September 19, 2023

Governor Gavin Newsom
1021 O Street, Suite 9000
Sacramento, CA 95814

Re: AB 1394 (Wicks) – Social Media: Sexual exploitation– Request for Veto

Dear Governor Newsom,

TechNet, our member companies, and our coalition greatly appreciated the author's openness to discussing our concerns and policy alternatives throughout the year. We actively participated in good faith negotiations, drafted redlines, and offered amendments that would have secured our neutrality to the bill and resulted in the removal of more child sexual abuse material (CSAM) from the internet. Disappointingly, our proposals were rejected and the bill as amended still raises serious concerns regarding its implementation and ability to withstand legal challenges.

These concerns lead us to the conclusion that this bill falls short of its noble intent and could jeopardize the progress made this year as well as the work our platforms have been doing for years in combating CSAM. We believe this is a policy area that is too important to get wrong.

It is therefore that we respectfully ask that you veto AB 1394, allowing the Legislature more time to convene stakeholder meetings over the interim recess to fix the numerous issues that still remain and pass the strongest CSAM bill in the country next year.

TechNet and our coalition negotiated in good faith to strengthen AB 1394

Our associations and our member companies strongly support the author's efforts to eradicate online sex trafficking, the distribution of child sexual abuse material (CSAM), and nonconsensual intimate imagery (NCII). Our commitment, and our member companies' commitment, to fighting back against sexual predators is crystal clear: the internet, and any platforms on it, should not be a safe haven for these activities and criminals should be prosecuted to the fullest extent of the law.

On June 26, TechNet approached Assemblymember Wicks with good faith amendments that would 1) make AB 1394 workable from both a legal and policy perspective and 2) result in the removal of more child pornography. We asked to sit down and negotiate, expressed a clear goal of negotiating industry-wide neutrality, and proposed a series of meetings to work in that direction.

Since that time, we've had more than a dozen discussions and meetings with the author, sponsors, and other key legislative personnel, and those meetings resulted in substantial progress.

During that process we made numerous concessions and focused our efforts on providing sound policy alternatives that would result in more child pornography being removed from the internet. For example, despite our strong opposition to increased civil liability, our suggested amendments did not aim to strike the two private rights of action against platforms that fail to comply with the bill. Importantly, our amendments attempted to protect AB 1394 from likely First and Fourth Amendment challenges that could invalidate the bill or help perpetrators keep evidence out of court to avoid prosecution for their abhorrent crimes.

Despite weeks of progress and positive conversations with the author's office, negotiations ground to a halt in the last three weeks of session. Without any discussion and little rationale provided, the author decided to upend previously agreed upon provisions and move the bill further from consensus. As discussed below, not only did this change upend a tenuous agreement but it also made the bill more likely to be preempted by Federal law, an outcome we worked hard to avoid.

September 8 amendments make the bill more likely to be preempted by Federal law

Section 3 (g)(1) of AB 1394 prohibits platforms from "knowingly facilitating, aiding, or abetting commercial sexual exploitation." This section is intended to mirror the Fight Online Sex Trafficking Act (FOSTA, 47 U.S.C. §230(e)(5)(A))[1], which creates a narrow exception to the immunity from civil liability for online platforms provided by Section 230 of the Communication Decency Act (47 U.S.C. §230)[2]. Courts have upheld FOSTA's constitutionality[3], with the Ninth Circuit explaining that FOSTA requires actual knowledge, with a defendant knowingly benefiting from, knowingly assisting, or knowingly facilitating sex trafficking activities.[4] The Court also notes that "knowingly benefitting" still requires actual knowledge and a causal relationship between their affirmative conduct and receipt of the benefit.[5]

The recent amendments confusingly alter the "knowingly" intent standard, meaning an entity has knowledge if it has been notified of the presence of CSAM. Setting aside how constructive knowledge of *CSAM* is equated with actual knowledge of *commercial sexual exploitation*, this is wholly inconsistent with FOSTA's narrow exception to Section 230. If AB 1394 is signed into law, state plaintiffs would need to meet a *lower* bar than what the Ninth Circuit has held in *Reddit* would be required to recover under federal civil claims, which is entirely antithetical to

[1] Available at https://www.law.cornell.edu/uscode/text/47/230
[2] *Id.*
[3] *Woodhull Legal Foundation v. United States* (D.C. Cir. 2023) at page 28. Available at https://www.cadc.uscourts.gov/internet/opinions.nsf/EB820C51595100D6852589E50054A365/$file/22-5105-2006738.pdf
[4] *Does 1-6 v. Reddit, Inc., 51 F.4th 1137 (9th Cir. 2022)*
[5] *Id.* at 17.

