Cooley

Data Privacy & Cybersecurity Law in 2025 and Beyond

June 10, 2025

Kristen Mathews, Tania Soris, & James Farnsworth

ACC Association of Corporate Counsel
NEW YORK CITY

Speakers

James Farnsworth
Chief US Compliance & Regulatory Counsel
Capgemini North America
New York

Kristen Mathews
Partner
New York
kmathews@cooley.com

Tania Soris
Associate
New York
tsoris@cooley.com

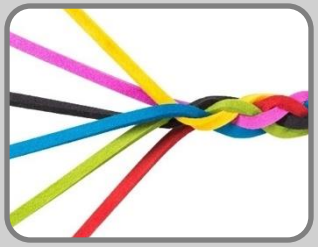
ACC Association of Corporate Counsel
NEW YORK CITY

Agenda

The Fragmented U.S. Consumer Privacy Landscape

Neural Privacy and AI in 2025

Youth Privacy: A Growing Priority



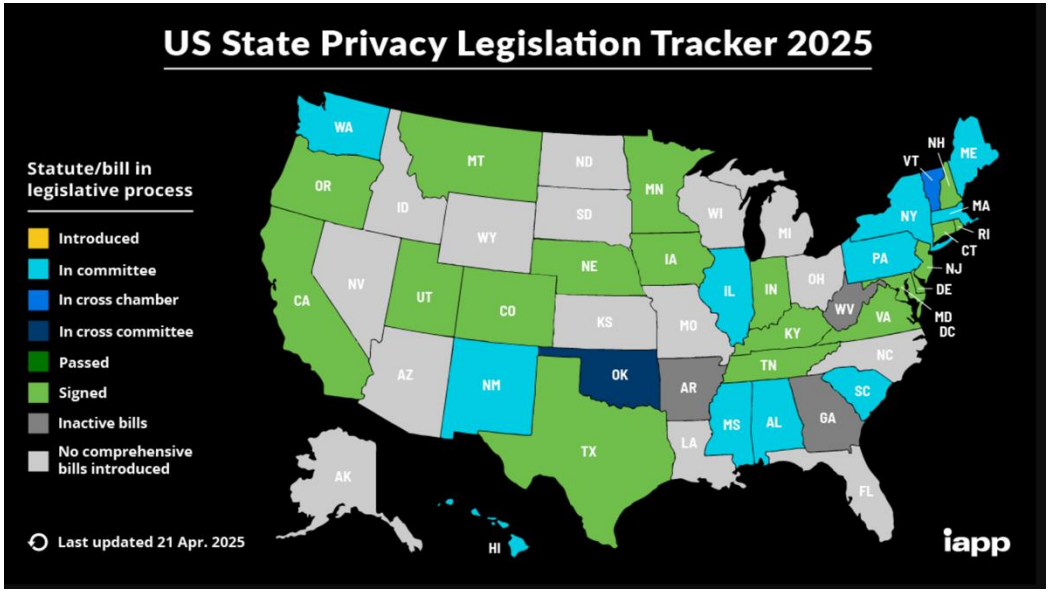
Practical Considerations – Harmonizing Compliance Efforts

The Fragmented U.S. Consumer Privacy Landscape

Cooley

The Fragmented U.S. State Privacy Landscape

- State-level surge: 19 states with comprehensive consumer privacy laws.
- Key features: consumer rights (*e.g.*, access, deletion, correction, opt out), transparency, data minimization, sensitive data protections.
- Challenges: compliance complexity for businesses.
- Federal stagnation: American Privacy Rights Act (APRA) introduced but not passed.



Federal Efforts: DOJ Final Rule Overview

- Effective April 8, 2025
- Restricts bulk transfers of U.S. “sensitive personal data” and “government-related data” abroad, which includes a set of “sensitive personal data relating to U.S. persons,” even if de-identified or encrypted
- Applies to data brokerage, vendor agreements, employment agreements, and investment agreements
- Applies directly to “U.S. persons”
- “Countries of Concern” currently include China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela
- “Covered Persons”

Federal Efforts: DOJ Final Rule Overview (Contd.)

