Privacy and AI Regulatory Compliance

CONEXXUS 365

CONEXXUS solve forward

Your Host:
Casey Brant

Standards Coordinator
Conexxus, Inc.

Your Moderator:
Carolyn O'Neill

Manager of Data Management,
Maverik/Kum & Go

Agenda

- Housekeeping
- About Conexxus
- Presenters
- Presentation
- Q&A

Housekeeping

This webinar is being recorded and will be made available on Conexxus365.org

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact 365@conexxus.org for questions regarding a certificate of webinar attendance for qualifying live events.

Interested in speaking or sponsoring a Conexxus365 event?
Contact 365@conexxus.org to discuss upcoming opportunities with our team.

Disclaimer

Conexxus does not endorse any products or services that may be described or mentioned in this presentation.

The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus.

By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.

Thank you to our 2025 Annual Sponsors!

Diamond Sponsors

Acumera
AiFA LABS
armor SAFE TECHNOLOGIES
Bulloch TECHNOLOGIES | DOVER FUELING SOLUTIONS | AvaLAN NETWORKS
Bluefin
FIELD ADVANTAGE
HUGHES An EchoStar Company
invenco by GVR
K3DES
Mako NETWORKS
NACS
NCR VOYIX

Emerald Sponsors

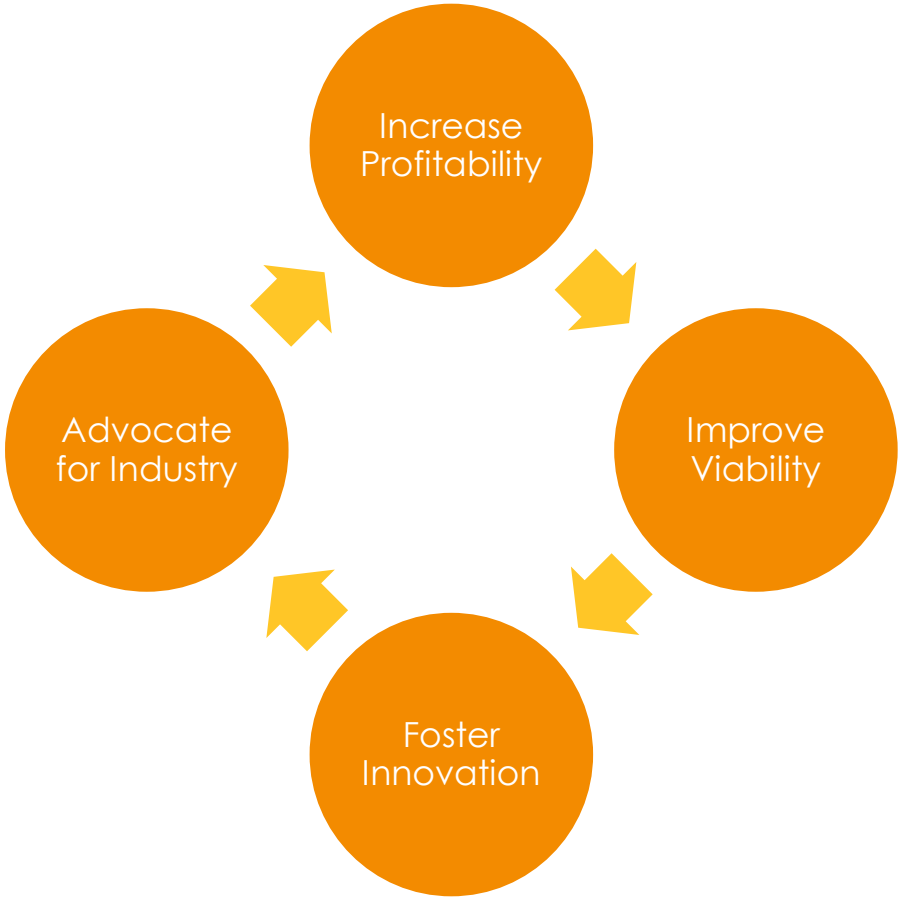
GS1 US
verifone
W. CAPRA

Garnet Sponsors

nouria
OPIS A DOW JONES COMPANY
PAR Retail
PDI TECHNOLOGIES
Stratus A PENGUIN SOLUTIONS® BRAND

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set **standards**…
  - Data exchange
  - Security
  - Mobile commerce
- We provide **vision**
  - Identify emerging tech/trends
- We **advocate** for our industry
  - Technology is policy



CONEXXUS 365

CONEXXUS solve forward

Connect with Conexxus

www.conexxus365.org

365@conexxus.org

www.conexxus.org

info@conexxus.org

@conexxus.org

Alan Thiemann

General Counsel,
Conexxus
athiemann@conleyrose.com

Privacy and AI Regulatory Compliance

2025 Matrix of US State Privacy/AI Laws

US Privacy/AI Compliance

A summary ("Matrix") of currently enacted state consumer privacy laws (already in effect or enacted and coming into effect as of April 1, 2025) has been prepared by Conexxus General Counsel Alan Thiemann and Allie Russell (Conley Rose, P.C.), to provide a readily available means for a retail merchant (or an industry technology service provider) to compare what compliance steps it should take based on where it is doing business and what types of personally-identifiable information (PII) it is collecting and processing. The current list of state consumer privacy laws now totals 21 and results in a complicated, nuanced compliance structure, so a merchant/service provider should consult with appropriate counsel to determine how to best pursue its legal options.

