A Comprehensive Analysis of U.S. Data Privacy Policies and Regulations

Report Date: November 15, 2025
Prepared By: Specialized Legal Counsel, U.S. Data Privacy & Regulatory Compliance
RE: An Exhaustive Report on All Federal and State Privacy Policies and Rules

---

Executive Briefing: The Fragmented U.S. Privacy Landscape in 2025

The United States does not have a comprehensive federal data privacy law.[1] This foundational absence has created one of the most complex, high-risk, and fragmented regulatory environments for data privacy in the world. In place of a unified standard, businesses must navigate a "patchwork" of regulations on two distinct and often overlapping fronts: (1) a mature set of sector-specific *federal* laws governing sensitive data like health and finance, and (2) a rapidly accelerating and diverging set of *state-level* comprehensive laws.[2]

The year 2025 marks a critical inflection point in this landscape. The momentum for state-level legislation, which accelerated significantly in 2024, has reached a new zenith. Eight new comprehensive state privacy laws have taken effect or were enacted in 2025 alone, bringing the total number of states with such laws to over 20.[2] This proliferation is no longer a niche compliance issue; it represents a central, enterprise-level risk.

This rapid fragmentation, however, presents a dangerous compliance trap. While the number of *jurisdictions* is fragmenting, the *new laws* themselves are largely *consolidating* around two primary models: the California Consumer Privacy Act (CPRA) and the Virginia Consumer Data Protection Act (VCDPA).[7] The sheer speed of legislative adoption is forcing new states to copy existing frameworks, leading businesses to mistake "similar" for "identical."

This report will demonstrate that the most significant legal and financial exposure lies not in the similarities, but in the *subtle divergences*—the critical mutations in key definitions such as "sale," "sensitive data," and "nonprofit exemption" that are buried within these copy-cat laws. The challenge is no longer just tracking the *number* of new laws, but forensically analyzing the

high-impact *mutations* between them.

This report systematically deconstructs this landscape. It will analyze the foundational federal laws, provide a deep comparative analysis of the divergent state-level regimes, detail the high-risk, non-comprehensive state laws that carry unique litigation exposure, and map the evolving enforcement strategies of a newly-emboldened class of federal and state regulators.

The Federal Privacy Framework: Key National-Level Policies and Rules

Before addressing the state-level patchwork, it is essential to define the foundational federal laws that govern specific, high-stakes data sectors. These laws are mature, have powerful enforcement agencies, and apply nationwide.

Health Information Privacy (HIPAA & HITECH)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its subsequent amendments establish the national standards for protecting sensitive patient information.[9]

- **Policies & Rules:**
  - **Scope:** The law applies to "Covered Entities" (health plans, healthcare providers, healthcare clearinghouses) and their "Business Associates" (vendors who handle data on their behalf).[9]
  - **Protected Data:** The law protects "Protected Health Information" (PHI), which is any individually identifiable health information relating to a patient's past, present, or future physical or mental condition, treatment, or payment.[9]
  - **The Privacy Rule:** This rule dictates *how* PHI can be used and disclosed. The general principle is that a Covered Entity cannot use or disclose PHI without patient authorization.[10] The primary exception is for "Treatment, Payment, or Health Care Operations" (TPO).[10]
  - **The Security Rule:** This rule mandates *safeguards* to protect electronic PHI (ePHI). It requires administrative, physical, and technical security measures to ensure the confidentiality, integrity, and availability of ePHI.[11]
  - **Patient Rights:** The Privacy Rule grants patients a "bill of rights," including the right to receive a Notice of Privacy Practices [10], the right to request restrictions on disclosure [10], and the right to access and obtain a copy of their PHI.[12]

- 2025 Developments & Evolution:
  For decades, HIPAA was a relatively static compliance framework. The 2025 landscape proves this era is over; HIPAA is now a dynamic and contested body of law, evolving in real-time to address both technological and political threats.
  1. **Cybersecurity Overhaul:** In response to "significant increases in breaches and cyberattacks," the Department of Health and Human Services (HHS) has issued a Notice of Proposed Rulemaking (NPRM) to significantly *strengthen* the Security Rule. This proposal aims to revise standards to address modern cyber threats and common deficiencies observed in investigations.[11]
  2. **Faster Patient Access:** Expected changes to the Privacy Rule in 2025 will *shorten* the timeframe for covered entities to respond to patient access requests from 30 days down to 15 days.[12]
  3. **Reproductive Health Data:** In 2024, HHS issued a rule to limit the disclosure of PHI for reproductive health care. However, on June 18, 2025, a U.S. District Court *vacated* most of this rule, demonstrating that PHI is now a central, contested element in post-Dobbs legal battles.[13]
- **Enforcement:** The HHS Office for Civil Rights (OCR) enforces HIPAA.[9] Penalties are tiered based on culpability. A Tier 4 violation (willful neglect, not corrected) can cost **$71,162** per violation, with an annual cap of **$2,134,831**.[14] "Knowing" violations can also result in criminal penalties, including fines up to **$250,000** and imprisonment for up to 10 years.[15] OCR has been highly active in 2025, issuing multiple six- and seven-figure fines for non-compliance, particularly related to ransomware investigations and failures to provide timely patient access.[16]

Children's Online Privacy (COPPA)

The Children's Online Privacy Protection Act (1998) (COPPA) is a federal law enforced by the Federal Trade Commission (FTC) that governs the online collection of data from children.[1]

- **Policies & Rules:**
  - **Scope:** Applies to operators of websites or online services "directed to children" under 13, or operators who have "actual knowledge" they are collecting personal information from a child under 13.[19]
  - **The Core Rule:** Businesses *must* provide direct notice to parents and obtain **"verifiable parental consent" (VPC)** *before* collecting, using, or disclosing a child's personal information.[20]
  - Parental Rights: Parents must be given the ability to review their child's personal information, delete it, and restrict its
    further use.20

- 2025 Developments: The Finalized Amended Rule
  In January 2025, the FTC finalized significant amendments to the COPPA Rule, which take effect on June 23, 2025, with a one-year compliance deadline of April 22, 2026.20 This update is a strategic policy maneuver designed to functionally ban the monetization of minors' data.
  - **Separate Consent for Ads:** The new rule *explicitly requires* operators to obtain **separate verifiable parental consent** to disclose children's information to third-party companies for purposes like targeted advertising.[23]
  - **Data Retention Limits:** The rule now requires operators to retain personal information *only* "for as long as reasonably necessary" to fulfill the specific purpose for which it was collected.[23]
  - **Updated Notices:** Direct notices to parents must now be more detailed, including the names and categories of *all* third parties receiving the data and the *purpose* of the sharing.[24]

  These rule changes, particularly the *separate* VPC for ads, are a form of "friction-based" ban. The FTC's press release stated the goal is "limiting companies' ability to monetize kids' data".[23] By requiring a *second*, high-friction consent that parents will likely deny, the FTC has made the ad-based business model for the under-13 audience operationally non-viable, achieving its policy goal without a legislative ban that could face legal challenges.
- Enforcement: The FTC enforces COPPA vigorously, often in tandem with its broad authority under Section 5 of the FTC Act ("unfair practices").25 Penalties are severe. The 2022 Epic Games (Fortnite) settlement was a record $520 million for alleged COPPA and Section 5 violations.25 The FTC has continued this trend in 2025 with enforcement actions against Disney, Cognosphere, and Apitor.27

