Bartlett D. Cleland
General Counsel and Director of Strategic Initiatives, NetChoice
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

Wisconsin Legislative Council Study Committee on the Regulation of Artificial Intelligence in Wisconsin

TESTIMONY

15 October 2024

Dear Chairman Bradley and members of the Wisconsin Legislative Study Committee,

NetChoice[1] is a trade association of leading e-commerce and online companies promoting the value, convenience, and choice of internet business models. Our mission is to make the internet safe for free enterprise and for free expression.

We work to promote the integrity and availability of the global internet and are significantly engaged in issues in the states, in Washington, DC, and in international internet governance organizations.

I want to thank the Chair, the committee and the Wisconsin legislature for giving NetChoice the opportunity to provide our point of view on artificial intelligence and how Wisconsin can benefit.

The Transformative Potential of AI

We are living in watershed years for generative artificial intelligence (AI) advancement. Weekly, we watch as AI's promises become reality. AI has the potential to profoundly enhance our lives across a wide range of domains, from healthcare and education to productivity and creativity. The applications just in health and wellness are incredible. Detecting cancer, identifying genetic markers for future illness, creating better medicines faster, lowering costs of healthcare and insurance, and assisting with improved communications for the hearing or speech impaired are just a few of more prominent benefits already underway. However, as with any transformative technology, AI introduces certain risks that we can carefully navigate.

Deepfakes, which are AI-generated synthetic media that features highly realistic yet false depictions of real people, exemplify both the potential benefits and dangers of AI. On one hand, deepfakes have many positive applications. In education, deepfakes could allow students to interact with historical figures or explore scientific concepts in immersive ways. In healthcare, they have great potential to aid in the treatment of Post Traumatic Stress Disorder. And in the arts, deepfakes open

[1] NetChoice is a trade association of e-Commerce and online businesses, at www.netchoice.org. The views expressed here do not necessarily represent the views of every NetChoice member company.

up new avenues for creativity and storytelling. Unfortunately, deepfakes can also be weaponized as tools for misinformation, fraud, and abuse.

However, before one can appropriately discuss the great potential or any necessary cautions about “AI”, it is important to understand exactly what is being discussed.

“AI” Might Not be What You Think

To keep it relatively simple, artificial intelligence can be sorted into three levels.

First, there are models that recognize and predict patterns by using algorithms to generalize unseen data, performing tasks without explicit instructions. This is most often referred to as machine learning and has been around and broadly used for more than 70 years. Today, one might encounter machine learning being deployed in facial recognition, SPAM filters, and predictive text. But machine learning AI also is hard at work in finance, health care, and social media optimization.

Next, there is generative artificial intelligence and is generally what is discussed today as “AI.” Generative AI creates new content from human input. These models adapt and learn within the parameters of their programming, training on our documents to learn what words mean. We see and read much about music or works of art being created with such technology as prompted by an input that uses a large language model (LLM) from which to derive its “intelligence,” largely a function of probability, statistics, and information theory, not completely unlike their use in machine learning. Whether Gemini, Claude, or ChatGPT, all are driven by generative AI in the same way.

Artificial general intelligence is the third category. This is Rosie the Robot from the Jetsons or the android Q on Star Trek: The Next Generation. This artificial intelligence matches or surpasses human cognitive abilities, and is still merely science fiction. Artificial general intelligence is not an inevitable result of a direct line from generative artificial intelligence. Whether such will ever exist remains a robust debate amongst philosophers, ethicists, computer scientists, theologians, and others.

Having at least this basic understanding of AI is critical for legislators and regulators. As policymakers grapple with the rapid advancements in AI and its potential impact on society, it is crucial to approach the regulation of this technology with care and precision. Imprecise definitions and overly broad language in AI-related legislation can lead to unintended consequences, stifling innovation and infringing upon free speech rights.

The Reality That AI is Already Heavily Regulated

There are hundreds of laws that govern AI today.

While some have called for extensive new regulations on AI, the reality is that this technology is already subject to a wide array of existing laws and regulatory frameworks. Any AI system must comply with the same rules as any other technology or business practice in its sector. Put simply, AI is just a tool. This means that AI applications in healthcare are regulated by HIPAA and FDA guidelines, AI in finance is subject to FCRA and ECOA, and AI in education must adhere to FERPA, to name a few examples. The notion that AI will inhabit some kind of lawless Wild West is simply false.

