April 14, 2023

The Honorable Dave Cortese
1021 O Street, Room 6630
Sacramento, CA 95814

RE: SB 646 (Cortese) – Sexual exploitation – OPPOSE

Dear Senator Cortese,

TechNet and the undersigned organizations must respectfully oppose SB 646 which creates standards around the removal of child sexual abuse material (CSAM) and obscene content that can't reasonably be met, some of which run counter to established industry best practices and federal law. While our association and our member companies are supportive of the author's efforts to eradicate online sex trafficking, the distribution of CSAM, and nonconsensual intimate imagery (NCII or 'revenge porn'), these types of harmful content pose unique challenges and cannot be addressed appropriately through imposing liability on platforms that are actively combatting these problems.

Platforms Aggressively Combat Commercial Sexual Exploitation and CSAM
We have attached a detailed fact sheet to our opposition letter. That fact sheet outlines the myriad ways our member companies are actively engaged in the fight against commercial sexual exploitation and CSAM. TechNet member companies take multi-faceted approaches to combat CSAM and commercial sexual exploitation on their services by creating and sharing software detection tools as well as partnering with local, state, and federal law enforcement agencies and the National Center for Missing and Exploited Children (NCMEC). NCMEC takes in federally mandated reports from our companies, assesses them, and refers them to federal, state, local and international law enforcement for investigation. Through our partnerships and collaborations, TechNet members have made considerable investments and pioneered new technologies to fight CSAM.

Federal law, 18 USC § 2258A, requires that online providers report instances of child sexual abuse material (CSAM) to the CyberTipline at the National Center for Missing and Exploited Children (NCMEC). NCMEC takes in reports, assesses them, and refers them to federal, state, local and international law enforcement for investigation. In addition, the law also requires providers to retain important data related to their reports in the event of a law enforcement investigation.
Since the early 2000s, the tech industry has been involved in efforts to use hash values to detect items previously identified as violations, identify the legal changes necessary for sharing of hash values among companies and the NCMEC, and legal changes to allow the advancement of the next generation of detection technologies. In 2009, PhotoDNA, an image matching software that can detect known CSAM, was developed and donated allowing NCMEC to license it for no cost to entities who

want to use its fingerprint-analysis process to identify repeat versions of previously reported images. Additional detection tools have been developed such as Google's CSAI Match and TechNet member companies have donated technical and financial resources to modernize the CyberTipline and to develop tools for better tracking and coordination of investigations by law enforcement.

SB 646 would frustrate ongoing efforts to identify and remove CSAM that are required by federal law and informed by industry best practices

First, the bill's provisions treat CSAM and NCII in the same manner, even though CSAM requires special handling due to its highly sensitive nature, legal status as contraband, and federal reporting requirements. For example, the bill requires that all copies of the actionable material, whether it's CSAM or NCII, should either be destroyed or returned to the victim upon notice. Returning CSAM, even to the victim, would be a federal crime. Destroying CSAM would similarly violate federal reporting laws, which also require preservation of reported material, but would also hamper critically important efforts to detect and remove future re-uploads of prohibited material.

In collaboration with NCMEC, our companies use complex hashing software to detect and remove known CSAM. Destroying the material without reporting it to NCMEC to assign hash values to it would risk re-victimizing the children involved as well as exposing companies to significant penalties for violations of federal law.

Unworkable Requirements

Additionally, we believe the two-day window to remove, destroy, or return actionable material, though intended to inspire quick action, could have unintended consequences. First, focusing on the two-day window, rather than on federally mandated reporting and collaboration with NCMEC and law enforcement could negatively impact those processes and make those efforts less effective. Special handling requirements, as this bill imposes, diverts staff from other detection and reporting activities and may unintentionally slow down the process of addressing illegal content. In the case of CSAM, company transparency reports show that a large percentage of removals of this content occur before any user has viewed the content due to proactive efforts to remove such content.

Even in the context of revenge porn or NCII, the two-day window could frustrate the bill's intent. Currently, SB 646 requires companies to act within two days of a notice from a victim or face significant penalties. However, companies responding to user reports of violative content need time and sufficient information to verify the identity of the reporter as well as identify and remove the actionable material. Furthermore, our companies in good faith try to discern if the content was the product of coercion and determine whether the subject of the video or image was under 18. This type of careful analysis is impossible to conduct within two days. Thus, the two-day window would likely result in a dramatic over removal of content in response to user reports, whether they contain actionable material or not, simply because there isn't enough time to properly verify the report in good faith. This

combined with the broad definition of "actionable material" raises constitutional concerns about the capture and removal of content that could be legal and protected forms of expression.

Further, requiring a company to designate a named agent to handle notifications of actionable material is unworkable and would make it more difficult to moderate CSAM and NCII. Platforms use different reporting mechanisms that are specifically tailored to their users, the type of content on their platform, and the content at issue that a user wants to report. This bill would instead impose an unworkable system that will actually make it more challenging to address CSAM and exploitative content. The volume of content that is posted across social media platforms (hundreds of millions of pieces of content per day) means that having a single agent for these notices would dramatically impede platforms' ability to respond to these requests and undercut the purpose of this bill.

SB 646 will have a significant chilling effect on lawful speech and violates established First Amendment principles

As noted above, SB 646 raises several constitutional concerns and its overbreadth creates a significant chilling effect on lawful speech. For example, Section 2 of the bill creates a strong incentive to over-remove content any time a request is submitted. Platforms deal with millions of pieces of content every single day. If confronted with a notice to take down content, they will air on the side of caution and remove it due to the significant liability exposure. They will have no choice but to do this even if the content does not violate their policies because the risk is too high. Though well-intentioned, this bill will result in more lawful speech being removed and fewer online spaces for people to communicate and share ideas with one another.

SB 646 is preempted by Federal Law

Section 230 of the Communications Decency Act (47 U.S.C. §230) generally protects platforms from liability for content that users generate with limited exceptions. This protection enables platforms to host third party content and to moderate third-party content on their platforms without fear of liability.

Without the protections of Section 230, the internet ecosystem would be dramatically different with a limited ability for users to post, share, read, view, and discover the content of others.

Fortunately, Section 230 explicitly preempts state laws such as SB 646 that would conflict with this protection. This bill creates liability for platforms based on third party content. It would also impose liability for failure to remove content, which the Ninth Circuit has held falls squarely within the preemption of Section 230.[1] Therefore, by imposing liability on platforms for their moderation decisions SB 646 conflicts with Section 230 and is likely preempted.

[1] *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009)

Other states such as Utah, Arizona, Texas, and Florida have all tried to duplicate this type of content-related legislation. We encourage California not to join those states in undermining Section 230, the First Amendment, and jeopardizing a functioning internet.

Thank you for your consideration. If you have any questions regarding TechNet's opposition to SB 646 (Cortese), 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
Jaime Huff, Civil Justice Association of California
Khara Boender, Computer and Communications Industry Association
Tammy Cota, Internet Coalition
Carl Szabo, NetChoice