Clark Hill

How State Privacy Laws and AI Are Reshaping Consumer Data Protection

Melissa K. Ventrone, Member
+1 312.360.2506
mventrone@clarkhill.com

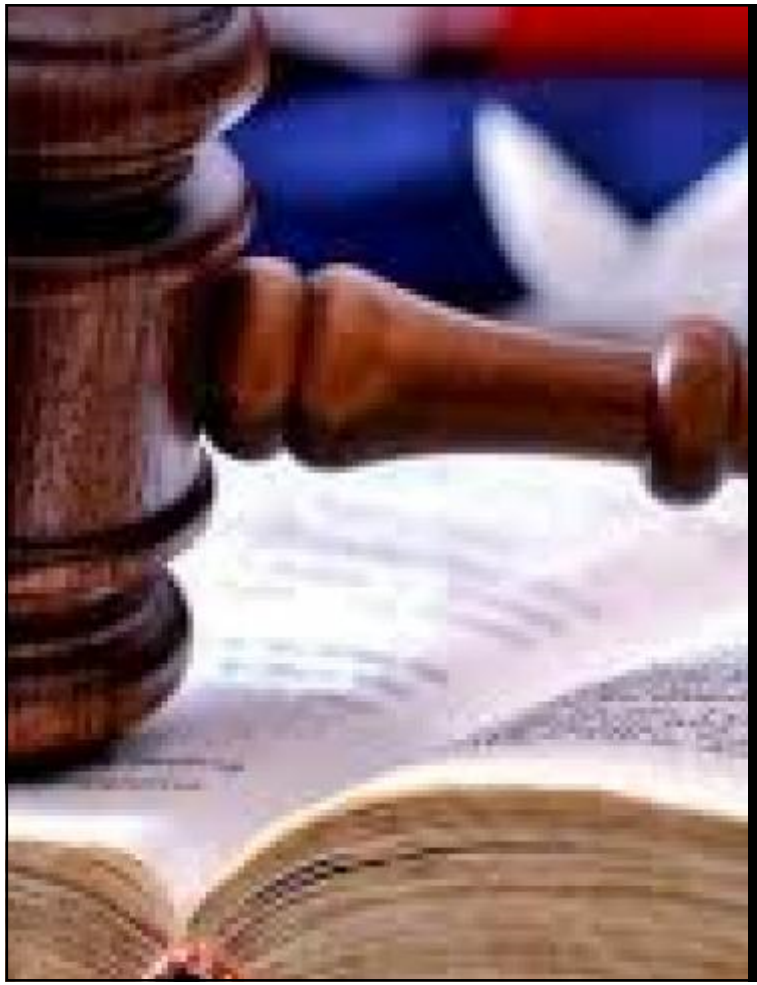
John F Howard, Senior Attorney
+1 480.684.1133
jfhoward@clarkhill.com

January 2026

1

Agenda:

1. Current Patchwork of Privacy Laws
2. Key Features of State Privacy Laws
3. AI Laws
4. Cybersecurity Risk Assessments / Data Protection Assessments
5. Compliance Challenges and Strategies



Federal Laws

No Comprehensive Federal Approach – Remains Industry Specific

Industry Specific Laws:

- GLBA, FTC, HIPAA, FCRA, COPPA, FERPA, SEC Safeguards Rule, etc..
- Critical Infrastructure Act reporting requirements
- US Int'l Trade Association's global cross-border privacy rules (CBPR)

Reduction in Federal Enforcement Activity – Shifting more responsibility to State Agencies

State Data Privacy Laws: Continued Expansion

19 states have comprehensive data privacy laws, covering roughly ½ of the US in 2026.

