Contact Center Compliance
DNC.com

The Enforcement Era: Staying Ahead in a Time of Privacy Crackdowns

Aaron Parry, Mac Murray & Shuster

12/8-9/2025

Phone
614-935-9955

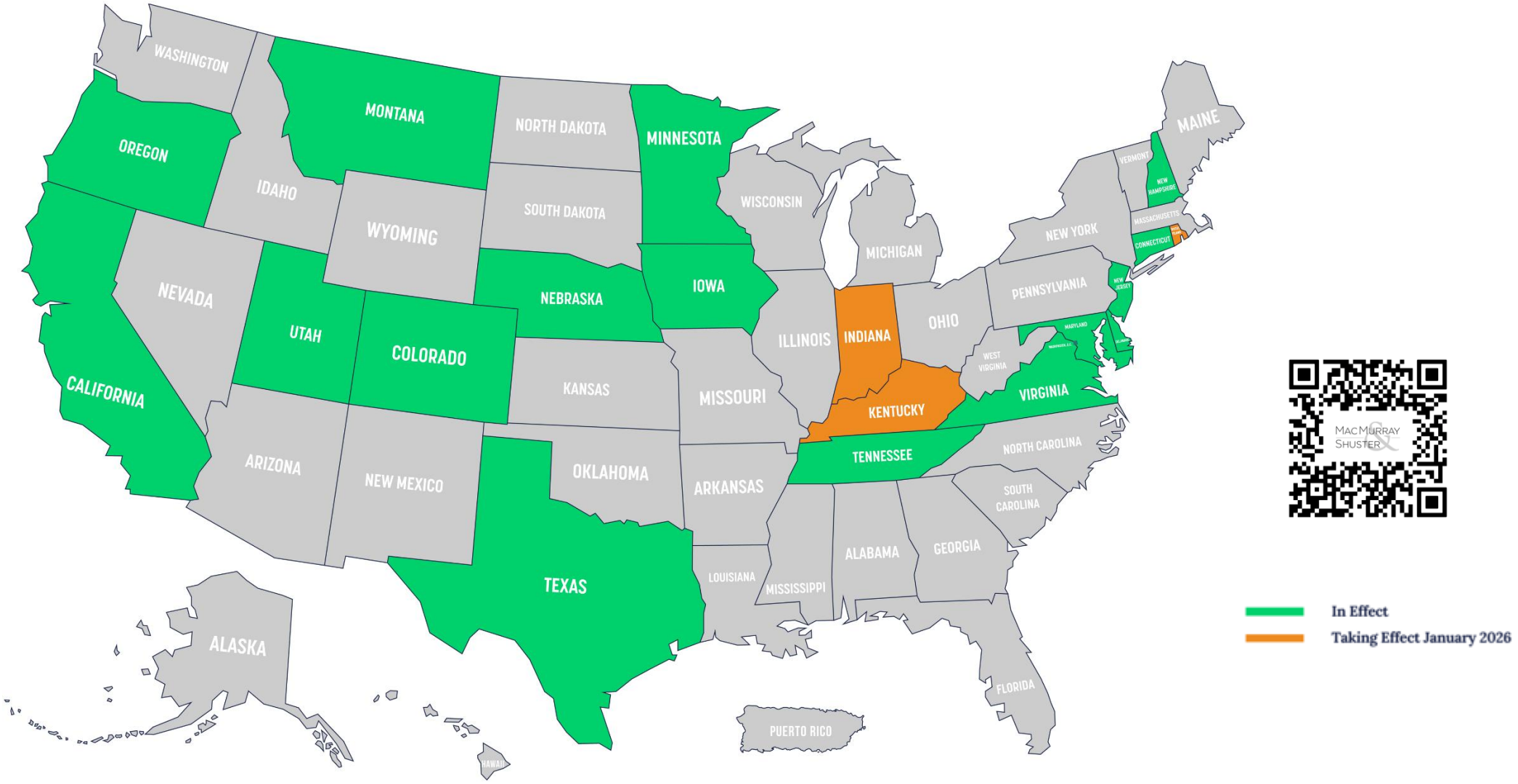
Email Address
aparry@mslawgroup.com

Website
www.mslawgroup.com

Disclaimer

The materials in this presentation are provided for informational purposes only and do not constitute legal advice. Transmission of the information is not intended to create, and the receipt thereof does not constitute, an attorney-client relationship. Every situation is different, and you should not act or rely on any information contained in this presentation without first seeking the advice of an attorney.

State Privacy Laws



Is My Company a Controller Under U.S. Privacy Laws?

Mac Murray & Shuster	Effective Date	Monetary Threshold	Consumer PI Control/ Process Threshold	Revenue + Sell/Share Threshold
California	1/1/2023	≥ $26.625M	≥ 100,000 consumers	≥ 50% of annual revenue from selling or sharing PI
Virginia	1/1/2023	None	≥ 100,000 consumers	> 50% of gross revenue selling PI + control or process PI of ≥ 25,000 consumers
Colorado	7/1/2023	None	≥ 100,000 consumers	Derives revenue or receives discount from selling PI + process or control PI of ≥ 25,000 consumers
Connecticut	7/1/2023	None	≥ 100,000 consumers	> 25% of gross revenue from selling PI + control or process PI of ≥ 25,000 consumers
Utah	12/31/2023	≥ $25M + another threshold	≥ 100,000 consumers	> 50% of gross revenue selling PI + control or process PI of ≥ 25,000 consumers
Oregon	7/1/2024	None	≥ 100,000 consumers	> 25% of gross revenue selling PI + control or process PI of ≥ 25,000 consumers
Texas*	7/1/2024	None	None	None
Montana	10/1/2024	None	≥ 25,000 consumers	> 25% of gross revenue selling PI + control or process PI of ≥ 15,000 consumers
Delaware	1/1/2025	None	≥ 35,000 consumers	> 20% of gross revenue selling PI + control or process PI of ≥ 25,000 consumers
