October 25, 2024

State of the States: Privacy Law Edition

Ali Jessani
WilmerHale

Sam Kane
WilmerHale

Stanton Burke
Gibson Dunn

Privacy+ Security Forum

Speakers

Ali Jessani

Senior Associate –
Cybersecurity and Privacy
WilmerHale

Stanton Burke

Senior Associate – Privacy, Cybersecurity & Data Innovation
Gibson Dunn

Sam Kane

Associate –
Cybersecurity and Privacy
WilmerHale

Overview

Privacy+ Security Forum

Overview

- At the federal level, US historically regulated privacy and security through a sectoral approach based on the type of data
- Similarly, US States historically focused on specific areas to regulate (e.g., HIV status, wiretapping, online privacy policies, and biometrics)
- However, after GDPR (and thereafter CCPA), the last 5 years brought a significant increase in new “comprehensive” state privacy laws
- While these state privacy laws have received much attention, the volume of the more “specialized/topical" state privacy laws (and nuances within comprehensive state privacy laws) is worth discussing
- This presentation will address a number of these state law privacy trends and enforcement priorities

Topics

Privacy+ Security Forum

Topics

1. Comprehensive privacy laws
2. UDAP statutes
3. Consumer health laws
4. Other health/sensitive data
5. Artificial intelligence
6. Targeted advertising
7. Children's privacy
8. Biometrics
9. Data brokers

State Comprehensive Privacy Laws

Privacy+ Security Forum

State Comprehensive Privacy Laws – Overview

- **A Growing Patchwork:** To date, 19 states have enacted comprehensive privacy laws (with 7 new laws enacted in 2024).
- **Predominance of the Non-California Model:** Most states with comprehensive privacy laws have hewed to models offered by states like Virginia or Connecticut, rather than adopt California's more-prescriptive model.
- **Recurring Themes**:
  - Transparency requirements (privacy policies and other notices)
  - Data subject rights (right to access, correct, delete, etc.)
  - Opt-out obligations for certain processing activities ("selling", "sharing" (includes targeted ads), use of SPI for non-permitted purposes, automated decision-making (includes profiling))
  - Consent for certain processing activities (use of sensitive data, biometrics, children's data, unexpected secondary data use, etc.)
  - Contracts (data processing agreements and third-party contracts)
  - Reasonable security
  - Data protection impact assessments
- **Continued Reliance on Government Enforcement:** No state *comprehensive* privacy law enacted to date has included a private right of action for privacy-related violations.
- **Not Truly "Comprehensive":** Though these laws are characterized as "comprehensive," they feature numerous exceptions for certain types of entities and information (e.g., GLBA, HIPAA, nonprofits, employee information, commercial information).

State Comprehensive Privacy Laws – Unique Provisions re: Scope

- **CA:** Data based exemptions vs. entity-based exemptions
- **TX, NE:** Includes a partial exemption for "small businesses"
- **MD, NV, CT:** Encompasses "consumer health data" not covered by HIPAA (similar to WA's MHMDA)
- **TN:** Provides affirmative defense if entity has a privacy program that conforms with NIST privacy framework
- **CO, NV, OR, DE, MD:** Does not fully exempt non-profits
- **TN, MT, FL, IA, MD, DE, CT, NH:** Longer than 30-day cure period

State Comprehensive Privacy Laws – Unique Provisions re: Rights/Obligations

- **CA, UT:** Requires offering the ability for consumers to *opt-out/limit* the processing of sensitive personal information (others are opt-in)
- **OR:** Requires controllers to specify (upon request) which third parties (by name) received personal data
- **TX, FL:** If sensitive data or biometrics is sold, requires posting additional notice (e.g., in TX, "NOTICE: We may sell your [sensitive personal data / biometric personal data]")
- **FL:** Right to opt-out of the collection of personal data through voice recognition or facial recognition
- **CA, CO:** Currently require recognizing universal opt-out mechanisms (CT, TX, DE, MT, NH, NJ, and OR will require universal opt-outs to be recognized starting in 2025 or 2026)
- **MD:** Expressly prohibits the "sale" of sensitive data (unless requested by the consumer), and requires controllers to limit the collection of personal data to services requested by the consumer
- **UT, IA:** Does not require data protection impact assessments

Unfair, Deceptive, or Abusive Acts or Practices Laws (UDAP)

Privacy+ Security Forum

Unfair, Deceptive, or Abusive Acts or Practices Laws (UDAP)

- **Overview:** Each state has some form of a general consumer protection law through which it is allowed to sanction unfair or deceptive acts or practices (similar to FTC's authority under Section 5).
- **UDAP Laws in the Privacy Context:** State AGs have relied on UDAP laws as a mechanism through which to sanction companies for privacy violations and promulgate privacy guidance. Recent examples include:
  - In September 2024, the Texas AG announced a settlement with Pieces Technology, a healthcare AI firm, resolving allegations that the company made false, misleading, or deceptive claims about the accuracy of its healthcare AI products in violation of the Texas Deceptive Trade Practices Act (DTPA).
  - In August 2024, the Texas AG sued General Motors for its collection and sale of consumers' private driving data, alleging that these practices violated the DTPA.
  - In July 2024, the New York AG relied on New York's UDAP law to issue guidance related to the use of online tracking technologies by businesses.