States with active laws:

- **California**
- **Colorado**
- **Connecticut**
- **Delaware**
- **Indiana**
- **Iowa**
- **Kentucky**
- **Maryland**
- **Minnesota**
- **Nebraska**
- **New Hampshire**
- **New Jersey**
- **Oregon**
- **Rhode Island**
- **Tennessee**
- **Texas**
- **Utah**
- **Virginia**

State Data Privacy Laws: More to Come

Laws new in 2026:

- **Indiana Consumer Data Privacy Act** (January 1, 2026)
- **Kentucky Consumer Data Protection Act** (January 1, 2026)
- **Rhode Island Data Transparency and Privacy Protection Act** (January 1, 2026)
- **Texas Responsible Artificial Intelligence Governance Act** (January 1, 2026)
- **Vermont Age-Appropriate Design Code Act** (January 1, 2027) – AG's rule making authority already in effect

California Delete Request and Opt-Out Platform (DROP)

- DROP went live in January 2026 – Mandated in the Delete Act (2023)
- Enforcement begins on August 1, 2026
- Data Brokers are required respond to DROP requests within 45 days
- Over 150,000 requests already received since January 1, 2026
- Only available to CA residents

Key Features of State Data Protection Laws

Common Features Shared Across State Laws:

- Required safeguards to protect consumer data
- Required contractual measures to obtain assurances from sub-processors / third parties
- Opt-in/Opt-out Consent: Clear consumer consent for data collection
- Transparency: Requirements to disclose how data is collected, used, and shared
- Stronger Consumer Rights: Data access, deletion, and correction rights
- Breach notification requirements

Key Differences:

- Private right of action
- Thresholds for applicability

State Interest in Privacy Enforcement

Consortium of Privacy Regulators

Attorneys general in California, Colorado, Connecticut, Delaware, Indiana, New Jersey and Oregon as well as the California Privacy Protection Agency have created the bipartisan Consortium of Privacy Regulators to collaborate on enforcing their respective state pr

- Minnesota and New Hampshire joined end of 2025
- Includes both Democratic and Republican-led states[iv]
- Key focus is to streamline enforcement of privacy protections across states.

8

Federal & State Regulators Target AI

State Level AI task forces: Monitor AI in multiple industries and recommend laws and regulations

Federal Push to promote and control AI innovation

- Federal agencies looking to pre-empt all AI state laws to try and control national approach

What is AI

Many forms (machine learning, deep neural networks, natural language processing, etc..) that rely on two basic types.

Generative (Dynamic) AI:

- A type of artificial intelligence technology that can produce various types of content, including text, imagery, audio and synthetic data.
- Generative AI learns the patterns and structure of its training data and generates content with similar characteristics

Analytical (Static) AI:

- Traditional AI" that focuses on analyzing existing data that can be used for predictions and automation

Artificial General Intelligence (AGI)/Artificial Super Intelligence (ASI):

- General intelligence models that are able to learn and mimic basic human thinking (AGI) or aspire to surpass the capabilities of humans (ASI).

State AI Laws

States have enacted laws to regulate the use of AI in, including criminal and civil laws

Laws target transparency, bias, and consumer protection

Types of requirements:

1. Notice provided to individuals of the use of AI (transparency/disclosure);
1. Testing and monitoring to ensure outputs remain as expected;
2. Cybersecurity Risk Assessment / Data Protection Assessments;

Types of AI Uses:

1. Chatbots;
2. Automated Decision Making Tools;
3. High-stakes processing

Intersection of Privacy Laws and AI Regulations

Privacy Laws Often Regulate AI-Driven Processing

- Right to opt-out of profiling and automated decisions driven by personal data
- Transparency and notice requirements
- Data minimization and consent for Sensitive data

AI-Specific Laws with Privacy Elements

- Colorado AI Act
- California AI Transparency Act
- California Transparency in Frontier Artificial Intelligence

Data Protection Impact Assessment vs Cybersecurity Risk Assessment/Data Protection Assessments

DPIA:

1. Mandatory under laws such as GDPR
2. Structured risk assessment to identify, analyze, and minimize risks to individual's privacy when handling personal data

CRA :

1. Mandatory under CCPA, NYDFS Cyber Regs, CO Privacy Act, VA Consumer Data Protection Act, and others
2. Structured risk assessment to identify, analyze, and minimize threats and vulnerabilities to digital assets, IT infrastructure, and sensitive data (PI).

