ObservePoint

The 5 Core Privacy Principles:

Preparing for Every State Law

How a Principle-Based Privacy Program Scales Across the U.S.

INTRODUCTION:

A Shifting Privacy Landscape

Across the United States, data privacy laws are advancing rapidly. California led the way with the **California Consumer Privacy Act (CCPA/CPRA)**, and now states like Colorado, Connecticut, Virginia, Texas, and Utah have followed suit.

Each law uses slightly different language, timelines, and requirements, which can make compliance feel like a moving target. For example, California requires a “Do Not Sell or Share” link and mandates businesses honor Global Privacy Control browser signals. Texas, with its well-staffed Consumer Protection Division and a slew of laws it can enforce, has already settled a billion-dollar case with Google over biometric data collection. Utah, meanwhile, provides a framework of 23 privacy practices and a maturity model for building long-term accountability.

This patchwork can feel overwhelming. The challenge for organizations is clear: **how do you comply across multiple states without chasing 50 different checklists?**

The answer is not memorizing every state’s law but building a **principle-based privacy program**. When programs are designed around a set of shared privacy principles, they scale naturally across jurisdictions, reduce compliance risk, and demonstrate accountability everywhere.

The 5 Core Privacy Principles

Looking across state laws, five principles consistently emerge. Together, they form the foundation of a privacy program that works nationwide:

Transparency
People deserve to know what data you collect and why.

Consent & Choice
Individuals should have control over how their data is used and shared.

Data Access & Control
Everyone should be able to access, correct, or delete their personal information.

Data Minimization & Retention
Collect only what you need and keep it only as long as necessary.

Accountability & Governance
Assign responsibility, monitor compliance, and prove your policies are being followed.

States may phrase them differently, but the principles remain the same.

Mapping Practices to the Core Principles and Case Studies

To illustrate how a principle-based privacy program functions in practice, this analysis focuses on **California, Colorado, Texas, and Utah.** These states represent four distinct yet complementary approaches to privacy regulation: California's rights-driven enforcement model, Colorado's GDPR-inspired balance, Texas's emerging enforcement momentum, and Utah's accountability-based framework. Together, they capture the full spectrum of how state privacy laws define, operationalize, and measure responsible data practices.

In addition, consider five real enforcement stories from across the United States. Each illustrates what happens when organizations fall short and why building programs around principles is the safer path forward.

1 Transparency

Across all state frameworks, transparency starts with what organizations tell people and whether those statements reflect reality.

This covers things like:

- Privacy policies
- Cookie categories
- Do not sell/share notices

And here's how our example states approach this:

- **Utah** emphasizes clear communication about what data is collected, how it is used, and who it is shared with.

- **California** requires consumer-facing privacy notices, "Do Not Sell or Share" links, and recognition of Global Privacy Control (GPC) browser signals.

- **Colorado** mandates detailed privacy notices listing categories of personal data and processing purposes.

- **Texas** requires businesses to provide clear, accessible explanations of the types of data collected and their intended use.

Common thread: Transparency is the foundation of lawful data use. Every state expects disclosures to match actual practices, not just policy statements.

Transparency Fail: DoorDash - California

Issue: DoorDash shared customer data through marketing cooperatives without clear disclosure or a meaningful opt-out.

Law Violated: California Consumer Privacy Act (CCPA); California Online Privacy Protection Act (CalOPPA).

Outcome: $375K Settlement with the California Attorney General; required updated privacy notices, opt-out functionality, and auditing.

Lesson: Transparency failures, especially around "selling" or "sharing" data, can be as costly as outright breaches.

2 Consent & Choice

The principle of Consent & Choice ensures individuals can meaningfully decide how their personal information is collected and used.

This covers things that happen before data collection, such as:

- Cookie banners
- GPC-enablement
- Opt-out mechanisms

How the states address:

- **Utah** integrates consent and user preference management into its broader accountability framework.

- **California** allows consumers to opt out of the sale or sharing of their data and requires opt-in consent for minors.

- **Colorado** establishes a universal opt-out mechanism and requires opt-in consent for sensitive data.

- **Texas** mandates opt-in consent for sensitive information and opt-outs for targeted advertising and sales.

