Good Morning, Chair Sariñana, Vice Chair Berghmans, and Members of the Committee:

My name is William Chanes Martinez. I am an Associate Attorney with Mariner Strategies, where I serve as Counsel to the State Privacy and Security Coalition (SPSC). SPSC is a multi-sector coalition of more than 30 companies and six trade associations spanning the retail, technology, telecommunications, automotive, healthcare, and payment card sectors. SPSC works with legislators and regulators across the country to develop data privacy and AI frameworks that protect consumers, drive consensus amongst stakeholders, and promote interoperability across states.

I also have a background in advising businesses on privacy law compliance and helping them navigate the complexity of rules across the United States, the European Union, the United Kingdom, the Middle East, and Brazil. Finally, I am a certified Artificial Intelligence Governance Professional, Information Privacy Professional in both the United States and Europe, and a designated Fellow of Information Privacy with the International Association of Privacy Professionals.

I appreciate the opportunity to share insights on how New Mexico can approach AI policy in a thoughtful and pragmatic way that puts consumers first without stifling industry innovation. My remarks will focus on three key points:

1. **Comprehensive data privacy legislation should come first because it creates the foundation for any responsible AI regulation.**
2. **The United States (and New Mexico) should not copy the European Union's model, but instead build on the state privacy framework already in place that advances interoperability while protecting consumers.**
3. **Finding consensus around AI before regulating it is essential to ensure clarity, consistency, and effective compliance.**

I. DATA PRIVACY IS THE FOUNDATION TO ANY AI LEGISLATION

When we talk about regulating artificial intelligence, the conversation often starts with algorithms. However, every AI system depends on one thing—data. What data is collected, how it's used, and how it's protected determines whether AI works safely and fairly. That's why comprehensive data privacy law is the foundation for any effective approach to regulating AI.

- **Consumer Rights**: Across the country, eighteen states have enacted comprehensive privacy laws modeled on the same national framework adopted in Virginia, Colorado, and Connecticut. Together, those laws protect more than 100 million Americans and give people meaningful rights over their personal information. They guarantee the right to know what personal data is collected, to correct inaccuracies, to delete data, and to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data or profiling in furtherance of automated decision that produces any legal or similarly significant effect concerning a consumer. These consumer rights give people real control over how their data is used, including when AI systems are involved. For example, if an algorithm is used to determine a consumer's eligibility for an insurance discount or to personalize a healthcare service, those same rights allow the individual to understand how their data was used and to request correction or deletion of inaccurate information.
- **Data Minimization**: Comprehensive privacy laws also set clear standards for how businesses must handle a consumer's data. Under the data minimization standard, a data controller must limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. In other words,

businesses cannot engage in mass collection of personal data – any such collection must meet this standard.

- **Purpose Limitation**: The companion principle—purpose limitation—requires that personal data be processed only for purposes that are reasonably necessary and compatible with those disclosed to the consumer unless the business obtains additional consent. In practice, this means a company cannot tell consumers it is collecting information for account verification and later use that same data to train an unrelated AI model without permission. It is a common misconception that broad disclosures in a privacy policy give companies free rein to use data however they wish. Recent enforcement actions by the Federal Trade Commission (FTC) and the California Attorney General make clear that regulators expect real alignment between what consumers are told and how their information is used.
    - ***FTC v. IntelliVision Technologies Corp. (2024)***: The FTC alleged that IntelliVision falsely claimed its facial-recognition technology was trained on "millions of faces" and free from gender or racial bias. In reality, the company used roughly 100,000 unique individuals and lacked reliable testing or substantiation for its claims. The settlement prohibits misrepresentations about AI training data, accuracy, or bias mitigation and requires rigorous documentation of model development. The case demonstrates that misusing—or misrepresenting—the purpose of data collection in AI contexts can amount to a deceptive practice under Section 5 of the FTC Act.
    - ***People v. Healthline Media LLC (2025)***: The California Attorney General found that Healthline shared readers' browsing data—including article titles suggesting medical diagnoses—with third-party advertisers, even after users opted out or sent Global Privacy Control

signals. The complaint alleged that this conduct violated the CCPA's purpose-limitation and opt-out requirements by repurposing sensitive health information for commercial advertising. The company paid $1.55 million and agreed to injunctive terms requiring stronger consent mechanisms, enhanced contractual controls, and regular compliance reviews.