- Prohibited Transactions vs. Restricted Transactions.
- Enforcement by DOJ and Commerce Department.
- Civil monetary fines of up to $374,474 per violation or twice the value of the transaction, whichever is greater.
- Criminal penalties of up to US $1,000,000- or 20-years' imprisonment are available for willful violations.
- Compliance Implications:
  - Assess existing data flows.
  - Implement a tailored compliance program.
  - Monitor changes to the new Rule.

Neural Privacy in 2025

Cooley

Neurotech That Can “Read” the Mind

- Advancements in neurotechnology can read data from the brain, and AI can derive information about people from the data.
- Some devices are implanted in the brain with surgery.
- Some devices are wearable, such as headbands, helmets, earbuds, wristbands, and extended reality headsets.
- Some devices not only read data but also can stimulate the brain to cause an effect.

Medical Use Cases

- Help ALS and stroke patients and individuals with paralysis use their minds to control their environment, and even their limbs.
  - Keyboards
  - Cursors
  - Exoskeletons
  - Wheelchairs
- Enable a person to communicate using brain signals.
- Detect an oncoming epileptic seizure in advance.
- Treat depression and anxiety.

Business Use Cases

Direct customers to products they like (*e.g.*, a fragrance selector)

Monitor employee engagement at work

Monitor employee attentiveness when driving a car or train, flying a plane, or on a dangerous factory floor or construction zone

Monitor student engagement in a classroom

Improve the results of advertising campaigns by detecting and adapting to viewer response

Use of brain data to uniquely identify a person

Colorado Requirements for Neural Data

Post a privacy notice informing individuals about the neural data they collect and their use, retention and disclosure of this information, including each purpose for which each kind of personal information is used and the kinds of third parties they share it with.

Obtain clear, freely given, informed, specific, affirmative and unambiguous consent from an individual before collecting or using their neural data, which such consent must include a disclosure re the names of any third parties to which the information is sold.

Consent wording must inform individuals of the names of any third parties to which the business sells this information.

Refresh each individual's consent every 24 months, absent having interacted with the individual in the meantime, or provide a user-controlled interface for the individual to manage their opt-out preferences at any time.

Colorado Requirements for Neural Data

Refrain from using dark patterns when obtaining consent from individuals.

Delete or de-identify this information when it is no longer necessary for the purpose for which it was collected, and in any event when an individual has withdrawn consent for its use.

Inform individuals of the purposes for which it uses this data and only collect such information that is reasonably necessary to fulfill, or that is compatible with, those purposes, absent additional consent.

Afford individuals the right and ability to access, correct and delete this information in the business's possession or control, and to opt out of the sale of this information or use for targeted advertising or to make important automated decisions.

Colorado Requirements for Neural Data

Conduct data protection assessments addressing the collection, use, retention and disclosure of this information.

Do not use this data for unlawful discrimination.

Take reasonable measures to secure this data.

California Requirements for Neural Data

- Similar to Colorado's Privacy Act; however, notable differences include:
  - More granular consumer "right to know"
  - "Notice At Collection" of data
  - Rather than a requirement that individuals opt *in* to the processing of their SPI, the CCPA instead provides a right to opt *out* of the processing of such information other than for specified purposes.
    - However, consumers do *not* have the right to opt-out of the use and disclosure of SPI if the SPI is not used by the business to infer characteristics about them.
  - Privacy policy must state retention period or criteria for retention period of SPI.