Financial Privacy (GLBA)

The Gramm-Leach-Bliley Act (1999) (GLBA) requires financial institutions to protect consumer financial data and is built on three key rules.[18]

- **Policies & Rules:**
  - **Scope:** Applies to "financial institutions," a broad term that includes not just banks, but companies that offer consumers financial products or services like loans, financial or investment advice, or insurance.[29]
  - **The Privacy Rule:** Requires institutions to provide customers with a clear and conspicuous privacy notice explaining their information-sharing practices.[29] It also gives consumers the right to **"opt out"** of having their nonpublic personal information shared with certain nonaffiliated third parties.[29]
  - **The Safeguards Rule:** Mandates that all financial institutions develop, implement,

and maintain a comprehensive, *written* information security program with administrative, technical, and physical safeguards to protect customer information.[28]
    - **The Pretexting Rule:** Prohibits the use of false or dishonest methods (pretexting) to obtain customer financial information.[28]
- 2025 Developments: The Safeguards Rule Breach Notification
  The most significant recent change to GLBA is an amendment to the Safeguards Rule that introduces a mandatory breach notification requirement. This new rule fundamentally shifts GLBA from a "policy" framework to a "reporting" framework.
    - **The New Rule:** Non-banking financial institutions must now notify the FTC *within 30 days* of discovering a "notification event" (a breach of unencrypted customer information) that affects **500 or more consumers**.[32]
    - This change transforms the Safeguards Rule from a passive, internal-facing compliance document into an *active, external-facing regulatory reporting function*. The 30-day clock creates immense pressure and provides the FTC with a real-time dashboard of security failures across the industry, which it can use to target enforcement.
- **Enforcement:** Enforced by the FTC [29] and the Consumer Financial Protection Bureau (CFPB).[31] For 2025, the CFPB has authority to issue penalties for "knowing" violations of federal consumer financial laws up to **$1,443,275** *per day*.[33]

Consumer Financial Reporting (FCRA)

The Fair Credit Reporting Act (1970) (FCRA) regulates the collection and use of consumer credit information and, unlike other areas of privacy, represents a "reverse-patchwork" where federal power is *centralizing*.[18]

- **Policies & Rules:**
    - **Scope:** Applies to "Consumer Reporting Agencies" (CRAs) (e.g., credit bureaus) and the entities ("furnishers" and "users") that provide and use the data.[35]
    - **The Core Rule ("Permissible Purpose"):** A CRA may *only* furnish a consumer report to a user who has a "permissible purpose" (e.g., for a credit application, employment, insurance).[36] Using consumer reports for general marketing is *not* a permissible purpose.[36]
    - **Consumer Rights:** Consumers have the right to access their report, request a credit score [37], and dispute inaccurate information.
- 2025 Developments: The Federal-State Power Struggle
  In 2025, the federal government is actively and aggressively clawing back authority from the states in the credit reporting sphere.
    1. **Medical Debt Rule:** The CFPB finalized a rule (effective March 17, 2025) that, in most

cases, *prohibits* creditors from obtaining and CRAs from reporting information on medical debts.[38]

2. **"Trigger Leads" Restriction:** The Homebuyers Privacy Protection Act (signed September 5, 2025) amends FCRA to *restrict* the practice of CRAs selling "trigger leads"—lists of consumers who have just applied for a mortgage—to other lenders.[36]
3. **The Preemption War:** This is the most significant development. In October 2025, the CFPB issued an interpretive rule *clarifying* that FCRA "generally preempts State laws that touch on broad areas of credit reporting".[39] This new rule *replaced* a 2022 rule that had a *narrower* view of preemption.[39] This is a *direct* move against states like Colorado, which passed its own law (HB 23-1126) prohibiting medical debt reporting. That state law is now being challenged in court *specifically* on the grounds of FCRA preemption.[40]

- **Enforcement:** Enforced by the CFPB and FTC. The CFPB announced a **$15 million** penalty against Equifax in January 2025 for FCRA violations.[41]

Table 1: Federal Privacy Law Framework (2025)

Law	Scope of Coverage	Protected Data	Core Policies & Rules	Enforcement Agency
HIPAA	Health plans, healthcare providers, and their "Business Associates".[9]	"Protected Health Information" (PHI).[10]	**Privacy Rule:** Requires patient authorization for use/disclosure.[10] **Security Rule:** Mandates safeguards for ePHI.[11] **Patient Rights:** Right to access, correct, and request restrictions.[10]	HHS Office for Civil Rights (OCR) [9]
COPPA	Websites/online services directed to	"Personal Information" from children	**VPC:** Must get "verifiable parental	Federal Trade Commission

	children <13 or with "actual knowledge" of collecting from them.[19]	<13.[20]	consent" *before* collection.[20] **2025 Rule:** Requires *separate* VPC for targeted ads.[23] **Parental Rights:** Right to review and delete child's data.[20]	(FTC) [1]
GLBA	"Financial Institutions" (e.g., banks, lenders, financial advisors).[29]	"Nonpublic Personal Information" (NPI).	**Privacy Rule:** Requires privacy notice and consumer "opt-out" of sharing.[28] **Safeguards Rule:** Requires a written information security program.[28] **2025 Rule:** Mandates FTC breach notification.[32]	FTC & CFPB [29]
FCRA	"Consumer Reporting Agencies" (CRAs), and data furnishers/users.[35]	"Consumer Reports" (credit and background info).[35]	**Permissible Purpose:** Users must have a valid, legal reason to access a report.[36] **Consumer Rights:** Right to access,	CFPB & FTC [37]

			dispute, and sue.[37] **2025 Rule:** Prohibits reporting of most medical debt.[38]	

Comprehensive State Privacy Laws: A Comparative Analysis of Policies and Rules

This is the "patchwork" itself. As of late 2025, over 20 states have enacted comprehensive data privacy laws.[3] Eight of these became effective or were passed in 2025 alone: **Delaware** (Jan 1), **Iowa** (Jan 1), **Nebraska** (Jan 1), **New Hampshire** (Jan 1), **New Jersey** (Jan 15), **Tennessee** (July 1), **Minnesota** (July 31), and **Maryland** (Oct 1).[2]

The most effective analysis is a *thematic* one, comparing the states across the core "policies and rules" that define them.

The Foundational Models: California (CPRA) vs. Virginia (VCDPA)

Nearly all 20+ state laws are derivatives of two foundational models.[8]

1. **The California Model (CPRA):** The California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), created the first "comprehensive" framework.[8]
    - **Philosophy:** Generally more consumer-protective.
    - **Key Features:**
        - **Broad Definitions:** Defines "personal information" broadly.[48]
        - **"Sale" Definition:** Defines "sale" *broadly* to include the exchange of data for "monetary **or other valuable consideration**".[1] This is designed to capture ad-tech data sharing.
        - **Sensitive Data:** Provides a consumer **right to "Limit"** the use and disclosure of sensitive data (an **opt-out** model).[6]
        - **Scope:** *Includes* B2B and employee data (the exemption for this data *expired*).[49]
        - **Enforcement:** Enforced by a *dedicated* agency, the **California Privacy**

Protection Agency (CPPA).[8]
        - **Private Right of Action:** A *limited* private right of action, but only for data breaches.[50]
2. **The Virginia Model (VCDPA):** The Virginia Consumer Data Protection Act was the second law passed and became the blueprint for the more business-friendly "VCDPA-model".[8]
    - **Philosophy:** Generally more business-friendly.
    - **Key Features:**
        - **"Sale" Definition:** Defines "sale" *narrowly* as "the exchange of personal data for **monetary consideration**".[51] This *excludes* most ad-tech data sharing.
        - **Sensitive Data:** Requires controllers to get consumer **opt-in consent** *before* processing sensitive data.[6]
        - **Scope:** *Permanently exempts* B2B and employee data.[49]
        - **Enforcement:** Enforced by the State Attorney General.[8]
        - **Private Right of Action:** None.

