May 22, 2024

Senate Judiciary Committee
One Capitol Square
Columbus, OH 43215

RE: SB 217 – "Regards AI-generated products, simulated porn, identity fraud" (Oppose)

Dear Chair Manning and Members of the Senate Judiciary Committee:

The above six co-signed organizations take seriously the shared responsibility of protecting online users from harmful and unlawful content. Responsible digital service providers have already taken aggressive steps to moderate dangerous and illegal content, consistent with their terms of service. The companies deliver on the commitments made to their user communities with a mix of automated tools and human review. Doing so is an evolving industry practice: since its launch, the Digital Trust & Safety Partnership (DTSP) has quickly developed and executed initial assessments of how participating companies implement the DTSP Best Practices Framework,[1] which provides a roadmap to increase trust and safety online meaningfully.

We acknowledge the legitimate concerns of consumers and lawmakers regarding nefarious online actors, particularly those utilizing emerging technologies. However, as written, SB 217 risks creating confusion surrounding compliance and could potentially stifle innovation without effectively addressing the underlying issues that fail to hold accountable those engaging in illicit activities. We appreciate your consideration of our concerns as further detailed below.

[1] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/2021/02/18/tech-giants-list-principles-for-handling-harmful-content.

Proposals regulating the use of AI systems should adopt a risk-based approach, prioritizing the development of protections against tangible harms.

SB 217 is not limited to high-risk cases, but instead, is targeted towards any AI-developed product. Due to the current ever-changing landscape of artificial intelligence, it is imperative to limit regulation on specific known harms. For instance, responsible digital service providers are proactively implementing safeguards to swiftly remove illegal or dangerous content like AI-generated images depicting CSAM, or inaccurate election information, such as AI-generated images showing false claims suggesting voters can text their ballots for the presidential election. Therefore, regulating narrowly tailored uses of such AI-generated content could be limited to specifics such as political advertisements for elections. By persistently addressing these well-defined and agreed-upon risks associated with AI-generated content, platforms foster an environment conducive to harm mitigation without impeding the innovation ecosystem, while providing technologically feasible and precise guidelines.

Limiting watermarking and labeling requirements to high-risk applications of AI-generated content also serves another purpose – protecting against counterproductive unintended consequences. For example, there are the risks of "notification fatigue" or "banner blindness," where users begin to ignore labels as they become more pervasive. This has been prevalent with website operators' attempts to comply with the EU's General Data Protection Regulation's website cookie disclosure requirements, which showed that overly broad disclosure obligations can be highly disruptive while providing limited consumer safety benefits.

Certain requirements in SB 217 are not currently feasible with available technology.

Under SB 217, "artificial intelligence systems" are required to be programmed to provide a distinctive watermark on any "AI-generated product" that informs the user that the particular product was generated using an "AI system." Currently, not all AI systems can be programmed to generate a watermark on every AI-generated product. Providing an AI watermark may not be technologically feasible in situations where the AI-generated content lacks sufficient detail or clarity, making it challenging for the watermarking algorithm to embed the watermark effectively without distorting or damaging the content. Additionally, if the AI-generated content is continually evolving, it can pose difficulties in accurately watermarking the content in real-time. Moreover, if the AI-generated content is distributed across platforms or systems that do not support watermarking integration, it can further limit the feasibility of implementing AI watermarks.

SB 217 raises questions about how to effectively watermark AI-generated text or voice responses. For example, when asked a question and provided a written response, a large language model (LLM) is unable to watermark AI-generated text. Connected devices like

Amazon Alexa or Google Home, which produce AI-generated voice responses, cannot watermark those voice responses. While we presume SB 217 aims to watermark AI-generated photos or videos, its current wording inadvertently covers a wide array of applications deemed as "AI products," such as delivery routes, resumes, background photos in advertising, broadcast football analytics, and film and music editing, among others.

To mitigate some of these dynamics, we suggest adding language to division (B) of Sec. 1349.10 such as *"to the extent that it is both technically feasible and commercially viable to do so."* Due to the significant civil penalties associated with violations in this section, this additional language allows for flexibility in cases where watermarking cannot be done.