Iowa	1/1/2025	None	≥ 100,000 consumers	> 50% of gross revenue selling PI + control or process PI of ≥ 25,000 consumers
Nebraska*	1/1/2025	None	None	None
New Hampshire	1/1/2025	N/A	≥ 35,000 consumers (controls or processes)	Derives > 25% of gross revenue from sale of PI + controls or processes PI of ≥ 10,000 consumers
New Jersey	1/15/2025	N/A	≥ 100,000 consumers (controls or processes)	Derives revenue or receives a discount on the price of any goods or services from sale of PI + controls or processes PI of ≥ 25,000 consumers
Tennessee	7/1/2025	≥ $25M + another threshold	≥ 175,000 consumers (controls or processes)	Derives > 50% of gross revenue from sale of PI + controls or processes PI of ≥ 25,000 consumers
Minnesota	7/31/2025	N/A	≥ 100,000 consumers (controls or processes)	Derives ≥ 25% of gross revenue from sale of PI + controls or processes PI of ≥ 25,000 consumers
Maryland	10/1/2025	N/A	≥ 35,000 consumers (controls or processes)	Derives > 20% of gross revenue from sale of PI + controls or processes PI of ≥ 10,000 consumers
Indiana	1/1/2026	None	≥ 100,000 consumers	> 50% of gross revenue selling PI + control or process PI of ≥ 25,000 consumers
Kentucky	1/1/2026	N/A	≥ 100,000 consumers (controls or processes)	Derives > 50% of gross revenue from sale of PI + controls or processes PI of ≥ 25,000 consumers
Rhode Island	1/1/2026	N/A	≥ 35,000 consumers (controls or processes)	Derives > 20% of gross revenue from sale of PI + controls or processes I of ≥ 10,000 consumers

*Texas & Nebraska: Applies to any entity that: (1) conducts business in Texas/Nebraska or generates products or services consumed by Texas/Nebraska residents; (2) processes or engages in the sale of PI; and (3) does not identify as a small business (independent business having fewer than 500 employees) as defined by the U.S. Small Business Administration. © 2025 Mac Murray & Shuster LLP

A refresher….

