistent with California's framework, which provides the most comprehensive compliance guidance of any state in the country. Businesses building California-compliant programs already operate under these rules.

Maryland's Online Data Privacy Act (MODPA) took effect October 1, 2025 and is now being enforced. It goes further than Connecticut in two of the most contested areas in the

industry document: it uses a "strictly necessary" standard for sensitive data processing regardless of consent, and it prohibits the sale of sensitive data outright. **Oregon** also bans the sale of certain categories of sensitive data, and **Virginia** recently banned the sale of precise geolocation outright as well. Vermont's approach on these same questions is not an outlier; it is consistent with a movement of states toward stricter treatment of sensitive data.

Connecticut SB 4 (2026) passed the Connecticut House 141-6 and the Senate 31-4 in May 2026 and is awaiting the governor's signature. SB 4 goes substantially beyond what the industry document presents as Connecticut's settled standard. It creates a centralized data broker deletion mechanism (i.e. the Delete Act), amends the CTDPA to prohibit the sale of precise geolocation data outright, redefines "publicly available information" to close aggregation loopholes, and adds new restrictions on facial recognition technology. Connecticut's own legislature, in real time, is moving toward the positions Vermont has taken in S.71 v3.3, not away from them.

The industry characterization of Vermont's approach as novel also fails on third-party disclosure. Vermont's privacy notice requirements (disclosing categories of personal data shared and categories of third parties) are consistent with most enacted state laws. Vermont also gives consumers the right upon request to obtain a list of specific named third parties to which their personal data has been sold. Rhode Island goes further by requiring named-party disclosure of data sales directly in the privacy notice itself, without requiring a consumer to ask. Oregon and Minnesota go further still, applying the named-party disclosure right to all third-party disclosures, not just sales. Vermont's approach is neither unprecedented nor the most demanding position in enacted state law. It sits at the more moderate end of a spectrum that multiple states have already established.

The direction of state privacy law is clear: stronger minimization, broader sensitive data protections, and stricter limits on data sales. The industry document presents a snapshot of where Connecticut was in 2022 and asks Vermont to bake outdated rules into law.

DEFINITIONS

Issue 1: "Biometric Data"

Industry claim: S.71 v3.3's definition is "overbroad" and will affect virtual try-on applications.

Response: The S.71 v3.3 definition covers data generated from "technological processing" of biological characteristics that "allow or confirm unique identification." The exclusions in S.71 v3.3 §2415a(3)(B) explicitly carve out digital photographs, audio/video recordings, and data derived from them "unless such data is generated to identify a specific individual." A virtual makeup try-on that does not identify the user is plainly excluded. **The industry's example is not supported by the statutory text.**

The Oregon Consumer Privacy Act uses substantively identical carve-out language: photographs, audio recordings, video recordings, and data derived from them are excluded from the biometric definition "unless the data were generated or used to identify a particular consumer." Oregon also defines biometric data to include information that may "allow" unique identification, not merely data collected for that purpose, which is the same functional approach Vermont takes. **The industry's claim that Vermont's approach is an overbroad outlier cannot be squared with Oregon's enacted law, which uses the same logic and has been in effect since July 2024.**

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 2: "Collect" as a Standalone Definition

Industry claim: Defining "collect" separately creates uncertainty and will overwhelm consumers with disclosures about ordinary website interactions.

Response: It is unclear how defining “collect” as a standalone term requires any additional requirements regarding disclosures about ordinary website interactions. Collection was previously a subset of the term “process” or “processing” and defining it separately adds clarity. The reason it was separated was to allow us to make clear for businesses that they may use personal data collected under the data minimization rules for targeted advertising purposes.

Issue 3: "Consent" Definition and Methodology

Industry claim: Requiring consent mechanisms to offer "symmetry in choice" and avoid "confusing" interfaces is unprecedented and will force costly UI redesigns.

