



NetChoice



Computer & Communications
Industry Association
Open Markets. Open Systems. Open Networks.



August 26, 2024

The Honorable Buffy Wicks
1021 O Street, Suite 8140
Sacramento, CA 95814

RE: AB 3211 (Wicks) – OPPOSE – As Amended August 23, 2024

Dear Assemblymember Wicks,

TechNet and the following organizations must respectfully oppose AB 3211 (Wicks), which sets overly prescriptive and technological infeasible requirements on developers of artificial intelligence (AI), large online platforms, camera and recording device manufacturers to incorporate content provenance and watermarking technology into their products.

TechNet, our coalition partners, and our member companies greatly appreciate the conversations we've had this year with you and your staff on this issue. While we made significant progress and appreciate the amendments that address some of our concerns, there are many issues left unresolved and unfortunately, we must maintain our opposition. We look forward to continuing this work next year as this technology, our understanding of its capabilities, as well as national and international standards on content provenance continue to develop. We outlined below some of our major concerns in anticipation of those conversations next year.

Federal Standard

While we understand the desire to regulate an emerging technology, this is an area that would benefit from Federal standards and regulation rather than a state by state approach. In President Biden's AI Executive Order, he tasked the Department of Commerce with "identifying the existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for: (i) authenticating content and tracking its provenance; (ii) labeling synthetic content, such as using watermarking; (iii) detecting synthetic content" and more. We believe in allowing this federal process to advance in order to establish standards that are "science-backed" and can be consistently applied across the country is important.

In the meantime, disclosure provides a meaningful way to alert consumers when they are interacting with AI-generated content. We would prefer an approach that prioritizes disclosure in the short-term while watermarking technologies are developing and able to advance to be deployed in a consistent and cost-effective manner down the line. Such an approach would allow consumers and businesses to

benefit from transparency and allow time for further innovation with regard to watermarking.

Overly Prescriptive Requirements on Content Provenance for 3rd Party Content and Camera Manufacturers are Technologically Premature

Many of our companies and platforms are at the forefront of developing content provenance and watermarking technology, which is still in its early stages. However, AB 3211 enacts incredibly prescriptive requirements for large online platforms to label and apply provenance data to all 3rd party content published on their platform. Scanning and affixing provenance data to all digital content at scale exceeds what platforms are capable of and in some cases what is even feasible. For example, this obligation for images may be close to technically feasible, but those capabilities do not exist yet for video and audio. The technology just doesn't have the accuracy and reliability yet that is required to justify mandating an obligation to detect and affix provenance data to every single piece of the millions of digital content that are posted every day.

AB 3211 also still imposes technically infeasible and commercially impracticable requirements regarding any "newly manufactured recording device." The state of the technology has not yet matured to enshrine this requirement in law at this time. There are only a handful of devices on the market today that have this capability, and it is unclear if there are any video cameras on the market with these capabilities. We would suggest a standard that is more permissive by requiring a manufacturer to provide at least one product or offering that allows users to incorporate provenance information into nonsynthetic content - rather than requiring it in every recording device. This more targeted approach would ensure that, if there are significant costs to developing and incorporating the technology, those costs don't have to be passed onto consumers that do not want them. Instead, consumers could choose this functionality, if desired, and the requirements could be phased in over time.

Disclosing Full Reports to the Department of Technology Could Jeopardize Security of GenAI Systems

While improvements have been made to the requirements around the bill's requirements for adversarial testing, our members have significant concerns about providing full reports of these exercises to the Department of Technology. Adversarial testing or red-teaming exercises are used to identify vulnerabilities by employing teams to probe a system's defenses and simulate attacks by malicious actors. What these exercises identify is incredibly valuable information, helping the company to identify and rectify its system's weak points. It's also incredibly valuable information for actual malicious actors, looking for information about where a system's vulnerabilities are and what a company is doing to mitigate them. We believe the bill should explicitly allow companies to redact sensitive information that could jeopardize the security or integrity of their systems. We would also suggest including a Public Records Act exemption and a confidentiality clause so that any sensitive information that is disclosed to the Department or any state

entity is protected. We agree with the bill's intent to increase transparency about the measures companies are taking to safeguard their systems, it just can't come at the expense of the security and integrity of those systems.

AI-Generated Content Isn't Inherently Bad

AB 3211 seems to treat all AI-generated content as inherently bad or risky. By requiring such thorough and prescriptive requirements for content labeling, the bill makes a value judgment consumers must be notified and aware of any content that was created by AI. While we agree with the intent to provide more information to consumers, in some instances it could create disclosure or notification fatigue. If watermarks and content credentials become so routine and placed on all content, whether AI-generated or not, users may start to ignore and disregard their presence. Rather than focusing on whether the content itself was AI-generated, synthetic, or inauthentic, we would advise focusing on the misuse of this technology.

Thank you for your consideration. If you have any questions regarding our opposition, please contact Dylan Hoffman, Executive Director, at dhoffman@technet.org or 505-402-5738.

Sincerely,



Dylan Hoffman
Executive Director for California and the Southwest
TechNet

Ronak Daylami, California Chamber of Commerce
Naomi Padron, Computer & Communications Industry Association
Carl Szabo, NetChoice