This "sale" definition is the primary fault line in U.S. privacy. However, the models are hybridizing. For example, New Jersey's law (NJDPA) is a VCDPA-style law but adopts California's *broader* "valuable consideration" definition of "sale" [1], demonstrating the high-risk, nuanced nature of this single legal term.

Core Policy: Consumer Rights

A standard "bill of rights" has emerged across all 20+ states.[54]

- **The Standard Rights:**
    - **Right to Access/Confirm:** To know if a company is processing your data.[54]
    - **Right to Correct:** To fix inaccurate data.[54] (A notable exception is Iowa's law, which *does not* include this right [56]).
    - **Right to Delete:** To have your data deleted.[54] (Iowa's is limited to data the consumer *provided*).[54]
    - **Right to Data Portability:** To get a copy of your data.[54]
- **The Opt-Out Rights:**
    - **Right to Opt-Out of "Sale":** *All* states provide this, though its power depends on the "Sale" definition.[54]
    - **Right to Opt-Out of Targeted Advertising:** Provided by *all* states *except* Iowa.[56]
    - **Right to Opt-Out of Profiling:** Provided by most states, but *not* Iowa.[56] Minnesota's law is unique, granting a right to *question* the results of profiling.[4]
- The "Universal Opt-Out" (Global Privacy Control - GPC):

This is the policy requiring businesses to honor browser-based signals (like GPC) as a valid opt-out request. This is rapidly becoming the de facto national technical standard.

- It is *mandated* by: Colorado [44], Connecticut [44], Texas [44], Delaware [56], Nebraska [56], Minnesota [56], New Hampshire [56], New Jersey [56], Tennessee [56], Maryland [56], Montana [6], and Oregon.
- Because a critical mass of over 10 states, including major economies, *mandates* that businesses implement the technical capacity to honor GPC, it is no longer operationally viable to build a state-by-state opt-out system. The fragmentation of *laws* has, ironically, forced a *convergence* of *technology*.

Core Policy: Business Obligations (Controllers & Processors)

All laws impose a similar set of duties on "Controllers" (the entity determining *why* data is processed) and "Processors" (vendors).

- **Privacy Notices:** All states require a clear, accessible privacy notice.[50]
- **Data Protection Assessments (DPAs):** All states require controllers to conduct and document DPAs for any "high-risk" processing activities, such as processing sensitive data, selling data, and profiling.[54]
- **Data Minimization:** All states require controllers to limit data collection to what is "necessary" for the disclosed purpose.[54]
  - However, Maryland's Online Data Privacy Act (MODPA) creates a *radical, new, and stringent* standard that has become the new "high-water mark."
  - MODPA limits collection to what is "reasonably necessary and proportionate *to provide or maintain a product or service requested by the consumer*".[57]
  - This language *prohibits* collecting data for *other* purposes (like R&D, future marketing, or AI training) *even if the consumer consents*.
  - MODPA also *bans the sale of sensitive data outright*.[57] This makes MODPA, not CPRA, the *strictest data minimization law* in the United States.

The Critical Divergence: Definitions and Exemptions

This is where the *real* compliance risk lies. The differences in *scope* and *definitions* determine *if* and *how* these laws apply to a business.

- Policy: "Sensitive Data" Consent (Opt-in vs. Opt-out)
  This is the second major "fault line" after the "Sale" definition.

    - **Definition:** Most states define "sensitive data" similarly: race/ethnicity, religious beliefs, mental/physical health diagnosis, sexual orientation, citizenship, genetic/biometric data, and precise geolocation.[3] This definition is expanding, with Connecticut adding "neural data" [58] and New Jersey adding "financial information".[53]
    - **The Consent Split:**
        - **Opt-In (Consumer must say "Yes"):** This is the **VCDPA-model** and the overwhelming *majority* rule. It is used in VA, CO, CT, DE, IN, KY, MD, MN, MT, NE, NH, NJ, OR, RI, TN, and TX.[4]
        - **Opt-Out (Company can process until consumer says "No"):** This is the **CPRA-model**. It is used *only* in **California** ("Right to Limit Use") [6], **Utah** [54], and **Iowa**.[6]
- **Policy: Applicability & Exemptions**
    - **B2B / Employee Data:**
        - **Exempt (Business-Friendly):** The *vast majority* of VCDPA-model states (VA, CO, CT, UT, etc.) have a *permanent* exemption for personal data collected in an employment or business-to-business (B2B) context.[49]
        - **Covered (Consumer-Friendly): California (CPRA)**. The exemption for B2B/employee data *expired*, meaning CPRA *fully applies* to HR and B2B vendor data.[49]
    - **Nonprofit Organizations:**
        - **Exempt (Traditional Model):** Most states, including CA, VA, CO, TX, etc., *exempt* nonprofit organizations from the law.[46]
        - **Covered (The New Trend):** The "nonprofit" safe harbor is eroding. A clear trend in the 2024/2025 class of laws is the *removal* of this exemption.
        - **Delaware (DPDPA)** [56], **New Jersey (NJDPA)** [53], and **Minnesota (MCDPA)** [56] all *include* nonprofits in their scope.
        - **Oregon (OCPA)** also applies to nonprofits, with an effective date of July 1, 2025.[46] This signals a major policy shift and a new compliance burden for universities, charities, and associations.

Table 2: Master Comparison of Comprehensive State Privacy Laws (Key Divergences)

State (Law)	Effective Date	Definition of "Sale"	"Sensitive Data" Consent	B2B/Employee Data	Nonprofit Exemption
California (CPRA)	Jan 1, 2023	**Valuable Consideration** [1]	**Opt-Out** ("Limit Use") [48]	**Covered** [49]	**Yes** (Exempt) [54]

Virginia (VCDPA)	Jan 1, 2023	Monetary Considerati on [51]	**Opt-In** [48]	Exempt [49]	**Yes** (Exempt) [54]
Colorado (CPA)	July 1, 2023	Monetary Considerati on [51]	**Opt-In** [54]	Exempt [49]	**Yes** (Exempt) [54]
Connectic ut (CTDPA)	July 1, 2023	Monetary Considerati on [51]	**Opt-In** [54]	Exempt [49]	**Yes** (Exempt) [54]
Utah (UCPA)	Dec 31, 2023	Monetary Considerati on [51]	**Opt-Out** [54]	Exempt [49]	**Yes** (Exempt) [54]
Texas (TDPSA)	July 1, 2024	Monetary Considerati on [51]	**Opt-In** [6]	Exempt [52]	**Yes** (Exempt) [54]
Oregon (OCPA)	July 1, 2024	Monetary Considerati on [51]	**Opt-In** [54]	Exempt [54]	**No** (Covered) [46]
Montana (MTCDPA)	Oct 1, 2024	Monetary Considerati on [51]	**Opt-In** [54]	Exempt [54]	**Yes** (Exempt) [54]
Delaware (DPDPA)	**Jan 1, 2025**	Monetary Considerati on [51]	**Opt-In** [54]	Exempt [59]	**No** (Covered) [56]
Iowa (ICDPA)	**Jan 1, 2025**	Monetary Considerati on [51]	**Opt-Out** [6]	Exempt [54]	**Yes** (Exempt) [54]
Nebraska (NDPA)	**Jan 1, 2025**	Monetary Considerati on [51]	**Opt-In** [56]	Exempt [54]	**Yes** (Exempt) [54]
New Hampshire	**Jan 1, 2025**	Monetary Considerati	**Opt-In** [54]	Exempt [59]	**Yes** (Exempt) [56]