Elections are on everyone's mind, and whether AI could be used in a negative way to trick voters has been discussed. However, the federal government has already declared intentional lying about the time, manner, or place of an election to prevent qualified voters from voting a crime. Wisconsin too has its laws governing elections in this state. This means today, the government is free to prosecute individuals publishing deepfakes that seek to subvert election integrity. Moreover, existing consumer protection laws, such as the FTC Act's prohibition on unfair and deceptive practices, already provide robust safeguards against AI systems that might mislead consumers or otherwise cause them harm.

The FTC has made clear that it will vigorously police the AI industry under its existing authorities, and has already brought enforcement actions against companies for making misleading claims about their AI products or failing to secure sensitive data used in AI development. At the same time, broadly applicable anti-discrimination statutes like the Civil Rights Act, Fair Housing Act and Americans with Disabilities Act all constrain the use of AI in high-stakes domains like employment, credit and housing to prevent disparate impacts. Finally, existing defamation and false light torts will protect the subjects of deepfake media from reputational harm.

To be clear, this is not to say that every conceivable AI harm is perfectly addressed by current law, or that thoughtful, targeted updates may not be warranted in certain areas. But the core frameworks for regulating the responsible development and use of AI are very much in place today. Policymakers and the public can take comfort in the fact that our existing legal structures are, by and large, well-equipped to prevent and remedy the highest-risk AI failures. This comfort will continue as laws, or regulations, focus on specific behaviors and outcomes rather than broad categories of tools. This approach will ensure that the law can adapt to the rapidly evolving AI landscape while still protecting the rights and interests of individuals and society as a whole.

Before rushing to pass sweeping new AI-specific regulations, we should think carefully about how they would interact with this dense, overlapping web of existing rules. The goal should be to strategically fill discrete gaps, not to create a redundant layer of AI law that could impede innovation while adding little marginal protection for the public. In this, Wisconsin has provided a good example to itself, and to others, already.

Mitigating Harms and Consumer Protection

As with any other technology and tools, bad actors will predictably abuse AI to harass women, sexually exploit minors, to attempt to undermine public trust in our democratic processes. Law enforcement already reports that abusers are using AI tools to generate realistic depictions of real children in sexual situations, then arguing in court that since the explicit images were "AI-generated," they skirt existing child pornography laws. Elsewhere, criminals are using deepfake technology to falsely depict adults in compromising, sexual situations to extort, defame and intimidate victims.

Though amendments to existing laws may be appropriate to capture harms wrought by deepfake technology under certain circumstances, the vast majority of malicious deepfake uses are already illegal under existing statutes. Laws against harassment, defamation, fraud, identity theft, and copyright infringement all apply to deepfakes, just as they do to any other content. And election laws barring deceptive practices and voter manipulation encompass deepfakes aimed at election interference.

Wisconsin understood the need to address the gaps in the law, and did so in a targeted way. NetChoice applauds this action and is supportive of similar model law.

The Stop Deepfake CSAM Act
First, the Stop Deepfake CSAM Act would clarify that harmful AI-manipulated sexual images exploiting real minors are unambiguously illegal under existing federal child pornography statutes. Specifically, it would amend the definition of child sexual abuse material (CSAM) to include any visual depiction of a minor engaging in “actual or simulated” sexual conduct, where a criminal has used AI tools to “modify” sexually explicit material to include recognizable features of a real child.

This would prevent abusers from escaping accountability through the perverse argument that digitally manipulated CSAM gets a free pass.

The Stop Non-Consensual Distribution of Intimate Deepfake Media Act
Second, the Stop Non-Consensual Distribution of Intimate Deepfake Media Act would update privacy laws to expressly cover identifiable deepfake media shared with intent to harm. It would make it unlawful to distribute a deepfake depicting a non-consenting person engaging in fabricated sexual conduct with intent to coerce, harass or intimidate. This would close a loophole that allows deepfake harassment and exploitation to slip through the cracks.