Consumer Health Privacy Laws

Privacy+ Security Forum

Consumer Health Privacy Laws

- Washington's My Health My Data Act represents a new category of privacy laws
  - Passed in 2023; went into effect in 2024
  - Broad reach beyond traditional healthcare entities
  - Major attack on health-related advertising
  - Lots of ambiguities – that will be played out in court because of private right of action
  - Already inspired copycats (in NV and CT) with more likely to follow – big issue is if other states are going to also include a private right of action

Consumer Health Privacy Laws

- Key Provisions:
  - Broad consent and “authorization” obligations
  - Specific privacy notice obligations
  - Geofencing obligations
  - Access Control Requirements
  - Private Right of Action (through WA’s consumer protection statute)

Other Laws Regulating Health/Sensitive Data

Privacy+ Security Forum

Other Laws Regulating Health/Sensitive Data

- California Confidentiality of Medical Information Act
  - Builds upon health privacy obligations for HIPAA covered entities (but also goes beyond covered entities in terms of scope)
  - Two new amendments (AB 254 and AB 352) significantly expanded the scope of the law

Other Laws Regulating Health/Sensitive Data

- Genetic Privacy
  - At least ten states have passed laws regulating genetic information by D2C companies
  - Laws generally create consent, transparency, and deletion obligations
  - Generally enforceable by state attorneys general but can include a private right of action (e.g., Illinois)

State Comprehensive Laws and Sensitive Data

- All of the state comprehensive privacy laws create special obligations for the processing of “sensitive” data
- Categories of data that constitute “sensitive” data vary but there is significant overlap with most of the states
- Obligations generally include:
  - Opt-in/opt-out obligations
  - Data protection assessments
- CA and CO have expanded their definitions of sensitive data to include “neural” data

Artificial Intelligence Laws

Privacy+ Security Forum

Artificial Intelligence (AI) Laws

- **Differing Approaches to AI Regulation:** State legislatures are regulating AI in two primary ways: (1) developing AI-specific statutes, and (2) incorporating AI-relevant provisions into existing privacy laws.
- **AI-Specific Statutes:**
  - Colorado's new law (SB 205), although focused on preventing the discriminatory effects of high-risk AI, will broadly impose substantive requirements on businesses that develop and use AI systems.
  - Utah's AI Policy Act requires certain disclosures to consumers around the use of generative AI; California's AI Transparency Act (SB 942) and AB 2013 are similarly oriented around AI transparency.
  - 2024 saw several ambitious, but unsuccessful, proposals, most notably in California (SB 1047) and Connecticut (SB 2).
  - Other narrow issue or use case-specific laws have either passed or been proposed (e.g., deepfakes, employment, state governments).
- **AI-Relevant Provisions in Existing Privacy Laws:**
  - New state privacy laws define "personal information" broadly and create compliance obligations for companies subject to these laws (relevant for both training AI models and for AI use cases).
  - Certain US state privacy laws have created rights for residents to opt out of "profiling" in furtherance of solely automated "decisions that produce legal or similarly significant effects concerning the consumer."

Targeted Advertising

Privacy+ Security Forum

Pixels/Trackers/Targeted Advertising

- Tracking technologies (cookies, pixels, etc.) deployed on websites and apps can be used to collect or share personal data about consumers
- Increasing focus by regulators and plaintiffs' bar on use of technology
- Plaintiffs' lawyers are primarily using laws like California's Invasion of Privacy Act (CIPA) and other state wiretapping statutes to allege that the placement of these technologies is illegally recording consumers without their consent
  - The risk is greater in the 11 states with two-party consent
- The federal Video Privacy Protection Act is being used in a similar manner
- Plaintiffs have also relied on state common law claims, constitutional claims, and (in some cases) state comprehensive privacy laws to initiate lawsuits against companies' use of tracking technologies.

Children’s Privacy

Privacy+ Security Forum

Children's Privacy – Overview

Current Landscape

- Since 2000, **COPPA** has been the cornerstone of youth privacy
- COPPA imposes requirements on operators of online services that are directed to children under 13 that have **actual knowledge** they process information from children under 13
- However, with increasing screen time particularly during the pandemic, lawmakers have expressed concerns about the protections for minors' personal information
- **Now**…
  - **Federal**: deliberating KOSA and COPPA 2.0
  - **State**: 3 different approaches
    - Amending state privacy laws
    - Enacting broader "age-appropriate design" laws for applicable online services
    - Enacting social media laws applicable to social media and gaming platforms

Children's Privacy – State Level Protection

State Youth Privacy Requirements (currently enforceable)

- **CA:** Prohibits businesses from selling children's (under 16) PI unless opt-in consent is obtained
- **FL**: Prohibits companies from processing sensitive data of children under 18 without authorization
- **CT**: Requires data controllers to obtain consent when selling minors' information (under 18)