(NHDPL)		on [51]			
New Jersey (NJDPA)	**Jan 15, 2025**	**Valuable Consideration** [1]	**Opt-In** [54]	Exempt [59]	**No** (Covered) [53]
Tennessee (TIPA)	**July 1, 2025**	Monetary Consideration [51]	**Opt-In** [56]	Exempt [52]	**Yes** (Exempt) [54]
Minnesota (MCDPA)	**July 31, 2025**	Monetary Consideration [51]	**Opt-In** [4]	Exempt [52]	**No** (Covered) [56]
Maryland (MODPA)	**Oct 1, 2025**	Monetary Consideration [51]	**Opt-In** [4]	Exempt [52]	**Yes** (Exempt) [54]

High-Risk State Regulations: Specific-Purpose Laws and Private Rights of Action

Compliance with the "comprehensive" laws is *insufficient* to manage U.S. privacy risk. A separate category of laws—narrowly-focused but with extreme penalties and litigation risks—creates the highest *financial* and *legal* exposure.

Biometric Data (Illinois BIPA)

- **The Law:** The Illinois Biometric Information Privacy Act (BIPA) (2008).[60] It is *not* a comprehensive law; it regulates *only* "biometric identifiers" (fingerprints, face scans, retina scans, etc.).[60]
- **The Policies & Rules:** BIPA prohibits private companies from collecting or storing biometric data *unless* they first:
  1. Provide **written notice** of what is being collected.[62]
  2. Provide written notice of the specific **purpose** and **retention schedule**.[62]
  3. Obtain **written consent** (a "written release").[62]

4. It also *prohibits* selling or profiting from biometric data.[61]

- **The Core Risk:** BIPA's danger comes from its unique **private right of action**.[62] This allows *any* individual (e.g., an employee, a customer) to sue a company *directly* for a *technical violation* of the notice-and-consent rules. The Illinois Supreme Court has affirmed that a plaintiff *does not need to show actual harm* to sue. The litigation risk became so severe (with courts awarding damages "per-scan") that in 2025, the Illinois legislature *amended* BIPA to limit liability to a *single violation* per person, rather than *each time* an employee clocks in.[63] This amendment *confirms* the existential-level risk the law created.

Consumer Health Data (Washington MHMDA)

- **The Law:** The Washington "My Health My Data" Act (MHMDA).[44]
- **The Policies & Rules:** Passed in response to the *Dobbs* decision [65], MHMDA is designed to protect consumer health data *not* covered by HIPAA.[65]
  - **Extremely Broad Scope:** Applies to *any* legal entity doing business in Washington that processes "consumer health data." There are **no applicability thresholds** (e.g., revenue, number of consumers).[65]
  - **Strict, Separate Consent:**
    1. Requires **explicit, opt-in consent** *just to collect* the data.[66]
    2. Requires a ***separate*** **explicit, opt-in consent** *to share* the data.[66]
  - **Selling:** Requires a **written, signed authorization** from the consumer.[67]
  - **Geofencing Ban:** Makes it *unlawful* to use a geofence around any facility that provides health care services.[67]
- **The Core Risk:** MHMDA is arguably *more* dangerous than BIPA. It combines BIPA's **private right of action** [65] with a *broader scope* (no thresholds) and *stricter, more-easily-violated rules* (e.g., "opt-in to *collect*"). This "collect-without-consent" rule is one that almost no website or app is currently designed to handle, making every company doing business in Washington a potential class-action defendant.

Data Broker Registries (CA, TX, OR, VT)

- **The Laws:** A handful of states have passed laws to regulate the opaque "data broker" industry: **California, Texas, Oregon, and Vermont**.[69]
- **The Policies & Rules:**
  - **Registration:** These laws require any entity that qualifies as a "data broker" to

register annually with the state (e.s., CA CPPA, TX Secretary of State) and pay a fee.[69]
    - **The "Texas Anomaly":** Texas amended its law in 2025 to *expand* the definition of "data broker," removing a "principal source of revenue" qualifier, dramatically broadening its scope.[73]
- The California "Delete Act" (SB 361) & "DROP":
  California's law is the most aggressive. The "Delete Act" (SB 361) 75 creates a centralized "Delete Request and Opt-Out Platform" (DROP).76
    - **The Rule:** By **January 1, 2026**, this single web portal will allow a consumer to submit *one request* that directs *every registered data broker* in California to delete their data.[76]
    - **Operational Burden:** Data brokers will be *required* to access the DROP system at least *once every 45 days* to process these deletion requests.[78]
    - **Expanded Transparency:** The 2025 amendments also require brokers to disclose *what* they collect (SSNs, biometrics, union status, etc.) [75] and whether they sell data to **foreign adversaries** (China, Russia), law enforcement, or **AI developers**.[75] This is "policy-by-infrastructure," designed to break the data broker business model by imposing massive, recurring operational costs.

The Nevada Anomaly (SB-220)

- **The Law:** Nevada's law (SB-220) is often *mistakenly* grouped with comprehensive laws.[81]
- **The Policies & Rules:** The law provides a *single* right: the right to opt-out of the **"sale"** of personal information.[82]
- **The Core "Tell":** Nevada's law defines "sale" in the *narrowest possible way*: (1) only for **"monetary consideration"** *and* (2) only to a person who will then **"license or sell"** that data to *other* people.[85] It is not a general privacy law; it is a data broker law.

Table 3: High-Risk & Specific-Purpose State Laws (2025)

Law	Data Type Regulated	Core Requirement (Policy & Rule)	Private Right of Action (PRA)?
Illinois BIPA	Biometric Data [61]	**Written Notice & Written Consent** *before* collection.[62]	**Yes** [62] (High litigation risk)
Washington	"Consumer Health	**Separate Opt-In**	**Yes** [65] (High

MHMDA	Data" (broadly defined, non-HIPAA) [65]	**Consent** *just to collect* data. **Separate Opt-In Consent** *to share* data.[66]	"sleeper" risk)
California Delete Act (SB 361)	Data held by "Data Brokers" [75]	Must register with CPPA.[79] Must process deletions from the **central "DROP" portal** every 45 days.[78]	No (Enforced by CPPA)
Nevada SB-220	Personal Information	Consumer right to **Opt-Out of "Sale."** "Sale" is narrowly defined as **monetary** + for **re-sale**.[85]	No (Enforced by AG)

The Regulatory Landscape: Enforcement, Penalties, and 2025 Evolution

A law is only as strong as its enforcement. In 2025, the enforcement landscape has become fragmented, aggressive, and collaborative.

