House Chair Tricia Farley-Bouvier
Senate Chair Michael Moore
Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
Massachusetts State House
24 Beacon St. Room 274
Boston, MA 02133

Statement

of

Matthew Mittelsteadt

Technology Policy Fellow

Cato Institute

For the

Massachusetts Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity

September 11, 2025

Re: Bills Related to Artificial Intelligence and Algorithms

House Chair Tricia Farley-Bouvier, Senate Chair Michael Moore, and distinguished members of the Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity:

My name is Matthew Mittelsteadt, and I am a technology policy research fellow at the Cato Institute. My research focuses on policy questions surrounding emerging technologies like Artificial Intelligence (AI).

While promoting consumer safety is the clear and noble goal of many AI legislative proposals, policymakers must weigh not only the direct safety outcomes of these rules but also the potential downstream risks to consumers if the regulations prove overly burdensome or contribute to a fragmented, multi-state regulatory patchwork.

In this statement for the record, I'd like to emphasize two consumer safety risks policymakers should consider as they attempt to strike balance in their AI legislative work:

- **Confused AI Transparency**: AI product transparency indeed holds natural consumer and safety benefits. If inter-state AI product transparency rules clash or are misaligned, however, differing standards, measures, and conclusions could counterintuitively decrease transparency.
- **The Denial of Safety-Enhancing AI Technologies:** Many of the most critical emerging AI use cases involve automating tasks humans and consumers have failed to manage safely. If regulations are overburdensome, or further a multi-state regulatory patchwork, these benefits could be denied, and lives could be lost.

Confused AI Transparency

Today, algorithmic transparency rules are perhaps the most common denominator across state AI regulatory proposals. To the credit of legislators, transparency can indeed help minimize safety concerns. With solid data, consumer choice can be better informed and AI safety risks appropriately managed. Such benefits, however, depend on data being clear, simple, and ideally aggregated. If a patchwork of conflicting state rules emerges, we risk nurturing the opposite. From a multitude of transparency regulations will naturally spring a

confusing collage of differing standards, measures, and conclusions. For consumers, *more* transparency rules could counterintuitively yield *less* transparency.

Given current AI reality, such unharmonized state transparency rules are likely. In industry, there is currently little consensus on measuring "AI ground truth." A first challenge is definitional: what even is AI? Because AI is not a specific technology but more a general notion or goal, there are hundreds of possible definitions and limited regulatory consensus. This opens a wide door to policy diversity and challenges a consistent approach to regulatory scope across states.

A second difficulty is measurement. Evaluation obsolescence is a persistent industry challenge: almost as soon as evaluation criteria are introduced, they are rendered moot by shifts in the technical landscape. As a result, gold standard metrics are in constant flux and ballooning in number as experts introduce countless would-be replacements to attempt to fill the void. Such a unique swirl means any transparency regulations passed by Massachusetts are almost certain to measure and report inconsistently with competing states.

These realities are a breeding ground for consumer confusion and perhaps an opening for consumer harm. If definitions of AI are inconsistent, for instance, it's easy to imagine a consumer in state-straddling Fall River seeing a service labeled "AI" on one block and "not AI" a few streets over. Likewise, if states create a mess of uneven evaluations, consumers are sure to misinterpret safety data, or worse, tune out evaluations altogether.

Unlike a unified national approach, fragmented consumer transparency regulations naturally invite conflict and confusion. As more states inaugurate clashing consumer transparency rules, AI clarity may be the casualty.

Denial of Safety-Enhancing Technologies

A second, more significant risk is the denial of safety-enhancing AI technology. While AI is often pigeonholed as an efficiency driver, the most critical emerging use cases involve automating tasks humans have demonstrably failed to manage safely.