- **AI Application**: These principles are particularly critical for AI, which relies on large datasets. The more data that's collected and repurposed without guardrails, the greater the risk of misuse, exposure, or diminished data quality. Data minimization and purpose limitation help ensure that data collection is both necessary and aligned with stated purposes. Businesses should ask, "Is the data we're collecting necessary for this system to function, and is it being used for the reason we told consumers?" This approach promotes transparency and accountability while also improving AI performance by reducing noise and ensuring data integrity. When AI systems are trained on sensitive data, businesses must also conduct a data protection assessment to evaluate associated risks.
- **Data Protection Assessments**: Comprehensive privacy laws also require businesses to conduct data protection assessments (DPAs) when engaging in processing activities that present heightened risks to consumers—such as targeted advertising, profiling, or the use of sensitive data. In the AI context, a DPA helps identify and mitigate potential harms before deployment. For example, when an AI model is trained on sensitive personal data—like biometric, health, or precise geolocation information—businesses must evaluate whether the processing is necessary, proportionate, and accompanied by appropriate safeguards. These assessments not only promote accountability

but also ensure that organizations can demonstrate compliance if regulators review their practices.

- **Data Security**: Comprehensive privacy frameworks also impose reasonable data security requirements, which are especially critical for AI systems. Data controllers must implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. For example, access controls and encryption. When data is properly secured, it reduces the risk that training sets or model outputs will expose sensitive personal information or replicate compromised data.
- **Interoperability**: The benefits of this framework extend beyond individual rights. Privacy laws that align with the national model also promote interoperability. In the absence of a federal privacy law, states that harmonize their approaches create consistency for both consumers and companies. It means a person's rights—and a company's obligations—don't change every time data crosses a state line. Without that alignment, we risk a patchwork of conflicting rules that undermine compliance and confuse consumers. We've already seen how this works in practice. Recent amendments to Connecticut's Data Privacy Act similarly requires data controllers to assess risks from automated decision-making, giving regulators the tools to evaluate how AI systems affect consumers. Both examples show that AI oversight can be built effectively on top of a well-designed privacy foundation.
- **Conclusion**: For New Mexico, this is the best path forward. Adopting a comprehensive privacy law that aligns with the national framework would give New Mexicans the same rights as residents in other states, establish clear obligations for businesses, and create the legal infrastructure needed to regulate AI responsibly.

II. THE U.S. SHOULD NOT COPY THE EU MODEL FOR AI REGULATION

- **<u>Different Legal System</u>**: The European Union's AI Act spans nearly 900 pages and is built for a very different legal and regulatory structure—one characterized by centralized authority, uniform application, and extensive administrative rulemaking. The United States, by contrast, operates under a decentralized system with overlapping federal and state jurisdictions. Attempting to import the EU's one-size-fits-all model would be both impractical and counterproductive.
- **<u>GDPR Example</u>**: When states first began developing privacy laws, they successfully drew on elements of the EU's General Data Protection Regulation (GDPR) and adapted them into what is now recognized as the national privacy framework. States like Colorado and Connecticut translated GDPR's core principles (e.g., transparency, purpose limitation, and consumer rights) into a uniquely American structure that balances consumer protection with operational flexibility. However, the same approach cannot be applied to AI regulation. While GDPR provided a conceptual foundation for privacy, the EU AI Act is fundamentally different in both scope and design. It relies on centralized oversight (at the Union and Member State level), detailed pre-market conformity assessments, and risk classifications that are difficult to reconcile with the U.S. model of state-driven, sector-specific policymaking. Attempting to replicate that system would slow innovation, create jurisdictional conflicts, and undermine the agile governance that has made state privacy frameworks effective and interoperable.
- **<u>Economic and Innovation Consequences</u>**: The EU's experience also provides an economic cautionary tale. According to the European Central Bank, business investment in the euro zone grew by only 6.8% between Q4

2021 and Q4 2024, compared with 15.4% in the United States over the same period. A separate ECB analysis found that labor productivity per hour worked increased by just 0.9% between Q4 2019 and Q2 2024, underscoring Europe's stagnant productivity. Likewise, the Bank of Finland reports that venture-capital investment in the euro zone averages about 0.2% of GDP, less than one-third of the 0.7% of GDP seen in the U.S. Together, these data points reflect how Europe's highly prescriptive regulatory model has coincided with slower business investment, weaker startup formation, and limited capital flow into emerging technologies. The lesson for the United States is clear: while our states successfully transformed GDPR principles into a balanced and flexible privacy framework, the EU's approach to AI regulation cannot—and should not—be copied. Instead, the U.S. should pursue a pragmatic, outcomes-based framework that safeguards consumers while enabling innovation, competition, and accountability.

- **Conclusion**: The U.S. and New Mexico should forge a path that is interoperable with other state frameworks. And the good news is, we already have the building blocks. We can build on the state privacy frameworks already in place, rely on principle-based and flexible rules that adapt as technology evolves, and prioritize interoperability so businesses can comply across states without a tangle of conflicting requirements.