Response: The 2025 CTDPA amendments explicitly address dark patterns and the quality of consent mechanisms. Connecticut is moving toward Vermont's approach, not away from it. California’s privacy regulations also require businesses to offer “symmetry in choice” and avoid confusing interfaces when obtaining consent – the language in this definition was pulled directly from California’s regulations. More importantly, the Vermont AADC (Act 63) already imposes analogous requirements on covered businesses serving minors, including prohibiting "a singular setting that would make all of the default privacy settings less protective at once." The requirement that consent not use "choice architecture that impairs or interferes with the consumer's ability to make a choice" is consistent with FTC guidance on dark patterns and is reflected in the CTDPA's existing dark pattern provisions. Calling this unprecedented misreads the trajectory of state law. From an implementation standpoint, the claim that symmetry-in-choice requirements will force costly UI redesigns overstates the operational burden. Consent management platforms already in widespread use — including by nonprofits and university foundations — support compliant consent UI configurations as a matter of platform capability, not custom engineering. The delta between a compliant and non-compliant consent experience is typically a configuration decision within tools organizations are already licensing, not a ground-up rebuild. The cost argument assumes a baseline of intentionally asymmetric design that compliant organizations should not be defending.

Issue 4: "Identified or Identifiable Individual"

Industry claim: Including precise geolocation data, online identifiers, and device identifiers "sweeps in" advertising IDs and IP addresses beyond what other states do.

Response: This is a policy disagreement dressed as a legal accuracy claim. Advertising IDs and persistent device identifiers ***do*** identify individuals; that is their commercial purpose. The industry argument that consumers "would not expect" these identifiers to implicate their privacy is empirically contested and runs counter to the entire purpose of comprehensive privacy law.

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 5: "De-identified Data" and HIPAA Tie

Industry claim: Tying the de-identification standard to HIPAA's 45 C.F.R. § 164.514 imposes "healthcare-grade compliance costs on non-healthcare businesses."

Response: HIPAA's Expert Determination method (§164.514(b)) and Safe Harbor method (§164.514(b)(2)) are well-understood, widely implemented standards. Vermont is not inventing a new framework; it is referencing an existing one. Businesses that lack a HIPAA-equivalent de-identification process arguably are not actually de-identifying data in a meaningful sense. The claim that this "may discourage the use of de-identified data for beneficial purposes" proves too much: every meaningful de-identification standard has compliance costs. The question is whether the standard is meaningful, and HIPAA's is. Oregon's OCPA also references 45 C.F.R. § 164.514 as the de-identification standard for health-related data. Vermont is not alone in this approach.

The claim that HIPAA's de-identification standard imposes disproportionate costs on non-healthcare businesses assumes that those businesses are currently applying a rigorous alternative standard. In practice, data described as "anonymized" or "de-identified" in non-healthcare contexts frequently means pseudonymized – identifiers replaced or hashed, but re-identification possible through combination with other data sources. The HIPAA standard is demanding because meaningful de-identification is demanding. Referencing it does not impose healthcare compliance on non-healthcare entities; it establishes that de-identification claims should reflect actual de-identification.

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 6: "Derived Data" as a Standalone Definition

Industry claim: Separately defining derived data will require businesses to trace and delete algorithmic outputs, and will produce "bloated" privacy disclosures.

Response: The failure to define derived data is precisely what allows businesses to evade subject access requests and deletion rights by re-generating inferences from retained raw data. This is not hypothetical; it is a documented gap in state privacy laws that Vermont is closing.

California includes “inferences” within its definition of personal information, while Oregon explicitly includes "derived data" in its definition of "personal data". California and Oregon's approaches have been in effect for years with no reported compliance crisis. The CTDPA's 2025 amendments strengthened access rights to include inferences, moving in the same direction. Vermont's approach of defining the category upfront is more coherent, not less. Any business building California-compliant systems is already grappling with inferences and derived outputs under the CCPA's access rights framework.Defining derived data is not a novel burden; it is a logical extension of rights businesses already have to navigate.

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 8: "Precise Geolocation Data" Radius

Industry claim: The 1,850-foot radius (vs. Connecticut's 1,750 feet) will capture vacation photos and restaurant check-ins.

Response: The distinction between 1,850 and 1,750 feet is 100 feet. California’s privacy law also defines precise geolocation data at a radius of 1,850 feet, and Oregon’s data privacy law contains the same “present or past” location qualifier. However, a suggested compromise would be to match Oregon’s definition here (a state that also bans the sale of precise geolocation data). That definition reads: *[information derived from technology that] accurately identifies within a radius of 1,750 feet a consumer’s present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates.*

Issue 9: "Processing" / "Otherwise Handling"

Industry claim: The phrase "otherwise handling" eliminates any limiting principle.