Common thread: Consent must be clear, informed, and traceable, not hidden, achieved through manipulation, or assumed through silence.

Consent & Choice Fail: Allstate/Arity SDKs - Texas

Issue: Arity, an Allstate subsidiary, allegedly collected and sold sensitive geolocation and driving data via third-party SDKs without obtaining valid consent.

Law Violated: Texas Data Privacy and Security Act (TDPSA); Texas Deceptive Trade Practices Act.

Outcome: First enforcement action under the TDPSA (filed January 2025). The AG seeks civil penalties, data deletion, and restitution.

Lesson: Consent can't be buried in technical integrations; businesses are accountable for partners' data collection practices.

3 Data Access & Control

Data Access & Control gives individuals authority over their data once it is collected, so they can access, correct, or delete it.

It covers things like:

- Mechanisms to access, correct or delete
- Explanations of data processing

How the states address:

- **Utah** encourages organizations to build processes for responding to data access, correction, and deletion requests, ensuring transparency about how personal information is processed.

- **California** guarantees rights to know, delete, and correct data through accessible request mechanisms.

- **Colorado** mirrors these rights and includes a formal appeals process for denied requests.

- **Texas** provides similar access, correction, and deletion rights with specific timelines for response.

Common thread: Every state recognizes that user control does not end at consent; it extends through the entire data lifecycle.

Data Access & Control Fail: TicketNetwork - Connecticut

Issue: TicketNetwork failed to implement clear mechanisms for consumers to access or delete personal data and misrepresented compliance in its privacy notice.

Law Violated: Connecticut Data Privacy Act (CTDPA).

Outcome: $85,000 settlement, the first CTDPA enforcement action (July 2025). The company must update disclosures, submit compliance reports, and maintain a record of consumer requests.

Lesson: Users' ability to view, correct, and delete data is a legal requirement, not a User Experience (UX) enhancement.

4 Data Minimization & Retention

The Data Minimization & Retention principle limits collection to what is necessary and requires organizations to dispose of data responsibly.

This covers things like:

- Retention & disposal schedules
- Data classification & inventory

How the states address:

- **Utah** focuses on collecting only what is needed, maintaining clear retention schedules, and securely disposing of personal data.
- **California** requires businesses to disclose how long they keep each category of data and prohibits indefinite storage without purpose.
- **Colorado** restricts processing to what is adequate, relevant, and limited to legitimate purposes.
- **Texas** requires that data collection be "reasonably necessary and proportionate" to the stated purpose.

Common thread: Minimization and timely deletion are now enforceable obligations. Regulators increasingly treat over-collection and indefinite retention as privacy risks in themselves.

Data Minimization & Retention Fail: Blackbaud - Federal

Issue: Blackbaud, a cloud software provider for nonprofits and educational institutions, retained vast amounts of personal and donor data well beyond its business needs and failed to follow its own data-retention policies. When a 2020 ransomware attack struck, the excess data amplified the breach's impact and exposed millions of outdated records.

Law Violated: Section 5 of the Federal Trade Commission Act (unfair or deceptive practices). The FTC found that Blackbaud's unreasonable data retention and misrepresentations about deletion and security practices violated federal law.

Outcome: In May 2024, the FTC finalized a consent order requiring Blackbaud to:

- Delete personal data it no longer needs.
- Create and maintain a written data-retention schedule specifying purposes and deletion timelines.
- Strengthen security and governance controls to enforce data minimization.
- Stop misrepresenting its privacy, security, and data-deletion practices.

Lesson: Holding on to personal data "just in case" is no longer acceptable. The FTC now treats over-retention as a standalone privacy violation. Data minimization and deletion are enforceable compliance expectations, not optional best practices.

5 Accountability & Governance

Accountability & Governance turn privacy commitments into measurable practice.

This covers things like:

- Assigning leaders & accountability
- Training & awareness for employees
- Reporting & audits
- Incident breach responses

How the states address:

- **Utah's framework** centers on leadership, training, and oversight, ensuring agencies can demonstrate compliance through documentation and regular reporting.

- **California** emphasizes risk assessments, audits, and enforcement through the California Privacy Protection Agency.