- **Consumer Control Over Personal Information**
  - Specific rights, methods, and verification and response procedures
- **Data Privacy Principles & Data Security**
  - Collection, Use, and Retention Limits
  - Reasonable security and protection practices appropriate to volume and nature of PI
- **Heightened Protections For Sensitive PI**
  - Opt-in vs. right to limit vs. notice & opportunity to opt-out

A refresher….

- **Enhanced Disclosure Obligations**
  - Privacy Policy
  - Notice at Collection
  - Sale, targeted advertising, and profiling Notice
- **Service Provider and Third-Party Contracts**
  - Required contracts with parties who receive PI
- **Heightened Risk Processing**
  - Consent for certain processing
  - Assessments

State Updates

Continuous monitoring is an absolute must!

State Updates

- **California AB 566 (January 1, 2027)**
  - Requires browsers to include consumer-configurable opt-out signal functionality

- **Colorado SB 276 (May 23, 2025 (Definition revision: October 1, 2025))**
  - Redefines “Sensitive Data” to include precise geolocation data
  - Controllers must obtain consent to sell sensitive data

State Updates

- **Connecticut SB 1295 (July 1, 2026)**
  - **Expanded "Sensitive Data" Definition**
  - **Lower Applicability Threshold:** Applies to entities that:
    - Process 35,000 consumers' data
    - Process sensitive data
    - Sell consumer data
  - **Enhanced Consumer Rights:**
    - Know specifics about profiling for legal/significant effects
    - Obtain list of third-party data recipients
  - **Stronger Consent & Restrictions:**
    - Consent required to sell sensitive data
    - Prohibits sale/sharing of data for consumers under 18
  - **Privacy Policy Updates:**
    - Bolstered disclosures & material change procedures
  - **Data Protection Assessments:**
    - Clarifies "heightened risk of harm"
    - Adds enhanced obligations for profiling

State Updates

- **Kentucky HB 473 (January 1, 2026)**
  - Exempts certain health data collected by health care providers or covered entities in compliance with HIPAA.

- **Montana SB 297 (October 1, 2025)**
  - Lower Applicability Threshold: Applies to entities that:
    - Process 25,000 consumers' data
    - Process 15,000 consumers' data & derive >25% of gross revenue for sales
  - Removes exemptions for entities subject to GLBA
  - Adds requirements for controllers offering online services to minors (<18)

State Updates

- **Oregon SB 1121 (June 24, 2025)**
  - Provides 30-day right to cure after AG notice of violation
  - Cure period sunsets July 1, 2026
- **Oregon HB 2008 (January 1, 2026)**
  - Prohibits controllers from:
    - Processing personal data for targeted advertising or profiling (legal/significant effects) if consumer is under 16
    - Selling personal data:
      - About consumers under 16
      - If data reveals precise location within 1,750 ft radius

State Updates

- **Oregon HB 3875 (September 24, 2025)**
  - Extends law to motor vehicle manufacturers & affiliates handling data from vehicle usage
- **Texas HB 149 (January 1, 2026)**
  - Requires processors to assist controllers with compliance obligations related to personal information collected, stored, or processed by an AI system
- **Utah HB 418 (July 1, 2026)**
  - Adds consumer right to correct inaccurate personal data

State Updates

- **California CPPA Regulations**
  - ADMT, Risk Assessments & Cybersecurity Audits
    - Obligations for businesses using ADMT for significant decisions
    - Cybersecurity audits for high-risk businesses
    - Risk assessments for sensitive data, profiling, and ADMT
    - Phased compliance starting 2026
  - Accessible Deletion Mechanism
    - Includes registration, account access, and deletion request handling