Federal Enforcement Regime

- **Federal Trade Commission (FTC):** The *de facto* federal privacy regulator. It uses its broad authority under **Section 5 of the FTC Act** to police "unfair or deceptive trade practices".[1] A company's failure to follow its *own* privacy policy is considered "deceptive".[1] In 2025, the FTC is actively investigating and regulating AI [86], biometrics [87], data brokers [87], children's privacy [23], and health data.[87]
- **HHS Office for Civil Rights (OCR):** Enforces HIPAA.[9] Civil Money Penalties (CMPs) are tiered, reaching **$71,162** per violation for willful neglect, up to **$2,134,831** per year.[14]

Criminal penalties (fines + imprisonment) can also be sought.[15]

- **Consumer Financial Protection Bureau (CFPB):** Enforces GLBA and FCRA.[31] Penalties are adjusted for inflation.[34] For 2025, a "knowing" violation can be fined up to **$1,443,275** *per day*.[33]

State Enforcement Regime

- **State Attorneys General (AGs):**
  - **Authority:** For *all* comprehensive state laws (except California), the State AG is the *sole* enforcer.[88]
  - **The "Consortium" Risk Multiplier:** Businesses must not assume they face only one AG. In 2025, AGs are *not* working alone. They have formed a **"bipartisan Consortium of Privacy Regulators"** [90] to *coordinate* investigations and enforcement. As of October 2025, this group includes the AGs from CA, CO, CT, DE, IN, NH, NJ, MN, and OR, plus the CPPA.[90] This means a violation in one member state is effectively a violation in *all* member states. The legal risk is *multiplied*, and multi-state settlements, like the $5.1 million settlement over student data, are the new norm.[92]
- **California Privacy Protection Agency (CPPA):**
  - **Authority:** The CPPA is the *only* dedicated privacy enforcement agency in the U.S. and is extremely active.[8]
  - **2025 Enforcement Actions:** The CPPA has been highly active in 2025, issuing a **$1.35 million fine** (Tractor Supply) [91], a **$345,178 fine** (Todd Snyder) [95], a settlement with **Honda** [91], and a major enforcement *sweep* against Data Brokers.[79]
  - **Penalties:** As of 2025, fines are **$2,663** for each violation, or **$7,988** for *intentional* violations or violations involving *minors*.[98]

Key Compliance Provision: The "Right to Cure" & Its Expiration

This is one of the most significant, under-reported developments of 2025. The "warning phase" of U.S. privacy is over.

- **The Policy:** Most VCDPA-model laws included a "right to cure"—a mandatory 30- or 60-day "grace period" where an AG must *notify* a company of a violation, and the company can *avoid a fine* if it "cures" the violation in that window.[2]
- **The Rule (The "Sunset"):** This "right to cure" was a temporary period. In 2025, *it is expiring*.

- **EXPIRED (Jan 1, 2025):** Colorado (CPA).[6]
- **EXPIRED (Jan 1, 2025):** Connecticut (CTDPA).[44]
- **EXPIRING (Dec 31, 2025):** Delaware (DPDPA).[2]
- **EXPIRING (Dec 31, 2025):** New Hampshire (NHDPL).[2]
- **PERMANENT (No Sunset):** The more business-friendly states (Iowa, Nebraska, Tennessee) have a *permanent* right to cure.[2]

The expiration of the right to cure in major economic states like Colorado and Connecticut means that as of Jan 1, 2025, AGs in those states can *immediately* move to enforcement and fines. The "fix it when we're caught" approach is now financially catastrophic.

2025 Legislative Evolution: The "Moving Patchwork"

The "patchwork" is not static. States that *already have* laws are *already amending them* to be more stringent.[43]

- **Colorado (CPA):** Amended [43] to expand protections for minors <18 [99], add "precise geolocation" to sensitive data [99], and add specific biometric rules.[102]
- **Connecticut (CTDPA):** Amended [43] to add "neural data" to sensitive data and *lower* applicability thresholds (making the law apply to more businesses).[58]
- **Oregon (OCPA):** Amended [43] to *ban* profiling and targeted ads for kids <16 [104] and *ban* the sale of *all* precise geolocation data.[104]
- **Virginia (VCDPA):** Virginia *itself* has breached the "business-friendly" firewall of its own model. The VCDPA's primary feature was its *absolute* prohibition on any private right of action (PRA). However, a 2025 amendment (SB 754) *creates* a **limited private right of action** for violations related to "reproductive or sexual health information" (RHSI).[99] This proves that the "No PRA" wall is not sacred and that hot-button political issues (like post-Dobbs reproductive health) are the primary vector for creating new, high-risk litigation exceptions in otherwise "safe" states.

Table 4: Enforcement & Penalty Matrix (2025)

Agency	Law(s) Enforced	Penalty Structure (Per Violation)	2025 Example / Annual Cap
FTC	COPPA, GLBA, Sec.	Varies;	**COPPA:** $520M (Epic Games) [25]

	5	"Disgorgement"	
HHS / OCR	HIPAA	**Tiered:** - Tier 1 (Lack of Knowledge): $141 - Tier 4 (Willful Neglect): **$71,162** [14]	Annual Cap: **$2,134,831** (for same violation) [14]
CFPB	FCRA, GLBA	**Tiered (Per Day):** - Tier 1: $7,217 - Tier 3 (Knowing): **$1,443,275** [33]	**FCRA:** $15M (Equifax) [42]
CPPA	CPRA	**$2,663** per violation (inflation adj.) [98]	**$7,988** per violation (intentional or minor's data) [98] **Example:** $1.35M (Tractor Supply) [91]
State AGs	State Comp. Laws	Varies (e.g., $7,500 per violation under TX law) [6]	**Example:** $5.1M (Multi-state student data) [92]
IL Citizen	IL BIPA	**$1,000** (negligent) or **$5,000** (intentional/reckless) [63]	(PRA, uncapped class actions)
WA Citizen	WA MHMDA	**Actual damages** or statutory damages [65]	(PRA, uncapped class actions)

Table 5: State "Right to Cure" & Sunset Date Tracker (2025)

State	Cure Period (Grace Period)	Status in Nov 2025
Colorado	60-day	**EXPIRED (Jan 1, 2025)** [6]
Connecticut	60-day	**EXPIRED (Jan 1, 2025)** [44]

Delaware	60-day	**ACTIVE (Sunsets Dec 31, 2025)** [2]
New Hampshire	60-day	**ACTIVE (Sunsets Dec 31, 2025)** [2]
Minnesota	30-day	**ACTIVE (Sunsets Jan 31, 2026)** [2]
New Jersey	30-day	**ACTIVE (Sunsets July 15, 2026)** [2]
Maryland	60-day	**ACTIVE (Sunsets April 1, 2027)** [2]
Iowa	90-day	**PERMANENT** (No Sunset) [2]
Nebraska	30-day	**PERMANENT** (No Sunset) [2]
Tennessee	60-day	**PERMANENT** (No Sunset) [2]
California	N/A	**Discretionary** (No statutory right)

Strategic Synthesis: A Consolidated Model for U.S. Privacy Compliance

The preceding analysis proves that a "patchwork" compliance model—where a company attempts to build 20 different programs for 20 different states—is operationally impossible and legally indefensible. A state-by-state approach will fail.

The only scalable, defensible strategy is a **"Highest Common Denominator" (HCD) compliance framework.** This model synthesizes the *strictest* rule from *any* U.S. law on a given topic and applies that single, high-bar standard *nationally*. This creates a unified data governance program that is *over-compliant* in business-friendly states and *fully compliant* in the most aggressive ones.