III. FINDING CONSENSUS AROUND AI BEFORE REGULATING IT

Across the country, policymakers, consumer advocates, and companies are all struggling to agree on what counts as "AI." There is no shared definition for terms like *artificial intelligence system*, *automated decision-making*, or *high-risk AI system*. Nor is there alignment on who bears responsibility for outcomes—the entity who builds the model or the business that uses it. Every state is trying to solve the same problem, but the answers vary dramatically.

In Texas (HB 149), Iowa (HF 406), and Minnesota (SF 1886), lawmakers have defined AI to covers any technology that "infers from inputs how to generate outputs influencing physical or virtual environments." On paper, that sounds straightforward, but in practice it could sweep in everything from ChatGPT to a spell-checker or chatbot.

Other states have proposed legislation to narrow the focus. Massachusetts (HB 94), Connecticut (SB 2), Nevada (LB 642), Virginia (HB 2094), and New York (AB 768) all center regulation on *high-risk systems*. In Massachusetts, that includes systems that materially influence hiring, housing, health-care access, or education outcomes. Nevada uses the phrase "material legal or similarly significant effect." Connecticut ties the definition to decisions with significant legal, financial, or personal impact. Virginia's approach goes further, covering any system that autonomously makes—or is a substantial factor in making—a consequential decision. In practice, that could mean an algorithm that screens job applicants or prioritizes patients for limited medical services, even if a human ultimately confirms the result.

Differences also extend to who is regulated. The Colorado AI Act (SB 24-205) and bills in Virginia (HB 2094), Nevada (LB 642), and New York (AB 768) all adopt a two-tier structure: developers, who create or substantially modify AI systems, and deployers, who use them to make decisions about consumers. That model reflects a growing consensus that accountability should follow each link in the AI supply chain. Still, the exact duties vary. Some states require developers to provide documentation and risk assessments; others require deployers to notify consumers or conduct annual impact reviews. Texas, by contrast, embeds AI obligations within existing biometric and data-privacy statutes, avoiding a separate framework altogether.

The lack of uniformity has already produced mixed results. For example, Connecticut's SB 2 and Virginia's SB 2094 were stalled and vetoed, respectively, amid disputes over scope and accountability. In vetoing SB 2094, the Governor emphasized that existing laws already protect consumers and regulate discrimination, privacy, data use, and libel. He noted that the bill's rigid framework fails to reflect the fast-moving nature of the AI industry and would impose especially heavy burdens on smaller firms lacking large compliance teams.

Colorado's AI Act, meanwhile, was passed in just thirty-seven days, making it the first comprehensive state law regulating AI. Governor Jared Polis signed it, but he did so "with reservations." In his signing statement, he made it clear that the bill moved faster than the understanding behind it. He warned that the law created a complicated compliance system for both developers and deployers of AI and that its broad duties could confuse everyone—from small startups to large technology companies—if key definitions weren't refined before it took effect. The Governor also cautioned against the rise of a state-by-state patchwork, saying that consumer protections are essential but are "better considered and applied by the federal government" to ensure consistency. His message was straightforward: take the time to get it right.

And his concerns proved right. Earlier this year, Colorado returned to the issue with SB 25B-004, a follow-up measure that was supposed to clarify the AI Act. Instead of fixing the problems, lawmakers simply delayed the effective date to June 30, 2026. None of the big questions Governor Polis identified were resolved. So now, Colorado is both the first state to pass a comprehensive AI law and the first to postpone it while trying to figure out how to make it work.

That experience carries an obvious lesson. When legislation moves faster than the policy consensus behind it, the result isn't clarity—it's confusion. Governor

Polis's warning rings true: take the time to understand the technology, build consensus, and create a framework that actually works in practice.

For New Mexico, a pragmatic approach would serve the state far better. Instead of racing to pass an AI bill before those foundational questions are answered, New Mexico could follow the lead of Montana's House Joint Resolution 4 and Oregon's HB 4153, which established bipartisan workgroups to study AI's social, ethical, and economic implications before proposing new laws. Both states recognized that sound policy begins with education—bringing together technologists, consumer advocates, businesses, and lawmakers to define key terms, identify real risks, and understand where existing law already applies. By taking the time to study before regulating, New Mexico can protect consumers, foster innovation, and avoid the kind of uncertainty that even Colorado is still trying to sort out.

CONCLUSION

In closing, New Mexico has an opportunity to take a measured, forward-looking approach to AI policy. Building on comprehensive data privacy protections first will create a clear, interoperable foundation for any future AI regulation. By defining terms carefully and learning from the challenges other states have faced, New Mexico can avoid a patchwork of conflicting rules and instead craft a framework that safeguards consumers while supporting innovation.

Thank you, Madam Chair and Members of the Committee, for the opportunity to testify today. I would be happy to answer any questions.