- **Colorado Privacy Act Regulations**
  - Guidelines for identifying minors and addictive design evaluation

- **New Jersey Data Privacy Act Proposed Regulations**
  - Comprehensive proposed regulations

State Updates

- **CCPA ADMT Regulations**
  - **Pre-Use Notice Requirements:**
  - Must be clear, conspicuous, and delivered before data collection or repurposing
  - Include:
    - Specific purpose of ADMT use
    - Opt-out and access rights
    - Appeal process if exception applies
    - Explanation of how ADMT works and alternative decision-making if opted out
  - **Opt-Out Rights:**
    - Consumers can opt out of ADMT for significant decisions
    - Exceptions: Human appeal process, certain employment/work allocation uses
    - Businesses must offer multiple easy submission methods and confirm processing
  - **Access Rights:**
    - Consumers can request plain language explanations of:
      - Purpose of ADMT
      - Logic and role in decision-making
      - Future use of outputs
    - Must comply with CCPA verification and security standards

CCPA Risk Assessment Regulations

- **Activities Triggering**
  - Selling or Sharing PI
  - Processing Sensitive PI
    - Exception: Limited HR uses (e.g., payroll, benefits, legal compliance)
  - Using ADMT for significant decisions
  - Automated Profiling to infer attributes like intelligence, health, preferences, or behavior in employment or education contexts
  - Profiling Based on Sensitive Locations
  - Training ADMT or Biometric Technologies (e.g., facial recognition, emotion recognition) using PI
- **Submission to the CPPA**
  - Assessments in 2026–2027: Submit by April 1, 2028
  - Assessments after 2027: Submit by April 1 of the following year *(e.g., 2028 assessments → April 1, 2029)*

CCPA Cybersecurity Audit Regulations

- Businesses whose processing of consumer personal information presents "significant risk" to consumers' security:
  - Revenue-Based Trigger:
    - Derived ≥50% of annual revenue from selling or sharing personal information in the preceding calendar year.
  - Revenue + Volume Trigger:
    - Annual gross revenue > $26.625 million AND
    - Processed 250,000+ California consumers'/households' personal information, OR
    - Processed 50,000+ California consumers' sensitive personal information in the preceding year.
  - Staggered compliance: Phased in 2028–2030 based on company revenue tiers.

CCPA Regs Compliance Timeline

- **January 1, 2026**
  - New regulations effective
  - Risk assessments required for **new processing activities**
- **January 1, 2027**
  - Deadline to comply with ADMT regulations
- **December 31, 2027**
  - Deadline to complete risk assessments for **pre-existing processing activities**
- **April 1, 2028**
  - Submit certification for risk assessments
  - Submit certification for cybersecurity audits (companies > $100M revenue in 2026)
- **April 1, 2029**
  - Submit certification for cybersecurity audits (companies $50M–$100M revenue in 2027)
- **April 1, 2030**
  - Submit certification for cybersecurity audits (companies < $50M revenue in 2028)

State Enforcement

State Enforcement

- **CA Privacy**
  - Honda
    - 4 violations
    - $632,500 fine
  - Todd Snyder
    - 3 Violations
    - $345,178 fine
  - Tractor Supply
    - 4 Violations
    - $1.35 mil fine
- **CA DOJ**
  - Healthline
    - 4 violations
    - $1.55 mil fine
  - Jam City
    - 3 violations
    - $345,178 fine
  - Sling TV
    - 2 violations
    - 530,000 fine
- **CT AGO**
  - TicketNetwork
    - 1 violation
    - $85,000 fine
- **TX AGO**
  - Allstate et al.
    - 5 violations
    - Up to $7,500 per violation

State Enforcement

- **Excessive Verification Requirements**
  - Required consumers to provide up to eight personal data fields (e.g., name, address, VIN) to exercise opt-out and limitation rights
  - **Tip:** Design opt-out and limitation request processes to require no additional identity verification beyond what is necessary to confirm the request.