Based on the 2025 regulatory landscape, an HCD framework is built from the following

policies:

1. **On "Sale" of Data:** Adopt the **California/New Jersey** definition of "sale" as **"monetary or other valuable consideration"**.[1] This forces the business to map all ad-tech and data-sharing partnerships as potential "sales" and subject them to opt-out mechanisms.
2. **On "Opt-Outs":** Implement a **Universal Opt-Out (GPC)** mechanism *nationally*. This is no longer optional; it is a technical mandate from over 10 states [44] and a primary enforcement priority.[95]
3. **On "Sensitive Data":** Treat *all* sensitive data (using the *broadest* definition, e.g., NJ's, which includes financial info [53]) as requiring consumer **Opt-In Consent**. While California is "opt-out" [48], the *overwhelming majority* (18+ states) are "opt-in".[54] The "opt-in" model is the clear national standard.
4. **On "Data Minimization":** Adopt the **Maryland (MODPA)** standard: data collection must be **"strictly necessary"** for the *specific product or service requested by the consumer*.[57] This is the new high-water mark, and building a program around it future-proofs the business against all other states.
5. **On "Health Data":** Treat *all* consumer health data (including non-HIPAA, app, or inferred data) using the **Washington (MHMDA)** standard. This means **separate opt-in consent for collection** and *another* for sharing.[66]
6. **On "Biometric Data":** Adopt the **Illinois (BIPA)** standard *nationally*. All biometric collection requires explicit **written notice and signed consent** *before* collection.[62] This is the only way to mitigate the existential litigation risk.
7. **On "Scope":**
   - Assume **B2B/Employee data is COVERED**. The CPRA model [49] is the only one that applies to this data, and its dominance makes it the *de facto* standard.
   - Assume **Nonprofit status is IRRELEVANT**. The trend in the 2025 laws (DE, NJ, MN, OR) [46] is the *erosion* of this exemption.
8. **On "Risk Mitigation":**
   - Assume the **"Right to Cure" is GONE.** In key markets, it has already *expired*.[6] A compliance program must now be built on *prevention*, not *reaction*.
   - Assume **Enforcers are Collaborating.** A violation in one state will be shared with the **AG Consortium** [90], multiplying the financial risk.

In conclusion, the U.S. privacy landscape of 2025 is fragmented but consolidating around high-risk, consumer-protective principles. The "warning" phase is over, and the "enforcement" phase—driven by active, collaborative regulators (CPPA, AGs) and aggressive plaintiff's attorneys (BIPA, MHMDA)—has begun. A "Highest Common Denominator" framework is the only legally and financially sound path forward.

Works cited

1. Data Privacy Laws: What You Need to Know in 2025 - Osano, accessed November 8, 2025, https://www.osano.com/articles/data-privacy-laws

2. 2025 State Privacy Laws: What Businesses Need to Know for Compliance, accessed November 8, 2025, https://www.whitecase.com/insight-alert/2025-state-privacy-laws-what-businesses-need-know-compliance
3. The Current State of U.S. Consumer Privacy Laws: An Early 2025 Update | TrustArc, accessed November 8, 2025, https://trustarc.com/resource/us-consumer-privacy-laws-2025-update/
4. Which States Have Consumer Data Privacy Laws? - Bloomberg Law, accessed November 8, 2025, https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/
5. The Complete Guide to US State Privacy Laws for Small Businesses (2025-2026), accessed November 8, 2025, https://cookie-script.com/privacy-laws/us-state-privacy-laws-for-small-businesses-2025-2026
6. U.S. Data Privacy Laws: A Guide to the 2025 Landscape | Osano, accessed November 8, 2025, https://www.osano.com/us-data-privacy-laws
7. State Privacy Law in 2025—What to Expect - California Lawyers Association, accessed November 8, 2025, https://calawyers.org/privacy-law/state-privacy-law-in-2025-what-to-expect/
8. CDPA, CCPA and CPRA : Key Difference & Similarities | Mandatly, accessed November 8, 2025, https://mandatly.com/ccpa-compliance/difference-between-virginia-cdpa-ccpa-and-cpra
9. Summary of the HIPAA Privacy Rule - HHS.gov, accessed November 8, 2025, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
10. Patient Rights Under HIPAA - Updated for 2025, accessed November 8, 2025, https://www.hipaajournal.com/hipaa-rights/
11. HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information - Federal Register, accessed November 8, 2025, https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
12. HIPAA Updates and HIPAA Changes in 2025, accessed November 8, 2025, https://www.hipaajournal.com/hipaa-updates-hipaa-changes/
13. Regulatory Initiatives - HHS.gov, accessed November 8, 2025, https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html
14. HIPAA Violation Fines - Updated for 2025, accessed November 8, 2025, https://www.hipaajournal.com/hipaa-violation-fines/
15. HIPAA violations & enforcement | American Medical Association, accessed November 8, 2025, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement
16. Resolution Agreements | HHS.gov, accessed November 8, 2025, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

17. HIPAA Violation Fines & Lawsuit Settlements Directory - Compliancy Group, accessed November 8, 2025, https://compliancy-group.com/hipaa-fines-directory-year/
18. U.S. Privacy Laws - Epic.org, accessed November 8, 2025, https://epic.org/issues/privacy-laws/united-states/
19. Children's Online Privacy Protection Rule ("COPPA") - Federal Trade Commission, accessed November 8, 2025, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
20. Amendments to the COPPA Rule Now in Effect Publications - Bass, Berry & Sims PLC, accessed November 8, 2025, https://www.bassberry.com/news/amendments-to-the-coppa-rule-now-in-effect/
21. Data protection laws in the United States, accessed November 8, 2025, https://www.dlapiperdataprotection.com/?c=US
22. Unpacking the FTC's COPPA Amendments: What You Need to Know | White & Case LLP, accessed November 8, 2025, https://www.whitecase.com/insight-alert/unpacking-ftcs-coppa-amendments-what-you-need-know
23. FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data, accessed November 8, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data
24. Sweeping Changes to Children's Privacy Law Will Affect Businesses | Paul Hastings LLP, accessed November 8, 2025, https://www.paulhastings.com/insights/ph-privacy/sweeping-changes-to-childrens-privacy-law-will-affect-businesses
25. FTC Updates to the COPPA Rule Impose New Compliance Obligations for Online Services That Collect Data from Children - Gibson Dunn, accessed November 8, 2025, https://www.gibsondunn.com/ftc-updates-to-coppa-rule-impose-new-compliance-obligations-for-online-services-that-collect-data-from-children/
26. Children's Online Privacy Protection Rule - Federal Register, accessed November 8, 2025, https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule
27. Kids' Privacy (COPPA) - Federal Trade Commission, accessed November 8, 2025, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa
28. What is GLBA Compliance? A Guide for Financial Institutions in 2025 - Isora GRC, accessed November 8, 2025, https://www.saltycloud.com/blog/what-is-glba/
29. Gramm-Leach-Bliley Act - Federal Trade Commission, accessed November 8, 2025, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
30. Privacy and Security | Federal Trade Commission, accessed November 8, 2025,

