

Comprehensive privacy laws are broadly applicable, technology-neutral rules that establish baseline rights and responsibilities for the collection, use, and sharing of personal data throughout the economy. Because of their broad reach, these laws can fill regulatory gaps left by narrower frameworks such as HIPAA that do not apply to the consumer context. Additional sector-specific protections—for artificial intelligence, biometrics, consumer health, data brokers, location data, or youth online safety—can then build on that common foundation. For an overview of the state comprehensive privacy law landscape, see FPF’s 2025 report, [Anatomy of a State Comprehensive Privacy Law: Charting the Legislative Landscape](#).

ELEMENTS OF A COMPREHENSIVE LAW

Economy-Wide Coverage

- Primarily regulates **controllers** (entities making decisions about how and why to process personal data)
- Additional obligations for **processors** (entities handling personal data under a controller’s instructions)
- Carve-outs for entities or data subject to existing regulation (e.g., HIPAA, GLBA) and small businesses

Common Business Obligations

- Transparency, data minimization, purpose limitation, data security, processor contracts, and risk assessments
- These obligations govern the data lifecycle

Individual Data Rights

- Access, correction, portability, and deletion rights give individuals baseline control over personal data
- Opt-out rights address targeted advertising, sale of personal data, and profiling for significant decisions
- Opt-in protection for processing sensitive data
- Many states require controllers to recognize **opt-out preference signals**, allowing consumers to exercise opt-out rights on a default basis

PRIVACY AS A FOUNDATION

Sectoral Laws Can Target Heightened Risks and Close Regulatory Gaps

- A broadly applicable, technology-neutral, broadly applicable privacy law leaves fewer gaps as technology evolves
- States have shown a willingness to iterate and amend their laws based on enforcement outcomes and legislative activity in other states.
- States are already layering additional protections for health data, teenagers, biometrics, location, and automated decisionmaking onto comprehensive privacy frameworks.
- Targeted rules can address risks that require specific duties, restrictions, or rights, while building from an existing compliance framework

Current Legislative Trends

- Laws broadening their reach—lower thresholds and fewer entity-level exemptions
- Expanding definition of sensitive data
- Data minimization requirements putting substantive limits on data collection and use
- Heightened protections for minors’ data, precise geolocation, biometrics, and consumer health data
- New rights to know third-party recipients of your personal data and to contest adverse profiling decisions

CURRENT LAWS (BY YEAR)

2018 California
2021 Colorado, Virginia
2022 Connecticut, Utah
2023 Delaware, Indiana, Iowa, Florida*, Montana, Oregon, Tennessee, Texas
2024 Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, Rhode Island
2026 Alabama, Louisiana, Oklahoma, Vermont