State Enforcement

- **Authorized Agent Barriers**
  - Consumers faced unnecessary hurdles when authorizing agents to act on their behalf
  - **Tip:** Allow authorized agents to submit opt-out or limitation requests with only a signed permission from the consumer, and do not require direct consumer confirmation.

State Enforcement

- **Inadequate Privacy Disclosures**
  - Failure to maintain a compliant privacy policy
  - Failure to maintain employee privacy policy and notify job applicants of their CCPA rights
  - Failure to include required notice for selling sensitive PI

  - **Tip:** CCPA applies to employee data. Implement an EE privacy policy and processes to manage EE data in compliance with the CCPA.

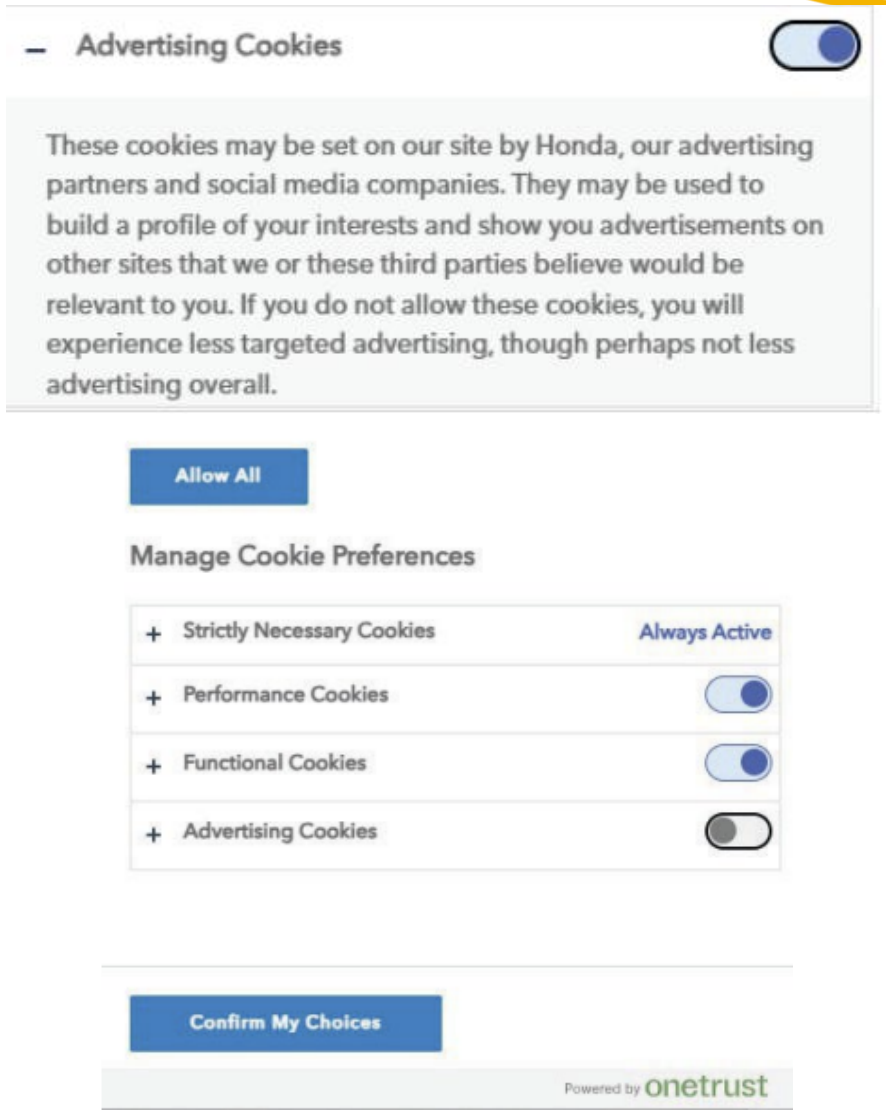
State Enforcement

- **Ineffective Opt-Out Mechanisms**
  - "Do Not Sell My Personal Information" webform did not stop data sharing via trackers, misleading consumers
  - Did not honor opt-out preference signals

  - **Tip:** Ensure website recognizes and responds to browser-based opt-out signals and sync cookie banner opt-out and other opt-out methods.