https://www.ftc.gov/business-guidance/privacy-security
31. Gramm Leach Bliley Act (Reg P) | American Bankers Association, accessed November 8, 2025, https://www.aba.com/banking-topics/compliance/acts/gramm-leach-bliley-act
32. FTC Finalizes New Notification Requirement for GLBA Safeguards Rule, accessed November 8, 2025, https://www.cov.com/en/news-and-insights/insights/2023/11/ftc-finalizes-new-notification-requirement-for-glba-safeguards-rule
33. CFPB Adjusts Various Penalty Amounts Based on Inflation | Consumer Finance Monitor, accessed November 8, 2025, https://www.consumerfinancemonitor.com/2025/01/08/cfpb-adjusts-various-penalty-amounts-based-on-inflation-2/
34. Civil Penalty Inflation Adjustments - Consumer Financial Protection Bureau, accessed November 8, 2025, https://www.consumerfinance.gov/rules-policy/final-rules/civil-penalty-inflation-annual-adjustments/
35. Fair Credit Reporting Act - Federal Trade Commission, accessed November 8, 2025, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act
36. Homebuyers Privacy Protection Act Amends FCRA - Hunton Andrews Kurth LLP, accessed November 8, 2025, https://www.hunton.com/privacy-and-information-security-law/homebuyers-privacy-protection-act-amends-fcra
37. A Summary of Your Rights Under the Fair Credit Reporting Act - files.consumerfinance.gov., accessed November 8, 2025, https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf
38. New Consumer Law Rights Taking Effect in 2025 | NCLC Digital Library, accessed November 8, 2025, https://library.nclc.org/article/new-consumer-law-rights-taking-effect-2025
39. Fair Credit Reporting Act; Preemption of State Laws - Federal Register, accessed November 8, 2025, https://www.federalregister.gov/documents/2025/10/28/2025-19671/fair-credit-reporting-act-preemption-of-state-laws
40. Brownstein Challenges Colorado Law Prohibiting Medical Debt Reporting, accessed November 8, 2025, https://www.bhfs.com/insight/brownstein-challenges-colorado-law-prohibiting-medical-debt-reporting/
41. Enforcement Actions - Consumer Financial Protection Bureau, accessed November 8, 2025, https://www.consumerfinance.gov/enforcement/actions/
42. What Just Happened at the FTC and CFPB: Wiley Consumer Protection Download (January 24, 2025), accessed November 8, 2025, https://www.wiley.law/newsletter-What-Just-Happened-at-the-FTC-and-CFPB-Wiley-Consumer-Protection-Download-January-24-2025
43. US State Comprehensive Privacy Laws Report - IAPP, accessed November 8, 2025, https://iapp.org/resources/article/us-state-privacy-laws-overview/

44. US State Privacy Legislation Tracker - IAPP, accessed November 8, 2025, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
45. 2025 State Privacy Law Tracker - Husch Blackwell, accessed November 8, 2025, https://www.huschblackwell.com/2025-state-privacy-law-tracker
46. Overview | U.S. State Privacy Laws - Lewis Rice, accessed November 8, 2025, https://www.lewisrice.com/u-s-state-privacy-laws/
47. The Growth of State Privacy Legislation - IAPP, accessed November 8, 2025, https://iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/
48. Virginia VCDPA vs California CPRA - TermsFeed, accessed November 8, 2025, https://www.termsfeed.com/blog/virginia-vcdpa-vs-california-cpra/
49. New Privacy Laws From Coast to Coast: Comparing California, Virginia and Colorado, accessed November 8, 2025, https://www.troutman.com/insights/new-privacy-laws-from-coast-to-coast-comparing-california-virginia-and-colorado/
50. The Always-Up-To-Date US State Privacy Law Comparison Chart ..., accessed November 8, 2025, https://sourcepoint.com/blog/us-state-privacy-laws-comparison-chart/
51. State Consumer Privacy Law Comparison Chart - Fisher Phillips, accessed November 8, 2025, https://www.fisherphillips.com/a/web/gzwry5pMdaaqJde9zr68H2/a66mrz/us-state-consumer-privacy-law_v2.pdf
52. New State Privacy Laws – Second Half of 2025 | ArentFox Schiff, accessed November 8, 2025, https://www.afslaw.com/perspectives/privacy-counsel/new-state-privacy-laws-second-half-2025
53. New Jersey Joins Data Privacy Party—New Jersey Data Protection Act Becomes Effective in January 2025 - Ogletree, accessed November 8, 2025, https://ogletree.com/insights-resources/blog-posts/new-jersey-joins-data-privacy-party-new-jersey-data-protection-act-becomes-effective-in-january-2025/
54. U.S. State Comprehensive Consumer Data Privacy Law Comparison, accessed November 8, 2025, https://www.foley.com/wp-content/uploads/2025/04/U.S.-State-Comprehensive-Consumer-Privacy-Law-Comparison-Chart_V10.pdf
55. Texas Data Privacy and Security Act - Texas State Law Library, accessed November 8, 2025, https://www.sll.texas.gov/spotlight/2024/07/texas-data-privacy-and-security-act/
56. 2025 State Privacy Laws Taking Effect: Key Compliance ..., accessed November 8, 2025, https://www.fisherphillips.com/en/news-insights/2025-state-privacy-laws-taking-effect.html
57. US Data Privacy Guide | White & Case LLP, accessed November 8, 2025, https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide
58. The State of State Privacy Laws: What Businesses Need to Know 2025 Edition - Miller Nash, accessed November 8, 2025,

https://www.millernash.com/firm-news/news/the-state-of-state-privacy-laws-what-businesses-need-to-know-2025-edition
59. New State Privacy Laws Take Effect in New Jersey and Delaware, accessed November 8, 2025, https://www.mcneeslaw.com/new-state-privacy-laws-new-jersey-delaware/
60. Biometric Information Privacy Act - Illinois General Assembly - -, accessed November 8, 2025, https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=5
61. Illinois Biometric Information Privacy Act (BIPA [Key Requirements] - Hyperproof, accessed November 8, 2025, https://hyperproof.io/illinois-biometric-privacy-information-act/
62. Biometric Information Privacy Act (BIPA) - ACLU of Illinois, accessed November 8, 2025, https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa
63. BIPA Update: Illinois Limits Liability and Clarifies Electronic Consent for Biometric Data Collection | Insights | Greenberg Traurig LLP, accessed November 8, 2025, https://www.gtlaw.com/en/insights/2024/8/bipa-update-illinois-limits-liability-and-clarifies-electronic-consent-for-biometric-data-collection
64. Protecting Washingtonians' Personal Health Data and Privacy | Washington State, accessed November 8, 2025, https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy
65. Washington's My Health, My Data Act - IAPP, accessed November 8, 2025, https://iapp.org/resources/article/washington-my-health-my-data-act-overview/
66. Closing the Privacy Gap: Understanding the Nuances and Heightened Risk of Washington's My Health My Data Act Publications, accessed November 8, 2025, https://www.bassberry.com/news/washington-my-health-my-data-act/
67. Washington's My Health My Data Act Comes Into Force – What You Need to Know, and Do | Insights & Resources | Goodwin, accessed November 8, 2025, https://www.goodwinlaw.com/en/insights/publications/2024/03/alerts-technology-hltc-my-health-my-data-act-mhmda
68. Chapter 19.373 RCW: WASHINGTON MY HEALTH MY DATA ACT - | WA.gov, accessed November 8, 2025, https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true
69. Data Broker Registries in the US 2025 - Monda, accessed November 8, 2025, https://www.monda.ai/blog/data-broker-registries-in-the-us
70. Why Are Hundreds of Data Brokers Not Registering with States?, accessed November 8, 2025, https://www.eff.org/deeplinks/2025/06/why-are-hundreds-data-brokers-not-registering-states
71. Texas and Oregon Adopt New Rules for Data Broker Laws - WilmerHale, accessed November 8, 2025, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20231214-texas-and-oregon-adopt-new-rules-for-data-broker-laws
72. Many data brokers are failing to register with state consumer protection