One example is cybersecurity. In 2024, the number of discovered software vulnerabilities surged 38 percent.[1] In 2025, meanwhile, the number of cyberattacks **grew** a remarkable 47 percent. As the volume of risks rapidly balloons, human defenders have failed to keep pace. The result has been a litany of real, physical harm. In 2024, a cyberattack on Change Healthcare left thousands of hospitals unable to process transactions. This forced delays in essential care such as chemotherapy and direct patient

[1] Adam Bannister, "CVE Surge: Why the Record Rise in New Vulnerabilities?," YesWeHack, January 2025

harm. It was also costly. According to the Massachusetts Health and Hospital Association, the average cost of this weeks-long cyber-attack for just 12 surveyed Massachusetts hospitals was $24,154,000 per day. [2]

Where humans have failed, however, defensive AI tools offer a glimmer of cyber hope. Early evidence suggests countless just-emerging AI tools can spot novel insecurities, write programming fixes, update flawed legacy systems, and autonomously detect attackers.[3] Perhaps the most promising safety opportunity is the potential for AI automated coding services to translate legacy software code written in cyber-insecure programming languages to modern "safe" versions.[4] Federal estimates suggest this use case alone could aid the elimination of up to 70% of cyber vulnerabilities. In a few short years—if not months—such safety enhancing AI could drive a digital safety revolution and prevent further harm.[5]

Driverless vehicles offer an even more compelling AI safety story. It's no exaggeration to claim human drivers are a safety liability. In 2023, there were 44,762 motor vehicle fatalities on American roadways and another 5.1 million crash-related emergency department visits.[6] Meanwhile in 2022, Massachusetts documented the most traffic fatalities in state history.[7] Against this safety crisis, safety enhancing AI may provide hope. According to recent data from Autonomous Vehicle firm Waymo, their vehicles have yielded 88% fewer "serious injury or worse" crashes and 79% fewer airbag deployment crashes.[8] A 2024 external study from Swiss Re, an insurer, has further corroborated these findings.[9] With such staggering figures, driverless cars could be the single biggest safety innovation in decades. In a matter of years, AI may all but eliminate this leading cause of death.

As your committee considers any new rules, I urge thoughtful caution. In both example cases, excessively burdensome regulation could halt this singular safety potential. These specific examples are also worth highlighting because their possibilities hinge on cross-state regulatory harmonization. In the case of cybersecurity, digital systems are often

---

[2] Alison Kuznitz, "Mass. Hospitals Feeling Fiscal Pinch from Change Healthcare Cyber Breach," WBUR News, March 12, 2024
[3] DARKNAVY, "Argusee: A Multi-Agent Collaborative Architecture for Automated Vulnerability Discovery," DARKNAVY, May 23, 2025,
[4] Matt Mittelsteadt, "Seizing AI's Trillion Dollar Cyber Opportunity," Cato.org, July 2025,
[5] "Memory Safe Languages: Reducing Vulnerabilities in Modern ...," NSA Cybersecurity Collaboration Center, June 2025
[6] "Motor Vehicle - Introduction - Injury Facts," National Safety Council Injury Facts, accessed September 11, 2025
[7] Christian MilNeil, "2022 Was Another Record-Breaking Year for Bloodshed on Massachusetts Roadways," Streetsblog Massachusetts, June 12, 2023
[8] Waymo, "Waymo Safety Impact," Waymo, 2025,
[9] Andrew J. Hawkins, "Waymo Still Doing Better than Humans at Preventing Injuries and Property Damage," The Verge, December 19, 2024

deeply integrated across jurisdictions, and therefore, safety success demands consistent tooling across state lines. If Massachusetts, or any one other state, inadvertently denies or limits essential AI security tools, it could create an unsecured weak point and easily spread attacks to all others. Interstate consistency is more essential in the case of driverless vehicles. If consumers or firms can't legally drive across states due to a patchwork, they simply won't use the technology. If rules are excessively unique, expansive, and complex, such safety costs will be hard to avoid.

Conclusion

Thank you for the opportunity to submit this statement. I welcome any further questions or the opportunity to further discuss my research related to issues of artificial intelligence, cybersecurity, and emerging technologies.