State Enforcement

- **Asymmetrical Privacy Choices**
  - Opting out of data sharing was more complex than opting in
  - **Tip:** Design consent and cookie management tools so that more privacy is as simple as or easier than less privacy.



State Enforcement

- **Vendor Contracts**
  - Could not produce contracts with ad tech vendors containing required privacy safeguards
  - **Tip:** Review all data disclosure scenarios to determine the appropriate relationship (service provider vs. third party) and ensure written contracts that include required provisions.

State Enforcement

- **Purpose Limitation Breach**
  - Used article titles revealing diagnoses (e.g., “The Ultimate Guide to MS for the Newly Diagnosed”) for ad targeting beyond disclosed purposes

  - **Tip:** Ensure that sharing PI (especially sensitive behavioral data—such as article titles implying medical diagnoses) aligns strictly with the consumer's reasonable expectations and is properly disclosed in privacy policy.

State Enforcement

- **Sale/Sharing of Minors' Data Without Consent**
  - Shared or sold personal data of users aged 13–16 without affirmative opt-in consent; inadequate protections for children under 13

  - **Tip:** Minors are afforded special protections under both comprehensive privacy laws and child privacy laws.

State Enforcement

- **Data Broker Registration**
  - Failed to register as Data Broker
  - **Tip:** Register as a data broker. This is a focus area!

State Enforcement

- **Deceptive Consent Banner**
  - Displayed three opt-out interfaces but continued deploying tracking cookies that shared PI
  - **Tip:** Do not display opt-out or consent banners that mislead consumers or do not work. Ensure all choices are honored and no tracking cookies or data sharing occur after an opt-out.

More than just the money….

- **Streamline Privacy Requests**
  - Simplify opt-out and limitation workflows.
  - Remove excessive verification requirements.
  - Collect only what's necessary for privacy requests.
- **Improve Opt-Out Mechanisms**
  - Reconfigure cookie banners and privacy portals.
  - Honor browser-based signals (e.g., Global Privacy Control).
  - Maintain effective opt-out tools (Opt-Out Monitoring).
- **Validate Third-Party Tools & Vendor Contracts**
  - Regularly test consent management platforms for proper functionality.
  - Update agreements with vendors and ad tech partners to include mandatory privacy safeguards (Contract Overhaul).
- **Employee Training & Retraining**
  - Implement CCPA compliance training for all relevant teams (HR, marketing, IT).
  - Include consumer rights handling and privacy best practices.
- **Governance & Transparency**
  - Conduct annual privacy audits for five years (Independent Verification).
  - Publish privacy metrics and compliance progress (Public Reporting).
  - Engage UX design review to ensure fairness and simplicity in privacy tools.

What Does Enforcement Look Like?

- Usually starts with an inquiry letter, civil investigative demand, or subpoena.
- Often months to more than a year long process
- Early responsiveness and actions can set the tone for the remainder of the investigation

Best Practices

- Engage experienced counsel immediately
- Preserve all relevant documents and communications
- Coordinate a centralized response team
- Communicate carefully and consistently
- Consider voluntary cooperation or settlement discussions

AI Laws: Just the surface

- Scope & Coverage
  - Standalone AI laws in a few states
  - Comprehensive privacy laws in many states regulating PI use for profiling.
- Applicability
  - Role: Developer vs. Deployer.
  - System Type: Standard AI vs. High-Risk AI.
- Consumer interaction disclosure (CA, CO, ME, UT)
  - Prominently disclose to each consumer at the beginning of a verbal interaction and in writing before a written interaction that they are interacting with AI

