TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone 909.380.2783
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

March 18, 2025

Senator Nicole Cannizzaro
c/o Nevada Senate
401 South Carson Street
Carson City, NV 89701

Re: SB 263 - AI Child Sexual Abuse Material

Dear Nicole Cannizzaro,

TechNet is proud to support SB 263 on expanding the scope of existing laws against child pornography to include material made using artificial intelligence. We also want to flag concerns on liability for flagging or reporting child sexual abuse material (CSAM).

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

TechNet is supportive of efforts to update state statutes so that individuals misusing artificial intelligence (AI) to create, disseminate, and otherwise act upon CSAM can be prosecuted. TechNet members take multi-faceted approaches to combat CSAM on their services and in the world. While each company must determine the most effective measures for that company in light of its primary audience, the features of its products, and the technical options presented by its architecture, TechNet member companies collaborate and share know-how and tools to fight CSAM.

<u>Safety by design</u>
Addressing CSAM risks is especially effective in the development and design of AI models. Integrating safety standards into the design process helps to proactively anticipate possible threats and prevent them from occurring in the first place once the technology is deployed. TechNet members employ several strategies to do this, including responsible sourcing of training datasets. Having CSAM and other exploitative content in a training dataset increases the risk of AI models being able to generate this harmful content. As such, industry works to actively detect and remove CSAM from their training data, as well as reporting found CSAM to appropriate authorities. Another helpful safety standard is iterative stress testing, which is the process of working to understand the capabilities of an AI model to produce contraband results. Responsibly conducting structured, scalable, and consistent stress testing allows industry to take

their findings, feed solutions back into the AI model, and further train the model so that any potential gaps are filled in.

Deployment

TechNet members are also leading on the development and refinement of industry standards and technologies to fight against CSAM for deployed AI models. This starts with prohibiting CSAM and other exploitative materials entirely from products through terms and conditions, policies, and enforcement. However, industry also ensures that there are safety net solutions in place to respond to criminal and illegal activities. One such practice is hash matching, which uses a foundational technology in the child protection ecosystem allowing for CSAM to be turned into a unique string of numbers through an algorithm. Once CSAM has been turned into a hash, it is compared via algorithms, without users' content ever being seen, against a hash list of known CSAM. This not only allows for a more efficient and thorough review of CSAM, but it also helps to protect victims from being retraumatized. There are additional technologies used by industry, like machine learning classifiers, to discover novel CSAM that are not yet known, which helps discover child victims in need and grows existing hash lists.

Ongoing maintenance and innovation

It's crucial to remain vigilant on potential abuses of AI models by individuals. TechNet members take great care to monitor their platforms and detect such abuses. Whenever bad actors build models that are meant to generate CSAM, for example, we remove these from platforms and search results. Companies also partner with expert third parties who specialize in flagging violative content, including CSAM, so that companies' internal teams can review and address the content appropriately. Furthermore, innovation in this area is key for more efficient and effective solutions to preventing CSAM. TechNet members are heavily investing internally and with public and private partners on research and development, like new technologies that protect user content from AI manipulation.

Procedures with law enforcement

TechNet members assist and collaborate with law enforcement to combat CSAM. Federal law, 18 USC § 2258A, requires that online providers report instances of CSAM to the CyberTipline at the National Center for Missing and Exploited Children (NCMEC). When CSAM is flagged, it is converted to hash and reported NCMEC, they take in reports, assess them by comparing the reported material in hash format to a list of known hash CSAM to determine if the material is new or not, and then refer them to federal, state, local and international law enforcement for investigation.

After CSAM is reported to NCMEC, it is investigated by law enforcement. State and local law enforcement may have limited familiarity with the details of how different online services work and how to request assistance in an investigation. Many providers and companies maintain dedicated teams to handle data requests from law enforcement, including the ability to respond around the clock to emergencies involving imminent harm. In addition, providers may publish instructions for law enforcement seeking to serve legal processes or to understand what records may be available. Providers also provide training through in-person events such as trainings held at NCMEC, regional

Internet Crimes Against Children Task Force meetings, and at the Dallas Crimes Against Children annual conference which attracts thousands of law enforcement personnel.

After CSAM is reported to NCMEC, it is frequently investigated by law enforcement. State and local law enforcement may have limited familiarity with the details of how different online services work and how to request assistance in an investigation. Many providers and companies maintain dedicated teams to handle data requests from law enforcement, including the ability to respond around the clock to emergencies involving imminent harm. In addition, providers may publish instructions for law enforcement seeking to serve legal processes or to understand what records may be available. Providers also provide training through in-person events such as trainings held at NCMEC, regional Internet Crimes Against Children Task Force meetings, and at the Dallas Crimes Against Children annual conference which attracts thousands of law enforcement personnel.

To ensure that TechNet members' efforts in the fight against CSAM can continue, particularly as AI technologies continue to evolve, we respectfully request the addition of the language below in the sections of SB 263 where established liabilities are being amended to add AI or computer-generated depictions of a child:

No civil or criminal charge for violations under this Act may be brought arising from actions taken to prevent, detect, protect against, report, or respond to the production, generation, incorporation, or synthesization of child sex abuse material.

Additionally, TechNet would like to recommend a provision that would ensure that liability falls solely on the person creating, viewing, promoting, or distributing CSAM—regardless of whether the material is generated using artificial intelligence or any other means. To achieve this, TechNet proposes the following options, which it will use only if intermediaries face liability under the bill:

As such terms are defined in 47 U.S.C. § 230, an interactive computer service is not liable for content provided by another person in violation of this act.

Thank you for your consideration and your efforts on this important issue. We are glad to serve as a resource to you and your office. Please do not hesitate to reach out should you have any questions.If you have any questions or concerns regarding our position, please contact Jose Torres, Deputy Executive Director at jtorres@technet.org or 909-380-2783.

Sincerely,

Jose Torres, MPA
Deputy Executive Director for California and the Southwest