- **Colorado** requires Data Protection Impact Assessments and assigns clear responsibility for data-protection oversight.

- **Texas** calls for designating a privacy lead, maintaining documentation of assessments, and ensuring continuous monitoring.

Common thread: Each state expects organizations to prove that privacy is managed, not just promised. Accountability is demonstrated through leadership, documentation, and verifiable action.

Accountability & Governance Fail: Meta - Texas

Issue: Meta's facial recognition features allegedly captured and stored Texans' biometric identifiers without proper consent or deletion.

Law Violated: Texas Capture or Use of Biometric Identifier Act (CUBIA); Texas Deceptive Trade Practices Act.

Outcome: $1.4 billion settlement (July 2024), the largest privacy settlement in Texas history. Meta must discontinue certain biometric features and strengthen governance programs.

Lesson: Governance failures, especially around sensitive data, can produce billion-dollar liabilities. Strong leadership and oversight are non-negotiable.

Building a Principle-Based Privacy Program

Implementing the five core principles requires both policy and proof:

Proof
means showing that these policies are actually working on your site or in your systems.

Policy
means writing clear notices, assigning roles, and publishing rights processes.

This is where **Consent Management Platforms (CMPs)** and auditing tools like **ObservePoint** play a critical role:

They **enforce transparency** by showing what tags and trackers are actually running.

They **capture and store consent signals** and ensure they flow downstream.

They **link rights requests** with actual consent and processing records.

They **flag unnecessary data collection** or hidden trackers.

They **provide audit-ready reports** that demonstrate oversight and accountability.

With CMPs and monitoring in place, organizations can operationalize the five principles consistently across all states, reducing compliance drift and building trust with consumers.

CONCLUSION:

From Principles to Practice

The wave of state privacy laws is not slowing down. If anything, it's accelerating. Organizations that focus on principles, not checklists will:

- Build programs that scale across states.
- Stay ahead of evolving laws without constant rework.
- Demonstrate compliance with evidence, not just policies.
- Strengthen trust with consumers by aligning promises with practice.

Privacy compliance is no longer just about avoiding fines. It's about closing the gap between **intention and execution** and proving to customers and regulators alike that you are worthy of their trust.

Sources

P. 5 — Transparency

California Attorney General Press Release
https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-doordash-investigation-finds-company

White & Case Analysis
https://www.whitecase.com/insight-alert/ccpa-settlement-illustrates-continued-focus-sale-consumer-personal-information

Arnold & Porter Summary
https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2024/04/doordash-ccpa-settlement

P. 6 — Consent & Choice

Texas Attorney General Complaint
https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45

Vinson & Elkins Summary
https://www.velaw.com/insights/texas-ag-targets-allstate-in-first-enforcement-of-texas-data-privacy-and-security-act/

WilmerHale Commentary
https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250121-texas-ag-brings-first-ever-lawsuit-under-a-state-comprehensive-privacy-law

P. 7 — Data Access & Control

Connecticut Attorney General Press Release
https://portal.ct.gov/ag/press-releases/2025-press-releases/attorney-general-tong-announces-settlement-with-ticketnetwork

National Law Review Summary
https://natlawreview.com/article/connecticuts-recent-privacy-settlement-shows-organizations-should-remain-cognizant

JD Supra Commentary
https://www.jdsupra.com/legalnews/connecticut-finalizes-first-ctdpa-7688507/

P. 8 — Data Minimization & Retention

FTC Press Release
https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-blackbaud-related-allegations-firms-security-failures-led-data-breach

FTC Case Library
https://www.ftc.gov/legal-library/browse/cases-proceedings/2023181-blackbaud-inc

Perkins Cole
https://perkinscoie.com/insights/update/ftc-brings-first-standalone-section-5-unfairness-claims-unreasonable-data-retention

HIPAA Journal
https://www.hipaajournal.com/ftc-finalizes-blackbaud-settlement/

P. 9 — Accountability & Governance

Texas Attorney General Press Release
https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture

Courthouse News Report
https://www.courthousenews.com/meta-settles-texas-biometric-privacy-lawsuit-for-1-4-billion/

Texas Standard Coverage
https://www.texasstandard.org/stories/meta-settlement-texas-privacy-laws/