Both are required when assessing new technology, such as AI, and high-risk processing – ongoing requirement

What Triggers a Cyber Risk Assessment

- Selling or Sharing Personal Information
- Processing Sensitive Data
- Definitions can vary by jurisdiction or industry
- SSN, race, financial account information (w/ access), medical information, biometric information, sexual orientation, genetic information, etc…
- Using Automated Decision-Making Technology (ADMT)/AI
  - Used to make significant decision, or
  - Poses a significant risk to an individual

14

Risk Assessment Required Components

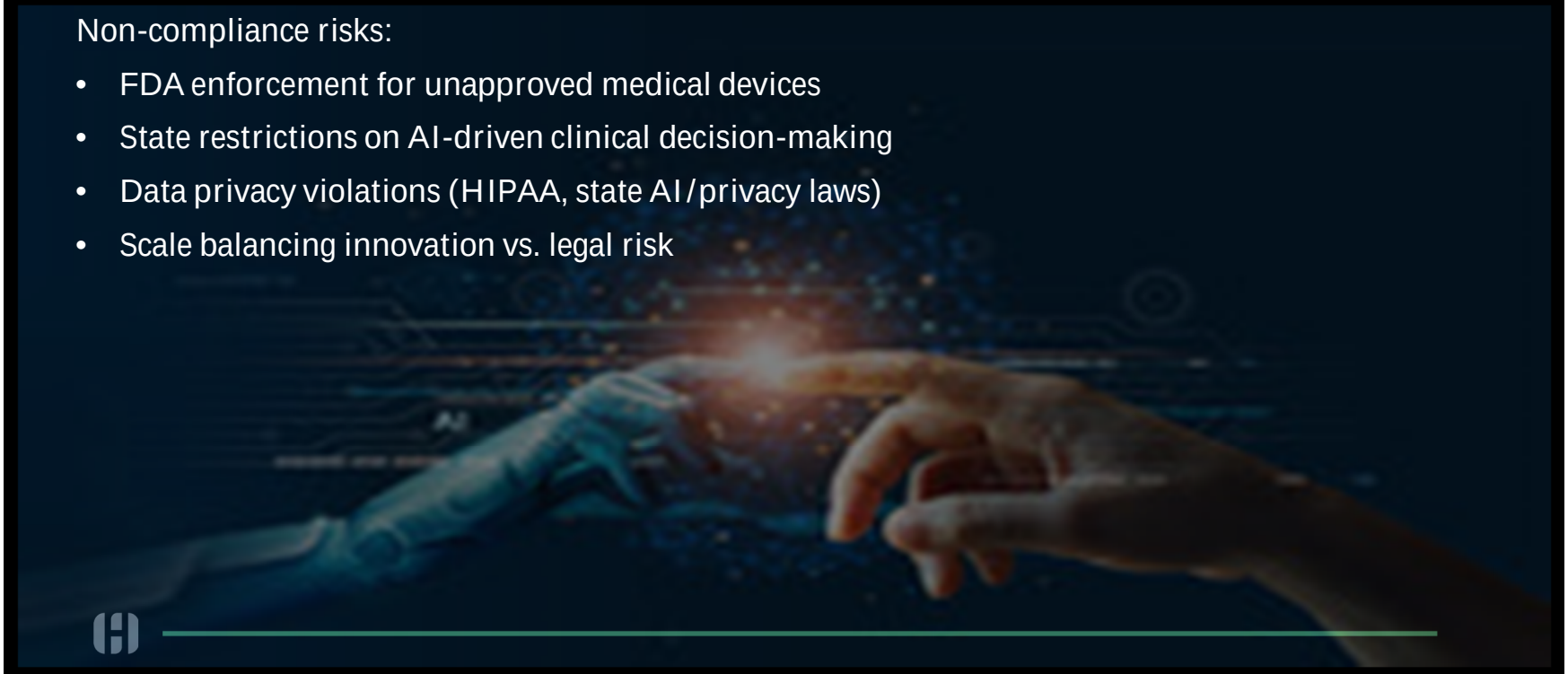
Risk Assessments must assess an organization's establishment, implementation, and maintenance of its cybersecurity program, including:

- Authentication mechanisms (provision, revocation, & maintenance)
- Data protection / encryption
- Account management / access controls (privileged account management)
- Asset inventories
- Data inventories / mapping
- Secure configurations (hardware/software)
- Vulnerability scans, penetration testing, independent audits
- Segmentation
- Anti-virus
- Logging / Monitoring
- Oversight / Governance
- Vendor management
- Incident response and disaster recovery

Why AI Compliance Matters

Non-compliance risks:

- FDA enforcement for unapproved medical devices
- State restrictions on AI-driven clinical decision-making
- Data privacy violations (HIPAA, state AI/privacy laws)
- Scale balancing innovation vs. legal risk



Perceived Risks Associated With AI Use

- Discrimination, prejudice, or favoritism
- Use of inaccurate or biased data models
- Over reliance
- Changes over time (Generative AI)

Benefits... more opportunity for efficiency gains and better heath outcomes

17

Potential Legal Risks

- Over reliance on AI determinations / outputs
- Discrimination / Discriminatory Practices (potential for bias in the AI models)

  Alignment Problem by Brian Christian
- Privacy (unauthorized uses or disclosures of health information)
- Cybersecurity (violation of State and Federal law or stated protections [privacy policy])

Enforcement Trends: What Regulators Are Watching

- California AG and CPPA targeting improper “sale” or “sharing” of personal information
- Pixel tracking lawsuits expanding from retail into other industries
- Class actions
- Delete Act and new DROP requirements
- State level privacy groups are urging enforcement of privacy laws

19

Emerging Issues

1. AI: States increasingly regulate AI tools
   - Texas Responsible AI Governance Act into Law
   - Illinois requires notice and consent if using AI in interviews
2. Sector specific: health data (New York and New Mexico Legislation)
3. Cyber incident reporting; Newly adopted UN Convention against cyber crime
4. Growing awareness of risks posed by location data and tracking
5. Growing number of statutes that regulate monitoring employees in the workplace

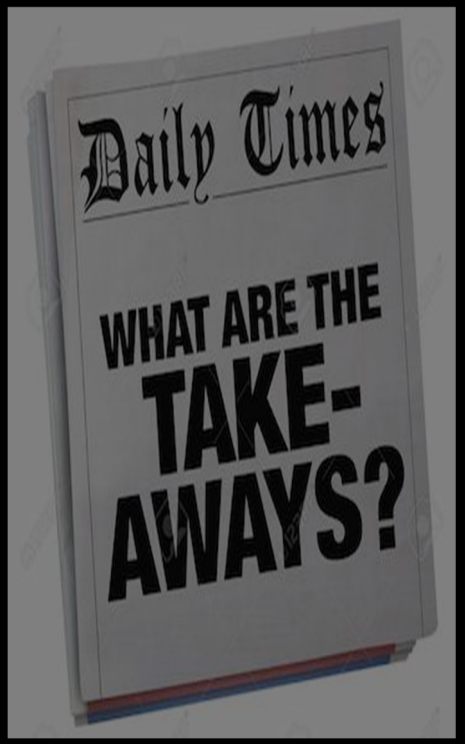
Compliance Challenges

- Overlap and divergence between State and Federal laws
- Growing complexity for companies to comply with varying state laws
- Tracking regulatory updates across jurisdictions
- Managing consumer rights workflows
- Aligning data governance with business workflows
- Balancing tech innovation with legal risk

Proactive Compliance Strategies

- Conduct state-specific data mapping and gap assessments
- Update privacy notices and consent mechanisms
- Implement role-based access and data minimization practices
- Train staff on multi-jurisdictional obligations
- Prepare for consumer requests (access, deletion, opt-out)
- Limit data retention where able
- Complete cybersecurity assessments

22



Final Takeaways

- State laws are reshaping the data privacy and cybersecurity landscape
- Entities in all industries are falling into scope
- Websites and online privacy policies provide information about Company's privacy activities
- Compliance requires agility, coordination, and education
- Entities need to be pro-active and take action now to avoid enforcement risk and preserve trust

Questions?

Thank You

Legal Disclaimer
The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill

25