Key definitions necessary for compliance should offer greater clarity to covered entities.

As previously mentioned, responsible digital services are already removing illegal and dangerous content pursuant to their terms of service and applicable law, including AI-generated images depicting CSAM. Nonetheless, it's important to acknowledge that no content moderation mechanism, including through human review or artificial intelligence, is infallible. Those who upload harmful material to any platform must be held accountable. Without a mechanism in place, bad actors will continue to perpetuate harmful content even if that content has been taken down in one instance on one platform. Therefore, we suggest amending the language to address nefarious users and hold them accountable, rather than solely relying on technology that may have limitations.

We propose adding language that clarifies that this section would not apply to "*the operator or deployer of artificially intelligent software designed for the production of imagery at the request of users where the content of such imagery is directed by the user, unless such software is especially made or especially adapted for, promoted for the production of, and/or intended to produce such matter.*"

To avoid creating a broad risk of liability, SB 217 should make clear that the knowledge standard under division (A) of Sec. 2907.321 is *actual* knowledge. As currently written, it remains ambiguous whether an individual could breach this provision merely by transmitting content deemed obscene or pertaining to an impaired person, regardless of their *actual* awareness. These concerns are further compounded by the vague definition of "impaired persons"—which seems to suggest that a person may be held liable unless they can accurately infer the mental state or intent of a third party—and the broad enforcement discretion provided in Sec. 2907.321 (B)(3) under which "the trier of fact may infer that a person in the material or performance involved is a minor or impaired person…".

To address these concerns, we suggest amending the language in division (A) of Sec. 2907.321 to "*no person, with **actual** knowledge of the character of the material or performance involved…*"

This suggested language clarifies that the operator or deployer of artificially intelligent software cannot be liable for the actions of its users unless such software is designed and intended to produce matter that depicts a person under 18 years of age personally engaging in sexual conduct. This additional language will provide sufficient immunity to generative AI operators/deployers to support further innovation while still ensuring that a tool that is both designed and intended to produce this type of heinous material is not immune from liability.

Ohioans would benefit from cybersecurity and antifraud measures.

Lawmakers should consider the private sector as collaborative allies in the fight against abhorrent uses of deepfake technology. This entails safeguarding entities from unwarranted liability associated with the collection or dissemination of specific materials aimed at detecting and preventing fraud or bolstering cybersecurity measures. This legislation, as drafted, does not offer these protections. Therefore, we propose adding cybersecurity and antifraud exemptions to clarify that the sharing of deepfake content for the purposes of cybersecurity or antifraud efforts is not considered the dissemination of the content, and hence, that entity would not be liable.

The private right of action would result in the proliferation of frivolous lawsuits.

SB 217 permits users to bring legal action against companies that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Ohio's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. This is especially concerning, as previously mentioned, given the vague definitions in SB 217 that are essential for businesses looking to achieve compliance. As lawsuits prove extremely costly and time-intensive, it is foreseeable that these costs would be passed on to individual users and advertisers in Ohio, disproportionately impacting smaller businesses and startups across the state.[2]

* * * * * *

[2] Trevor Wagener, *State Regulation of Content Moderation Would Create Enormous Legal Costs for Platforms*, Broadband Breakfast (Mar. 23, 2021), https://broadbandbreakfast.com/2021/03/trevor-wagener-state-regulation-of-contentmoderation-would-create-enormous-legal-costs-for-platforms/.

For the above reasons, we urge you to resist advancing legislation that fails to provide a meaningful compliance roadmap for covered services, while simultaneously not addressing the underlying pervasive issues that do not hold nefarious actors accountable. We look forward to continuing to work with the Committee on these important matters.

Respectfully submitted,

Chamber of Progress
Computer & Communications Industry Association (CCIA)
NetChoice
Software & Information Industry Association (SIIA)
Taxpayers Protection Alliance
TechNet