- Nevada is included in this Matrix because it covers privacy requirements related to businesses dealing with consumers. Although the law is largely focused on online business activities, there are sufficient requirements that may impact brick and mortar stores (See Section A). Florida is also included because it has more in common with other consumer privacy laws even though it is heavily focused on online businesses. Already in 2025, there are several additional states that have "active" consumer privacy laws working their way through the Legislatures: Ohio, Oklahoma, and Pennsylvania.

Fundamentals

This Matrix may also be of use to retail technology vendors who provide services to merchants that could involve the collection and use of consumer personal information. In most such situations, such a vendor is not the controller but would merely process consumer PI on behalf of merchants; accordingly, some of this information is not fully relevant but may nonetheless provide a vendor with a useful starting point for determining how to build its privacy compliance strategy.

- **Merchants are almost always a "controller" – the entity that determines what PII to collect and process.**
- **Service Providers/vendors are almost always the "processor" – the entity that handles PII on behalf of the merchant.**
- **A specific category in the Matrix (see Section D) compares current state laws affecting loyalty programs.**

State Privacy Law Scorecard

Pre-2025 State Laws

CA, CO, CT, FL, MT, NV, OR, TX, UT, VA

January 1, 2025

DE, IA, NE, NH

January 15, 2025

NJ

July 1, 2025

TN

July 31, 2025

MN

October, 1, 2025

MD (but does not apply to data processing before April 1, 2026)

January 1, 2026

IN, KY, RI

STILL NO PROSPECT FOR FEDERAL PRIVACY LAW

Emerging AI Regulations

The Matrix also includes information on how states are beginning to regulate artificial intelligence (AI) systems/tools (see Section H-J). Two states have adopted "stand alone" AI laws, while others have integrated some elements of AI regulation within their consumer privacy laws. Additionally, the Matrix includes provisions that, while not specifically AI focused, may still impact AI tools. This area of regulation promises to be very active in 2025 so Conexxus members should pay particular attention to how new state laws handle AI.

- More than 100 different bills addressing specific AI issues (e.g., healthcare, insurance, copyright) were passed during 2024, but only Utah and Colorado passed AI laws that may impact Conexxus members. Comprehensive AI regulatory legislation was passed by the California Legislature, but it was vetoed by Governor Newsom; accordingly, another attempt will likely be made in 2025; and California also enacted amendments to the CPPA that integrate AI regulation. Finally, model privacy legislation has been proposed by the Electronic Privacy Information Center that integrates regulation AI with consumer privacy regulation. Such a model bill could become the focal point in states that do not yet have consumer privacy laws.
- 900+ bills introduced so far in 2025. A bill regulating both AI developers and deployers was passed by the Virginia Legislature, but it was vetoed by Gov. Youngkin on March 24, 2025.

What to expect in AI laws?

Trump revoked Biden Executive Order on AI – moving to effort to “eliminate regulatory barriers.” NIST largely removed from role in generating national AI standards.

Colorado AI Act offers a compelling example. In May 2024, it enacted a first-in-the-nation law regulating AI developed and used for "consequential decisions," such as employment, education/training, lending, and housing. It distinguishes between “developers” and “deployers” of these high-risk tools and outlines parallel obligations for addressing risks. Colorado's partnership model — which reflects an emerging consensus in AI governance — is likely to be a template for future bills.

The thinking is that deployers determine how AI is configured, implemented and used to make consequential decisions, but they typically don't design AI tools. Developers decide how AI is designed and trained. But they cannot control or reliably know, access or anticipate their customers' data or use of AI to make consequential decisions. Not 100% accurate – many times deployers also separately train an AI tool, which can dramatically change how the developer designed the model.

2025 and Beyond

Many future state law debates are likely to focus on Model Legislation drafted by the Electronic Privacy Information Center ("EPIC") https://epic.org/wp-content/uploads/2024/09/State-Data-Privacy-Act-EPIC-CR. In 2023, EPIC proposed its initial model legislation, which was introduced and considered by several states during 2024. Maryland enacted the Maryland Online Data Privacy Act ("MODPA") with key provisions from the EPIC model, including data minimization rules. Versions of the 2023 Model also came close to passage in Vermont and Maine. Finally, a Massachusetts committee favorably reported the bill.