Importantly, both bills include robust safeguards for constitutionally protected speech. They explicitly exempt works of political commentary, criticism, satire or parody. And they provide a safe harbor for digitally manipulated media that includes a clear disclosure that the content is synthetic. These are the kinds of narrowly tailored legislative updates we need to combat discrete deepfake harms without chilling legitimate expression.

At the same time, these laws alone are not a panacea. To fully address the deepfakes challenge, we also need to equip law enforcement with the expertise and resources to pursue cases involving malicious synthetic media under existing legal frameworks. But by strategically closing loopholes while avoiding rushed, overbroad bans, we can mitigate the worst abuses of deepfakes without stifling innovation.

Appropriately, Wisconsin moved to put both protections in place to make sure that the use of AI could not edge around the current law.

Technology detecting AI generated material
A topic that does not receive enough attention is the ability of technology to detect AI use. More specifically the ability of AI to detect AI use is already well established.

Many software products detect the use of AI. These detectors work by examining sentence and paragraph structure as well as word choice. After the examination the probability that some text is AI generated will be generated. Similar software has been developed to identify AI images.

This sort of advance in technology, to limit or eliminate concerns about new technology, is a great example of the market addressing consumer's needs. Heavy regulation or misguided legislation could easily interrupt AI solutions to AI challenges.

Privacy

AI systems often require large amounts of data for training and operation, which raises concerns about how personal information is collected, stored, and used. Ethical collection, storage and usage have all been raised as part of the ongoing discussion.

Last year, the Wisconsin House took an important step in addressing these concerns by passing the Wisconsin Data Privacy Act. The law provides provisions for the collection, storage, use, and disclosure of personal information, and provides businesses and consumers with a legal framework for data security and privacy protection. However, the effort failed in the Senate.

The likely reintroduction and then the complete implementation of the law and its ongoing operation will be closely watched.

Principles for Trustworthy AI Development

To fully realize AI's positive potential across domains, we must proactively mitigate serious but avoidable negative impacts. But we can do this without heavy-handed government control that could jeopardize America's position as a global leader in AI innovation.

Instead of rushing to restrict AI development itself, policymakers should establish guidelines and incentives for the trustworthy development and deployment of AI systems, focused on three core principles:

Transparency
Organizations should commit to disclosing when AI is being used and for what purposes, empowering individuals to make informed decisions about engaging with AI systems. Where AI materially shapes outcomes for consumers, additional context about the key factors influencing the AI's decisions may be warranted.

Accountability
AI should be subject to the same rules and liability structures as any other tool. Existing laws, from non-discrimination statutes to product liability and privacy frameworks, already provide robust accountability mechanisms. The key is ensuring these laws are vigorously enforced in the AI context.

Security
Rigorous safeguards should be in place to protect the sensitive personal data used to train AI systems from breach or misuse. AI developers must employ state-of-the-art cybersecurity and data governance practices to preserve privacy and prevent AI from amplifying societal biases.

Conclusion

We believe the key to addressing challenges while unlocking AI’s full potential is to pursue a balanced, multi-stakeholder approach. Strategically updating existing legal frameworks for the digital age and encouraging voluntary industry initiatives around transparency, accountability and security is the best option.

AI is not a force to be feared, but a tool to be harnessed wisely in service of democratic values and aspirations. With the right governance frameworks and social norms in place, the United States, and Wisconsin, can and must retain our global leadership in this critical technological domain. Ceding the AI race to less open societies would not only forfeit the profound benefits for American consumers and businesses, but leave the future trajectory of this powerful technology in the hands of authoritarian regimes.

The choices we make today about how to approach AI governance will shape the fabric of American competitiveness, security and liberty for generations to come. We urge Wisconsin to continue on the path it has most often chosen, to address outcomes of laws not regulate or ban technology and innovation.

Thank you again for the opportunity to share our perspective on these critical issues. We look forward to continuing this important dialogue. As always we offer ourselves as a resource to discuss any of these issues with you in further detail, and we appreciate the opportunity to provide the committee with our thoughts on this important matter.

Sincerely,

Bartlett D. Cleland
General Counsel and Director of Strategic Initiatives
NetChoice