Response: California’s definition of processing does not even include a non-exhaustive list like we do in S.71 v3.3, so there is no limiting principle in its definition, which reads: “Processing” means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

That said, a suggested compromise would be to remove the non-exhaustive list of examples to be consistent with California.

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 10: "Processor" Definition Including Sub-Processors

Industry claim: Including persons acting on behalf of "another processor" will require businesses to renegotiate existing processor agreements.

Response: Sub-processor accountability is standard practice in GDPR-aligned compliance and increasingly in U.S. state law. The CTDPA itself requires controller-processor contracts to address sub-processors through downstream obligations. Requiring that sub-processors be covered is a consumer protection measure: data handed off down a chain of service providers should not lose its protections at the second link. The claim that this is unique to Vermont misreads the existing CTDPA contractual requirements, which already contemplate sub-processor arrangements.

That said, a suggested compromise would be to copy Vermont's AADC (Act 63 aka Kids Code) definition of "Processor" means a person who processes personal data on behalf of a controller.

Issue 12: "Personal Data" Including Household-Linked Devices

Industry claim: Including data linked to household devices creates "unintended consequences" for rights like access and deletion.

Response: The statute's authentication requirements (§2415d(c)(4)) address this: controllers are only required to comply with authenticated requests. The domestic violence scenario raised by the industry is already addressed; a controller is not required to honor a request it cannot authenticate to the actual consumer.

Oregon's definition of personal data is substantively identical to Vermont's on this point, covering "data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household." Oregon has been enforcing this definition since July 2024. The industry raised the same objections to Oregon's approach. Those objections did not materialize into the compliance crisis predicted. California's CCPA similarly covers information linked to devices and households. A business already compliant with California and Oregon law has already solved this problem.

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 13: "Publicly Available Information" Exclusions

Industry claim: S.71 v3.3's exclusions raise First Amendment concerns.

Response: "Raise First Amendment concerns" does not mean that the law violates the First Amendment. It means that an industry trade group might try to invalidate the law on First Amendment grounds, much like Trans Union did when it attempted, and failed, to invalidate the Fair Credit Reporting Act (FCRA) on similar grounds (Trans Union LLC v. FTC, 267 F.3d 1138 (D.C. Cir. 2001); Trans Union LLC v. FTC, 295 F.3d 42 (D.C. Cir. 2002)). Note that the FCRA is

a law that restricts the collection, sale, and use of personal information and includes Publicly Available Information (PAI), much like S.71.

Data brokers pose a safety risk to individuals when they compile and sell detailed profiles containing personal information, even if some of that information is publicly available. Data brokers that compile and sell publicly available information still pose privacy, safety, and security risks to individuals, so they should not be excused from privacy laws.

Connecticut SB 4, passed in May 2026, amends the CTDPA to redefine "publicly available information" along similar lines, closing the aggregation loophole that the industry here defends. The recommendation for the language in S.71 v3.3 comes directly from the Connecticut Attorney General's enforcement report.

Further, the Supreme Court has acknowledged that the dissemination of PAI can raise privacy concerns, because PAI is often protected by "practical obscurity" – in other words even though the information is "public," it is not easily available, a critical distinction that industry ignores. For example, in Vermont, court records of divorces are "public records." However, they are generally not put into the Courts' easily accessible public filing system, creating a barrier to data brokers trying to scrape these very sensitive, yet public, documents.

Industry frequently claims that their harmful practices raise First Amendment concerns, but courts have held otherwise.

Vermont Specific Note: Exact match of Vermont AADC (Act 63 aka Kids Code).

Issue 14: "Sensitive Data" Expanded Categories

Industry claim: Adding categories like philosophical beliefs, pregnancy status, income, and a "knew or should have known" minor standards are novel and create redundancies and friction.

Response: Several of these objections are factually incorrect or misleading in light of enacted Vermont and multistate law.