State Youth Privacy Requirements (enforceable in 2025)

- **VA**: Imposes additional requirements on controllers that process the personal data of a known child (under 13)
- **MD**: Prohibits sale and targeted advertising involving personal data of consumers under age 18
- **NY**: Bars services directed to minors (13-17) from collecting, sharing, or selling personal information without their informed consent unless strictly necessary
- **CO**: Adds enhanced protections when a minor's data is processed and a heightened risk of harm to minors exists

Proposals

- There are also proposals in HI, MN, NM, SC, VT, and VA

Children's Privacy – State Level Protection

State Age-appropriate Design Laws – target online services "reasonably likely" to be accessed by children

- **CA:** Age-Appropriate Design Code Act
  - Enjoined. The Ninth Circuit partially upheld the district court's injunction on DPIA requirement on First Amendment grounds but vacated the remainder of the injunction and remanded the case.
- **MD**: Age-Appropriate Design Code Act
  - Became **effective** on October 1, 2024.

Biometrics

Privacy+ Security Forum

Biometrics

- **Biometric data is broadly defined…**
  - Includes data or information about the physical, physiological, or behavioral characteristics of an individual that could be used to identify an individual
  - Examples: any retina or iris scan, fingerprint, voiceprint, scan or record of hand geometry, or scan or record of face geometry

- **And covers a broad range of technologies…**
  - Automated methods of recognizing or distinguishing people
  - Detecting or tracking of hands, faces, eyes, or voices
  - Use of avatars and certain augmented reality effects
  - Attribute prediction (such as age, gender, skin tone, race)
  - Use of AI on audio or video data
  - Calculating voice, tone, speech, eye contact, gait, etc.
  - Sentiment analysis

Biometrics

- **Illinois Biometric Information Privacy Act** ("BIPA") is the strictest standard for biometrics (if you comply with BIPA, you comply everywhere)
- Includes a robust private right of action and purely technical violations are enough
- Includes prescriptive requirements – including:
  - Public disclosure of a retention period (and deletion of biometrics within 3 years of last consumer interaction)
  - Cannot use biometrics for use cases consumer did not consent to
    - Consent must disclose what data is collected, the purpose, and retention period
  - Cannot sell, lease, trade, or profit from biometric data
  - Cannot disclose or disseminate biometric data without consent
  - Must store, transmit and protect biometric data using reasonable standard of care

Biometrics

- **Texas' Collection and Use of Biometric Identifiers Act** ("CUBI") was enacted in 2001 but not enforced until recently; with a few cases pending
  - No private right of action; no statute of limitations
  - AG takes position that every capture of biometric identifier is a separate violation

- **Washington's Biometric Privacy Law** prohibits "enrolling" a biometric identifier in a database for a "commercial purpose" without consent
  - No private right of action

- 10+ states have proposals for biometric privacy laws or are expanding comprehensive privacy laws to address biometrics
  - For example, Colorado's HB 1130 amends the ColoPA to include requirements analogous to BIPA (although, like CUBI, only the AG can bring lawsuits)

Data Brokers

Privacy+ Security Forum

Data Brokers

- CA, OR, TX, and VT have passed laws requiring data brokers to register with the state (and, in some cases, adopt additional security measures for safeguarding personal data)
- CA has significantly modified its law with the DELETE Act
- The laws vary in their definitions but there is often overlap
  - The laws also tie back to the state's comprehensive privacy law in some cases
- Seems to be "low hanging fruit" for legislatures
- Arguably the biggest risk for companies is reputational

Enforcement Priorities

Privacy+ Security Forum

Enforcement Priorities

- **California Taking the Lead:** California poses a unique enforcement risk because: (1) it has two enforcement bodies (the California AG and California Privacy Protection Agency); (2) the CCPA/CPRA regime is arguably the most prescriptive of the comprehensive state privacy laws; and (3) the CPPA continues to build out a robust regulatory regime to accompany the CCPA/CPRA's statutory requirements.
    - The Texas AG has been notably active on privacy issues recently, suggesting that it may be a key state-level privacy enforcer in the years to come.
    - Regulators in Colorado and Connecticut are also actively enforcing their privacy laws.
- **Focus on Low-Hanging Fruit:** Regulators are likely to focus on "low-hanging fruit" (e.g., privacy policies, "Do Not Sell" links, etc.) and use cases involving sensitive data and targeted advertising.
    - February 2024 report from Connecticut AG identified privacy policies, sensitive data, teens' data, and data brokers as enforcement priorities.
    - California AG has conducted "investigative sweeps" in several areas, including streaming services, employee and job applicant information, and mobile apps.
    - Texas AG launched data privacy and security initiative in June 2024.

Key Takeaways and Conclusion

Privacy+ Security Forum

Questions & Contacts

Ali Jessani

Senior Associate –
Cybersecurity and Privacy
WilmerHale

Stanton Burke

Senior Associate – Privacy, Cybersecurity & Data Innovation
Gibson Dunn

Sam Kane

Associate –
Cybersecurity and Privacy
WilmerHale