The 2024 Model Legislation, while it has withdrawn some explicit language from the 2023 version, would require regulating "harmful/discriminatory AI", continues to focus on AI regulatory issues under the heading "Consumer Rights." Section 4(f) of the Model provides that: "A controller or processor may not collect, process, or transfer personal data in a manner that discriminates against an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services on the basis of an individual's race, color, sex, sexual orientation, gender identity, disability, religion, ancestry, or national origin." Section 4(g)(1) states that this restriction does not apply for the purpose of a controller or processor self-testing to prevent or mitigate unlawful discrimination.

- Both Sections 4(f) and 4(g) were taken almost verbatim from the 2023 Model Legislation's "AI Regulation" section. What makes this language additionally worrisome for Conexxus members is the issue with AI's notorious bias, which potentially leads to the question whether any use of AI is capable of complying with this language.
- Equally troublesome is the inclusion of "profiling" as another prohibited activity – one which likely covers the use of AI, even if it is not expressly stated. While "profiling" consumers is covered under some existing state laws (e.g., California, Maryland), only Colorado has enacted specific legislation regulating AI in a manner similar to the Model Legislation. Clearly, these provisions comingle AI regulation with consumer privacy regulation, which is likely to represent an onerous burden on many Conexxus members.
- "Profiling" is defined (Section 1(31) as any form of processing performed on personal data to evaluate, analyze or predict personal aspects including an individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Again, many merchants and retail technology companies engage in profiling, so it may be difficult to comply with this provision.
-

Additional AI Actions

California “dangerous AI” law passed by State Legislature at tend of 2024, would have required “kill switch” to give regulators control over the AI system. Vetoed by Governor Newsome but is likely to return again in 2025.

Virginia Legislature passed a bill mandating middle of the road regulations – opposed by both sides. Governor Youngkin vetoed on March 24, stating the bill would have blunted innovation. Copycat bills pending in CA, CT, MA, NE, NM, and NY. Similar Texas bill replace with “lite” regulatory approach.

NJ has established a Civil Rights Innovation Lab to develop best practices for “responsible AI.”

Internationally, there is a move towards liberalizing EU AI Act but no consensus. Both the US and the UK refused to sign the Paris AI Accord -- signaling a desire for more flexibility and less regulation.

Determing Your Compliance Plan

The Matrix covers the myriad of state laws that have passed, many of which include unique provisions, a privacy compliance program that simply picks the strictest state to comply with as a standard is not a prudent approach. While California was initially regarded as the state with the strictest privacy law when only a few other state laws were in place, that very quickly became an incorrect characterization as other states started including provisions even stricter than California's (e.g., Maryland's minimum necessary requirement). On the opposite perspective, California is only 1 of 2 states (plus NH) which fails to recognize employee personal information and business contact information is NOT regulated PI; the states are mixed in their treatment of anonymized/aggregated data as PI.

These distinctions mean that a business that is facing compliance across multiple states need to inventory each state's law, its requirements, and the organization's data practices to determine what a comprehensive compliance program will entail.

DISCLAIMER: The Matrix is not intended to be, nor should it be, used as a determination of your legal rights or obligations. It is provided merely as an aide for a Conexxus member to evaluate its compliance with applicable state consumer privacy laws and regulations and emerging AI laws/regulations.

Compliance Steps

Steps for general compliance with privacy laws:

1. Conduct a privacy assessment.

2. Create a privacy policy, and implement appropriate notice of and consent to it.

3. Create a privacy rights request webpage, and a management structure and internal procedure t to fulfill privacy rights requests made by individuals.

4. Empower a privacy officer, train employees about privacy and cybersecurity law compliance, and (if the business handles sensitive personal information) prepare a data privacy assessment (DPA) report to evaluate the level and impact of risk.

Management, Training, and DPAs

The last steps to comply with privacy laws are to create a management structure for cybersecurity and privacy, and train employees about it. Also, if the business handles sensitive personal information (e.g., biometric information, geolocation), it must prepare a DPA report. The primary purposes of such a report are as follows.

- Identify the standard(s) used for the privacy assessment.
- Summarize the scope of and process for that assessment.
- Identify all personal information and sensitive personal information handled by the business, all uses of it, and the legal bases for such activity.
- Map the flow of the organization's collection and use of such information, including all internal and third party systems used to do so.
- Identify the employees, vendors, services providers, and other third parties responsible for handling the information.
- Identify risks to the privacy and security of the information, the safeguards implemented to mitigate those risks, and any additional steps to further do so.
- Classify the levels of mitigated risks (e.g., high, medium, low).

Stay Tuned for

Q&A