On minors: The "knew or should have known" standard is not novel; it is the Vermont AADC's own framework. S.71 v3.3's integration of "knew or should have known" for sensitive data classification is consistent with, and reinforced by, Vermont's AADC. The industry's claim that this "effectively requires age-gating across all digital services" ignores that the AADC already establishes an age assurance framework with rulemaking authority delegated to the Attorney General, authority that specifically includes designing "privacy-preserving" age verification methods that minimize burden. Maryland's MODPA also applies its minor data protections to anyone under 18 using the same "knows or should know" framing.

On pregnancy status: S.71 v3.3 defines "consumer health data" separately to include gender-affirming health data and reproductive/sexual health data. The redundancy objection misreads the statute: the sensitive data classification operates across the entire act, while consumer health data provisions trigger specific obligations under §2415k. These operate at

different layers of the statute. Delaware's definition of sensitive data also includes pregnancy status.

On philosophical beliefs: This category exists in GDPR Article 9 and in California's comprehensive privacy law, but a suggested compromise would be to remove this if there are concerns.

On income and indebtedness: Given Vermont's rural economic context and the documented harms of financial data aggregation by data brokers (the subject of H.211, which passed the Vermont House in March 2026), covering income and debt data as sensitive is a principled policy choice, not a technical error.

On transgender and nonbinary status: Connecticut, Delaware, Maryland, New Jersey, and Oregon expressly include "status as transgender or nonbinary" in their sensitive data definition. Vermont's inclusion of this category is in line with those five states.

Issue 15: "Targeted Advertising" / "Commonly Branded"

Industry claim: "Commonly branded" is not in any other state law and creates ambiguity.

Response: "Affiliate" is a defined term in S.71 v3.3 (§2415a(1)), and it includes entities sharing "common branding." The "commonly branded" qualifier in the targeted advertising exclusion is consistent with that definition and limits the exclusion to genuine first-party contexts within a recognized brand family. A co-branded promotion with an unaffiliated third party is not a "commonly branded" relationship under the affiliate definition. That said, at the end of the day, a suggested compromise would be to copy Connecticut 2025.

APPLICABILITY

Issue 16: "Greatest Protection" Conflict Rule

Industry claim: The "greatest protection" standard is "completely subjective" and "threatens to undermine the entire statute."

Response: This objection conflates interpretive difficulty with legal invalidity. Choice-of-law provisions favoring greater consumer protection exist in multiple state frameworks. Vermont's approach is that where two applicable laws conflict, the more protective one governs, which is a principled rule, not an arbitrary one. Vermont courts regularly resolve statutory conflicts; this provision gives them a clear directive.

EXEMPTIONS

Issues 17-25: HIPAA and Health-Related Exemptions

Industry claims: Various objections to how S.71 v3.3 structures HIPAA-related exemptions, including the absence of a limited data set exemption, no intermingled-data exemption, and the scope of the health care record exemption.

Response: The committee heard testimony from and further worked with financial, insurance, and health care sector representation to craft necessary HIPAA-related exemptions for Vermont, as a result, certain exemptions will inherently be outliers specific to Vermont, just as there are state-specific exemptions as seen in various states. If the committee wants to edit and/or remove these exemptions, further consideration and testimony is suggested.

Issue 21: Third-Party Administrators

Industry claim: S.71 v3.3 exempts third-party administrators, which is an outlier.

Response: The committee heard testimony from and further worked with financial, insurance, and health care sector representation to craft necessary HIPAA-related exemptions for Vermont, as a result, certain exemptions will inherently be outliers specific to Vermont, just as there are state-specific exemptions as seen in various states. If the committee wants to edit and/or remove these exemptions, further consideration and testimony is suggested.

Issue 26: Nonprofit Exemption

Industry claim: S.71 v3.3 only exempts specific categories of nonprofits rather than all § 501(c) organizations.

Response: Connecticut’s broad nonprofit exemption has been criticized by privacy advocates and state attorneys general, including Connecticut's own AG in enforcement reports. It is also worth noting that nonprofits are not exempt from CTDPA’s health data provisions nor from COPPA. Previous versions of this bill covered all nonprofit organizations, but the narrower approach proposed in S.71 v3.3 was drafted in response to concerns from Vermont nonprofits. Oregon's OCPA, Alabama’s APDPA, Colorado’s CPA, Delaware’s DPDPA, Maryland’s MODPA, Minnesota’s MCDPA, Montana’s MCDPA, and New Jersey’s NJCCIC all take a similar targeted approach, exempting only specific nonprofit categories rather than all 501(c) organizations.