agencies, accessed November 8, 2025, https://www.malwarebytes.com/blog/news/2025/06/many-data-brokers-are-failing-to-register-with-state-consumer-protection-agencies
73. Texas Expands and Modifies Data Broker Registration Law - WilmerHale, accessed November 8, 2025, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250904-texas-expands-and-modifies-data-broker-registration-law
74. Texas Amends Data Broker Law Definition and Applicability Thresholds, accessed November 8, 2025, https://www.hunton.com/privacy-and-information-security-law/texas-amends-data-broker-law-definition-and-applicability-thresholds
75. California Expands Data Broker Registration Requirements - Hunton Andrews Kurth LLP, accessed November 8, 2025, https://www.hunton.com/privacy-and-information-security-law/california-expands-data-broker-registration-requirements
76. Information for Data Brokers - California Privacy Protection Agency (CPPA) - CA.gov, accessed November 8, 2025, https://cppa.ca.gov/data_brokers/
77. Law & Regulations - California Privacy Protection Agency (CPPA) - CA.gov, accessed November 8, 2025, https://cppa.ca.gov/regulations/
78. California's Latest Trio of Privacy Bills: What Businesses and Consumers Need to Know, accessed November 8, 2025, https://www.bytebacklaw.com/2025/10/californias-latest-trio-of-privacy-bills-what-businesses-and-consumers-need-to-know/
79. California Delete Act Enforcement Sweep [Alert] - Cozen O'Connor, accessed November 8, 2025, https://www.cozen.com/news-resources/publications/2025/california-delete-act-enforcement-sweep
80. Governor Signs Landmark Defending Californians' Data Act - Senator Josh Becker, accessed November 8, 2025, https://sd13.senate.ca.gov/news/press-release/october-9-2025/governor-signs-landmark-defending-californians-data-act
81. Consumer rights and compliance under Nevada privacy law - Cookiebot, accessed November 8, 2025, https://www.cookiebot.com/en/nevada-privacy-law/
82. Nevada Privacy Law in a Nutshell - CookieYes, accessed November 8, 2025, https://www.cookieyes.com/blog/nevada-privacy-law/
83. Nevada Privacy Law Compliance | Solutions - OneTrust, accessed November 8, 2025, https://www.onetrust.com/solutions/nevada-privacy-law-compliance/
84. Nevada | Jurisdictions - DataGuidance, accessed November 8, 2025, https://www.dataguidance.com/jurisdictions/nevada
85. Nevada's New Privacy Law: More Bark than Bite, accessed November 8, 2025, https://practicalprivacy.wyrick.com/blog/nevadas-new-privacy-law-more-bark-than-bite
86. Privacy and Security Enforcement | Federal Trade Commission, accessed November 8, 2025, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/p

rivacy-security-enforcement
87. 10 Key Privacy Developments and Trends to Watch in 2025 - Wiley Law, accessed November 8, 2025, https://www.wiley.law/alert-10-Key-Privacy-Developments-and-Trends-to-Watch-in-2025
88. 2025 Brought Us Eight US “Comprehensive” Privacy Laws, What's Next?, accessed November 8, 2025, https://www.eyeonprivacy.com/2025/10/2025-brought-us-eight-us-comprehensive-privacy-laws-whats-next/
89. State attorneys general stepping up privacy enforcement, watchdog finds, accessed November 8, 2025, https://therecord.media/state-ags-enforcement-privacy-law
90. The BR Privacy & Security Download: November 2025, accessed November 8, 2025, https://www.jdsupra.com/legalnews/the-br-privacy-security-download-2072781/
91. Latest News & Announcements - California Privacy Protection Agency (CPPA) - CA.gov, accessed November 8, 2025, https://cppa.ca.gov/announcements/
92. Settlement Against Illuminate Education Highlights Expanding Enforcement of Student Data Privacy Laws (via Passle), accessed November 8, 2025, https://technologylaw.fkks.com/post/102ltvl/settlement-against-illuminate-education-highlights-expanding-enforcement-of-stude
93. Attorney General Bonta Joins States in Securing $5.1 Million in Settlements from Education Software Company for Failing to Protect Students’ Data, accessed November 8, 2025, https://oag.ca.gov/news/press-releases/attorney-general-bonta-joins-states-securing-51-million-settlements-education
94. California Consumer Privacy Act (CCPA), accessed November 8, 2025, https://www.insideprivacy.com/category/ccpa/
95. California Privacy Protection Agency Intensifies Enforcement: Recent Enforcement Actions and Trends | Insights | Mayer Brown, accessed November 8, 2025, https://www.mayerbrown.com/en/insights/publications/2025/05/california-privacy-protection-agency-intensifies-enforcement-recent-enforcement-actions-and-trends
96. Washington Data Broker Agrees to Pay Fine for Failing to Register, accessed November 8, 2025, https://cppa.ca.gov/announcements/2025/20250729.html
97. CPPA Brings Enforcement Action Against Florida Data Broker, accessed November 8, 2025, https://cppa.ca.gov/announcements/2025/20250220.html
98. California Privacy Protection Agency Announces 2025 Increases for CCPA Fines and Penalties, accessed November 8, 2025, https://cppa.ca.gov/announcements/2024/20241217.html
99. 2025 Mid-Year Review: US State Comprehensive Data Privacy Law Updates (Part 1), accessed November 8, 2025, https://www.mayerbrown.com/en/insights/publications/2025/09/2025-mid-year-review-us-state-comprehensive-data-privacy-law-updates-part-1

100. Privacy Protections for Children's Online Data | Colorado General Assembly, accessed November 8, 2025, https://leg.colorado.gov/bills/sb24-041
101. Colorado AG Proposes Updates to Colorado Privacy Act Rules to Address Minors' Online Safety | Davis Wright Tremaine, accessed November 8, 2025, https://www.dwt.com/blogs/privacy--security-law-blog/2025/08/colorado-privacy-act-rule-updates-minors
102. Colorado Finalizes Privacy Act Rules: Key Updates for Businesses - Data Matters, accessed November 8, 2025, https://datamatters.sidley.com/2025/01/09/colorado-finalizes-privacy-act-rules-key-updates-for-businesses/
103. New Colorado Privacy Act Rules Adopted | Byte Back, accessed November 8, 2025, https://www.bytebacklaw.com/2024/12/new-colorado-privacy-act-rules-adopted/
104. Oregon's Privacy Law Update Adds to Patchwork Approach to Minors and Location Data, accessed November 8, 2025, https://www.eyeonprivacy.com/2025/07/oregons-privacy-law-update-adds-to-patchwork-approach-to-minors-and-location-data/
105. Oregon Amends Consumer Privacy Act - Hunton Andrews Kurth LLP, accessed November 8, 2025, https://www.hunton.com/privacy-and-information-security-law/oregon-amends-consumer-privacy-act