AI Laws: Just the surface

	Website Disclosures	Pre-interaction Disclosure	Adverse Post-use Notice	Consumer Rights	Risk Assessments	Prohibited Behaviors
Developer of AI Systems	Yes	Yes	No	No	No	Yes
Deployer of AI Systems	No	Yes	No	No	No	Yes
Developer of High-Risk AI Systems	Yes	Yes	No	No	No	Yes
Deployer of High-Risk AI Systems	Yes	Yes	Yes	Yes	Yes	Yes

AI Considerations

- Potential “Sale” Disclosure
  - Avoid inputting consumer PI into AI tools unless necessary.
  - Use techniques to pseudonymize or anonymize PI.
  - Ensure agreements with AI providers prevent the use of PI for their own purposes or combining it with other users' data.
- Consent for Secondary Uses
  - Clearly disclose the purposes of using PI, including AI-generated marketing, in privacy policies and consent forms.
  - Obtain explicit opt-in consent for using PI for secondary purposes.
- Privacy Principles
  - Ensure transparency about privacy practices.
  - Prevent discriminatory use of PI and minimize PI retention time.

2026 predictions

- **Federal Comprehensive Privacy Law**
  - Low Probability of Passage: Political gridlock over preemption and private right of action makes enactment unlikely.
  - If Enacted: Expect strict data minimization, unified consumer rights, strong minor protections, FTC enforcement, and broad state law preemption with carve-outs.
  - If Not Enacted: FTC will expand rulemaking and enforcement; sector-specific bills likely (e.g., children's online safety).
  - Key Implication: Continue building compliance programs around evolving state laws.

- **Federal AI Regulation**
  - Regulations > Legislation: Agencies (FTC, EEOC, CFPB) will use existing authority to regulate AI in high-risk sectors.
  - Focus Areas: Bias testing, transparency, documentation, and procurement standards.
  - Preemption: State AI laws will remain; federal activity will not override them.
  - Key Implication: Prepare for overlapping state and federal AI requirements; vet AI models for bias and risk.

2026 predictions

- **State Privacy Laws**
  - New Laws Coming: Expect more states to adopt comprehensive statutes with consumer rights, sensitive data protections, and risk assessments.
  - Amendment Era: Existing laws will tighten, adding AI provisions and stricter rules for minors.
  - Enforcement Surge: Multi-state sweeps and costly compliance mandates.
  - Key Implication: Update privacy programs frequently; remediate common violations like broken opt-outs and deficient notices.

- **State AI Laws**
  - Expansion: At least 10 states will pass AI-specific laws requiring impact assessments, disclosures, and human-in-the-loop safeguards for high-risk uses.
  - Key Implication: Implement centralized AI governance to track all algorithmic systems.

2026 predictions

- **Children's & Teen Protections**
  - State AADC Laws: More age-appropriate design codes with stricter defaults and parental controls.
  - Federal Action Possible: Child privacy may advance faster than general privacy.
  - Key Implication: Apply special protections for minors, including limits on targeted ads.

- **Other Predictions**
  - Biometric Laws: New statutes with private rights of action; implement consent and retention policies now.
  - Data Brokers & Ad Tech: Universal opt-out enforcement will tighten; review tracking and consent tools.
  - Privacy-Security Convergence: Risk assessments must address privacy and AI risks alongside cybersecurity.
  - Litigation Trends: Rising suits under biometric laws, wiretapping statutes, and AI-related contract disputes.

Contact Center Compliance
DNC.com

Thank you!

Contact us:

Office Address
6525 W Campus Oval Ste 210,
New Albany, OH 43054

Email Address
info@mslawgroup.com

Office Number
614-939-9955

Website
mslawgroup.com

Aaron Parry
aparry@mslawgroup.com