The nonprofit sector has operated under COPPA, FERPA, HIPAA (for covered entity relationships), and CAN-SPAM without a categorical carve-out. The idea that state comprehensive privacy law should be different has no principled basis in the existing regulatory landscape.

The industry's implicit premise (that nonprofit tax status signals lower privacy risk) does not hold at operational scale. Large national nonprofits routinely deploy the same digital advertising infrastructure as for-profit enterprises: behavioral tracking pixels, third-party data co-ops, appended constituent lists, and consent management platforms governed by the same ad-tech vendors. Organizational mission does not determine whether a constituent's health history, giving behavior, or online activity is at risk of misuse or unauthorized disclosure. A blanket

exemption based on tax status would provide the same protections to a small community food pantry and a large national health-mission organization processing millions of records, a distinction the law should not ignore.

The 35,000-consumer applicability threshold already functions as a de facto exemption for small and community-based nonprofits. The organizations most likely to trigger coverage under S.71 v3.3 are those with meaningful digital footprints such as those large enough to run national campaigns, operate data co-op relationships, or deploy analytics infrastructure across multiple platforms. A blanket 501(c) exemption does not protect Vermont's local nonprofits; it protects large-scale data operations that happen to be tax-exempt.

This concern is particularly acute for health-mission nonprofits. An organization whose work centers on patients, survivors, and caregivers is processing health-adjacent data that is precisely what Vermont's sensitive data framework is designed to protect. Exempting those organizations wholesale would leave their constituents with fewer rights against the entities they trust most with their most sensitive information, the opposite of the bill's intent.

The state-law record bears this out. States that enacted broad nonprofit exemptions have seen those exemptions function as operational loopholes for data co-op participation, list rental, and digital advertising practices that would otherwise require consumer notice and opt-out rights. The targeted exemption structure in S.71 v3.3 closes that gap while preserving appropriate carve-outs for organizations whose data processing is genuinely distinct – victim services, fraud prevention, and enrollment reporting among them.

Issue 27: Political Committees

Industry claim: Vermont does not separately exempt political committees.

Response: Connecticut's political committee exemption covers candidate committees, party committees, and political committees. Vermont's statute does not provide this exemption. This is an intentional policy choice, not an oversight, and reflects Vermont's interest in ensuring political data operations remain subject to privacy standards and not exempting ourselves from the laws we are passing.

Issue 30: Security and Fraud Prevention / "Targeted At"

Industry claim: Limiting the fraud prevention carveout to illegal activity "targeted at or involving" the controller prevents businesses from taking protective steps.

Response: The statutory text (§2415i(a)(9)) permits responding to "any illegal activity targeted at or involving the controller or processor or its services." This is a broad carveout where an entity could evade the data minimization requirements in the bill by claiming they were “protecting against” fraud generally. Limiting it to fraud "involving the controller's services" ensures that businesses can collect and use data to combat fraud within their organizations without leaving a huge loophole in the law.

CONSUMER RIGHTS

Issue 31: Authorized Agent Authority

Industry claim: Extending authorized agent authority beyond opt-out rights to access, correction, and deletion "creates massive consumer identity theft risks."

Response: The statute's authentication requirements (§2415d(c)(4)) specifically address this concern: a controller is not required to comply with a request it cannot authenticate using "commercially reasonable efforts." An authorized agent operating fraudulently does not get a pass under S.71 v3.3; authentication is a prerequisite. The industry's identity theft concern is presented as if the statute provides no safeguard. It does. California's CCPA also permits authorized agents to exercise the full range of consumer rights, including access and deletion, subject to verification requirements. Vermont's approach is consistent with California's.

Issue 33: Third-Party Deletion / Single Compliance Pathway

Industry claim: Providing only one compliance pathway for third-party deletion removes flexibility.

Response: The option that Connecticut provides (and we delete) is a massive loophole for data brokers to treat deletion requests as opt-out requests instead. Data brokers and other third parties should have to honor a consumers' deletion request just as controllers do.

CONTROLLERS' DUTIES

Issue 34: Data Minimization

Industry claim: Applying "reasonably necessary and proportionate" to both collection and processing, rather than just collection, is an overbroad departure from the national standard.