Montana Requirements for Neural Data:

- Two different privacy policies.
  - One: A high-level privacy policy overview with basic essential information about the entity's collection, use and disclosure of neural data.
  - Two: A prominent publicly available privacy notice that includes, at least, information about the entity's data collection, consent, use, access, disclosure, transfer, security, retention and deletion practices for neural data.
- Obtain initial express consent for the collection, use or disclosure of a consumer's neural data. Such consent must specify how the entity may share the neural data.
- Obtain a consumer's separate express consent to transfer or disclose a consumer's neural data to any third party other than the entity's processors. This consent must include the name of the third party to which the neural data is transferred or disclosed.

Montana Requirements for Neural Data:

- Obtain a consumer's separate express consent to use neural data beyond the primary purpose and inherent contextual uses.
- Obtain a consumer's informed express consent to transfer or disclose a consumer's neural data to third persons for research purposes.
- Obtain a consumer's express consent to market to the consumer based on the consumer's neural data.

Montana Requirements for Neural Data:

- Obtain a consumer's express consent to sell the consumer's neural data in exchange for valuable consideration.
- Comply with applicable law requiring valid legal process before disclosing neural data to law enforcement or any other governmental agency, absent a consumer's express consent.
- Develop, implement and maintain a comprehensive security program to protect consumers' neural data against unauthorized access, use and disclosure.
- Provide a process for consumers to access and delete their neural data, and revoke any consent provided by the consumer with regard to their neural data.
- Neural data collected in Montana may not be stored within the territorial boundaries of any country currently sanctioned by the US or designated as a foreign adversary of the US.
- Neural data collected in Montana may only be transferred or stored outside of the US with the consent of the consumer.
- Entities may not disclose a consumer's neural data to any entity offering health insurance, life insurance or long-term care insurance, or to the consumer's employer, absent the consumer's express consent.

Youth Privacy: A Growing Priority

Cooley

NY Child Data Protection Act

- Effective June 20, 2025
- Minors: Under 18
- Applies to operators that provide an online service: (a) With actual knowledge that a user is a minor (under 18), or (b) Where the online service is primarily directed to minors.
- Key requirements include:
  - Operators may process a minor's PI only if processing is strictly necessary for enumerated permissible purposes or if they obtain: (a) Verifiable parental consent for minors under 13, or (b) Informed consent from minors aged 13–18.
  - Consent is required for advertising and marketing.
  - Operators must inform third parties that a user is a minor or that services are directed to minors.
  - Compliance obligations apply to processors.
  - Enforcement by the AG, who may seek civil penalties of up to $5,000 per violation.

NY Stop Addictive Feeds Exploitation (SAFE) For Kids Act

- Effective: Signed on June 20, 2024; the AG has yet to promulgate rules and regulations.
- Minors: Under 18
- Applies to social media platforms that provide or offer "addictive feeds" as a significant part of their services.
- Requirements:
  - Platforms must verify a user's age before providing an addictive feed.
  - Platforms are prohibited from sending overnight notifications to minors without parental consent.
  - Default safety settings must be enabled on platforms.
  - Enforcement: The AG may seek civil penalties of up to $5,000 per violation.

Practical Considerations – Harmonizing Compliance Efforts

Cooley

Addressing a Patchwork of Privacy Laws and Obligations

- How to Keep Track of the Differences in State Laws
  - It's more complex than when we had 5 states two years ago!!!
- Adopting a Universal vs. Specific Approach
- Case Study: Implementing/Modifying Privacy Notices
  - Relying on the Highest Standards for a Universal Approach
  - Applying Notices to the Applicable Jurisdiction
- Case Study: Addressing Different Requirements and Age Triggers in Child Data Protection Laws

Addressing a Patchwork of Privacy Laws and Obligations

- How to Address New Data Transfer Rules in a Global Company
  - Know Your Data and Where It Is Going (it's not just GDPR's cross border transfer rules anymore)
    - Mapping is essential for the range of cross border transfer rules, data localization rules and national security restrictions
  - DOJ Final Rule regarding bulk sensitive personal data
    - Covered Data
    - Covered Transactions
    - Covered Persons/Countries of Concern

Questions?

Cooley