Response: Responding to the State Privacy and Security Coalition and Chamber's concerns with the data minimization rule in previous versions of the bill, S.71 v3.3 adopts California's data minimization standard. It combines the language from the California Consumer Privacy Act and its accompanying regulations so that any business that is already complying with California's law would not have to change their practices. Many companies build their privacy framework around California's rules because they are stricter than what exists in most other state privacy laws.

California's law applies data minimization to collection, use, retention, and sharing, and that is mirrored in the rules proposed in S.71 v3.3. The CPPA's Enforcement Advisory No. 2024-01 on data minimization is unambiguous: the standard applies to "every purpose for which they collect, use, retain, and share consumers' personal information." Any business currently compliant with California law is already operating under the same minimization requirement. Vermont is not

asking those businesses to do anything they aren't already doing for their largest regulated market.

SPSC's framing also assumes that data minimization is primarily a collection-time decision – that once a business collects personal data, they should be able to use it however they wish. But this is where much of the abuse of personal data happens – behind the scenes in ways consumers don't expect, such as the sale of their data to data brokers. It is these secondary uses that cause the most significant privacy risks. Limiting the standard to collection while leaving processing unregulated would protect consumers at the front door while leaving the back door open.

In addition, SPSC ignores the extreme risk of over-collecting and over-retaining personal information caused by data security breaches. It is common for data breaches to be much more serious than they should have been because the attacked companies have failed to delete information they no longer had use for, or have collected and stored more information than they actually needed.

Issue 36: "Strictly Necessary" Standard for Sensitive Data

Industry claim: The "strictly necessary" standard for sensitive data processing prevents consumers from receiving personalized services they want and is far more restrictive than "every other state."

Response: First, the claim that this is "far more restrictive than every other state" is incorrect. This matches the standard in the Maryland Online Data Privacy Act.

The "strictly necessary" standard means a business cannot collect and use sensitive data speculatively for whatever purpose they please so long as the consumer "consents." We know from practice that consent is easily manipulated – companies simply require "consent" to their terms in order to use the app or service. There is no "disagree" button that allows you to keep using the app even if you don't agree to the terms. That is not a meaningful privacy protection, and it does not, despite SPSC's memo's claims, give consumers any meaningful "control" over their sensitive data. The "strictly necessary" standard instead requires businesses to have a legitimate processing purpose for collecting and using sensitive data.

In practice, the "strictly necessary" standard does not prevent organizations from offering personalized services; it requires that the data collection supporting those services be scoped to what the service actually needs.

Issue 37: Minors and Targeted Advertising

Industry claim: The bill's exceptions for "covered businesses" and "covered minors" under Vermont law create a "two-track compliance regime."

Response: The "covered business" and "covered minor" references are cross-references to Vermont's AADC. The AADC establishes a comprehensive framework for businesses serving minors, including definitions, age assurance rulemaking, and data minimization obligations. This bill's minor provisions integrate with, rather than duplicate, this framework. Calling this a "compliance cliff" misunderstands that Vermont has enacted a coherent statutory ecosystem, not an accidental overlap.

Connecticut's 2025 amendments took a similar approach: SB 1295 raised the minor protection age from 16 to 18 and imposed a categorical prohibition on targeted advertising to minors, stricter than the consent-based approach the industry endorses. Oregon's OCPA prohibits the sale of personal data and targeted advertising for consumers ages 13 to 15 without consent. Vermont is not an outlier on minor protection; the entire field is moving this direction.

Issue 38: Prohibition on Sale of Sensitive Data

Industry claim: An outright ban on selling sensitive data "eliminates consumer choice" and could "reduce access to products and services for those populations" by preventing advertising based on race or sexual orientation.

Response: The claim that prohibiting the sale of sensitive data, including racial origin, sexual orientation, and health data, harms the populations those categories describe is extraordinary. The documented harms of sensitive data markets, including discriminatory profiling, targeting of reproductive health data, and sale of immigration status information, are precisely why those categories are designated sensitive in the first place.

Maryland's MODPA prohibits the sale of sensitive data outright, regardless of consent, and is now in effect and being enforced. Oregon bans the sale of location data and the personal data of minors. Virginia bans the sale of location data, and Connecticut's SB 4, passed May 2026 and awaiting Governor approval, prohibits the sale of precise geolocation data. The assertion that banning sensitive data sales "prevents advertising based on race/sexual orientation, reducing access to products and services" conflates targeted advertising with access to services. People do not lose access to services because their most sensitive personal data cannot be sold to third parties.

Issue 39: Targeted Advertising and "Transfer"

Industry claim: Using "transfer" as a concept alongside "processing" creates undefined compliance risk. The memo also claims that "no other comprehensive state law contains this kind of outright prohibition."

Response: SPSC's claim here that "no other comprehensive state law contains ***this kind of outright prohibition"*** does not make sense in the context of the provision they cite, which, rather than restriction, is a permissive provision that specifically ***allows*** controllers and processors to transfer personal data for targeted advertising purposes.

In other states, transfer is a form of processing. We pull it out and give it its own definition here so we can set rules for particular forms of data transfers.

Issue 41: NIST Framework Mandate for Sensitive Data

Industry claim: Mandating NIST frameworks for sensitive data security locks businesses into specific compliance methodologies.

Response: The Privacy & Cybersecurity Frameworks are defined in S.71 v3.3 (§2415e(a)(2)(B)) to include the NIST Privacy Framework (Version 1.0, January 2020) and Cybersecurity Framework (Version 2.0, February 2024) "or any successor versions thereof." NIST frameworks are not static mandates; they are updated standards, and Vermont's reference tracks those updates automatically. These are the most widely adopted security standards in the United States. The claim that they will require "costly re-engineering" is at odds with how most large and mid-sized companies already document their security posture.

ENFORCEMENT

Issue 47: Private Right of Action

Industry claim: Even a limited private right of action for companies over $1 billion in annual revenue will generate class-action litigation and higher consumer prices.

Response: The private right of action in this bill applies only to companies with over $1 billion in annual revenue, a threshold that by definition excludes small and medium-sized businesses. The concern about compliance costs at that revenue level deserves scrutiny: billion-dollar companies have greater resources to comply and better capacity to absorb litigation risk. They can also afford the staff necessary to ensure compliance with the law. The claim that this threshold creates an "arbitrary compliance cliff" that disadvantages growing companies is the same argument made against every tiered regulatory threshold in every sector; it has never been accepted as a reason to exempt large companies from accountability entirely.

Issue 48: AG Rulemaking Authority

Industry claim: Granting rulemaking authority to the Attorney General creates ongoing uncertainty for businesses.

Response: The Vermont AADC (Act 63) already grants the AG rulemaking authority on age assurance and compulsive use standards, effective July 1, 2025. S.71 v3.3's AG rulemaking authority is consistent with that existing framework.

Regulatory flexibility through rulemaking is not a flaw, it is how privacy law keeps pace with technology. Locking the entire framework in statute with no rulemaking authority produces the opposite problem: law that cannot adapt to new practices and becomes obsolete before it is

even enforced. The multistate record bears this out. Colorado's rulemaking process under the CPA has allowed its framework to address AI-driven profiling, sensitive data processing, and universal opt-out mechanisms in ways the original statute could not have anticipated at enactment. California's CPPA has used its rulemaking authority to issue enforceable guidance on data minimization, automated decision-making, and risk assessments – keeping pace with ad-tech developments that postdate the original CCPA by several years. Rulemaking is also an opportunity for states to provide guidance and clarity to businesses in ways that are not possible in statute.

Issue 49: Fraud Liability for Data Protection Assessment Failures

Industry claim: Treating data protection assessment failures as fraud with treble damages is "wildly disproportionate" and will deter candid self-assessment.

Response: The fraud provision (§2415g(h)(4)) applies only when a controller "knowingly" fails to complete a required validation or includes "false information" in a data protection assessment. This is not a strict liability for imperfect compliance; it is a penalty for deliberately breaking the law and falsifying records. The claim that this will deter candid internal documentation assumes that businesses will respond to fraud liability by lying in their assessments rather than by completing them honestly. That assumption says more about the industry's compliance culture than about the statute's design.

****

SPSC COMPARISON DOCUMENT

The aforementioned State Privacy and Security Coalition (SPSC) comparison document follows:

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.	