Section 230. It plainly lowers the intent required to be found in violation of the bill, is clearly inconsistent with Federal law, and therefore, is likely to be preempted by Section 230.

This is not a result our coalition wants. Throughout the process we have proposed amendments in the hopes that this bill would successfully avoid a legal challenge after passage. Our coalition repeatedly raised this issue throughout the process and we were heartened when the author and Senate Judiciary Committee amended the bill to require a "knowingly" intent standard by striking "recklessly, or negligently" from the bill. While we were negotiating on amendments discussed below, the author worked out these changes with a limited group of stakeholders, only informing us about them after the decision had already been made to amend the language into the bill. Despite commitments in committee that this provision would not change, and our warnings about the bill's preemption issues if it was, this change invites a legal challenge that the state seems highly likely to lose.

Rather than agreeing to a state codification of FOSTA, which would have given victims the opportunity to sue platforms in state court, the author and sponsors seem determined to once again test well settled case law. It is worth remembering that in the event that this law is challenged or struck down, it will be of no benefit to victims.

Our proposed amendments protecting the bill against Fourth Amendment issues were rejected

As noted above, our coalition and members came to every conversation with the goal of creating the strongest piece of legislation in the country related to the removal of child sexual assault material from the internet. Our companies and their internal teams have many years' worth of experience not only designing new tools to combat CSAM but also creating new partnerships with victims' advocates, nonprofits, and law enforcement, which informed our engagement and negotiations. In recent years there have been more cases and precedents around digital searches and the Fourth Amendment that are relevant to this bill.

The Fourth Amendment not only prohibits the government from conducting unreasonable searches and seizures without a warrant but has been interpreted to prevent the government from deputizing private actors, such as online platforms, to conduct warrantless searches.[6] Obligations imposed upon a private party by statute can transform the private party into a government agent when it conducts searches as a result of the statute. For example, in *United States v. Ackerman*,[7] the Tenth Circuit Court of Appeals held that the National Center for Missing and Exploited Children was a government agent as a result of the federal statutes imposing obligations with respect to the operation of the CyberTipLine and CyberTips. The court further held that NCMEC's search of the defendant's email attachments,

[6] The Fourth Amendment prohibits warrantless searches that are conducted by private entities when they are acting as an agent or instrument of the government at the time they conduct the search. *See, e.g., Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994).

[7] *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016)

obtained via the CyberTipLine, therefore violated Fourth Amendment even when statute did not specifically require NCMEC to open and view those attachments because the statutory scheme "was more than enough to suggest both [legislative] knowledge of and acquiescence in the possibility that NCMEC would do exactly as it did here."[8]

Where a private party conducts a search while acting as a state actor, the search violates the Fourth Amendment, and courts will suppress the results of that search.[9] This means that evidence collected by AB 1394 could either be suppressed, thus making a prosecution more difficult, or if it was the subject of a conviction it could result in that conviction being overturned.

The last thing TechNet, our coalition, or our members want is for a criminal defendant to be able to overturn their conviction based on evidence collected as a result of this bill.

This area of law is still evolving but our associations and companies grappled with how best to achieve this bill's goals without leaving any room for criminal defendants to challenge their convictions. To that end, we proposed amendments that would clarify that platforms are not required to affirmatively search or scan for illicit material. We believe this amendment would help prevent Fourth Amendment challenges and ensure that the perpetrators of these heinous crimes remain behind bars.

This change was rejected with no explanation.

Our proposed amendments to incentivize the removal of more CSAM from the internet were rejected

In our initial conversations with the author, it was clear that the goal of AB 1394 was to make substantial progress in the fight to remove CSAM from the internet. With that goal top of mind, TechNet convened dozens of meetings with our member companies and a coalition of tech associations to work on substantive policy suggestions. As an example of how difficult this task is, we had several promising policies that we quickly realized were either unconstitutional, unworkable, or both. Legislating in this space is difficult and we did our level best to make sure there was no stone unturned.

We ultimately coalesced around creating an incentive for online platforms to join NCMEC's Take It Down program.[10] Similar to its CyberTipline, Take It Down is a

[8] *Id.* at 1302.
[9] *See, e.g.*, *United States v. Reed*, 15 F.3d 928, 933 (9th Cir. 1994) (holding that information gathered during search of hotel room by a hotel employee who was a government actor at the time of search should be suppressed); *United States v. Walther*, 652 F.2d 788 (9th Cir. 1981) (affirming suppression of evidence found during search by an airline employee when the employee was found to have been acting as a government agent at the time of the search); *Stapleton v. Superior Court of California*, 70 Cal. 2d 97 (Ca. 1968) (holding that evidence found during search of defendant's automobile by employee of a credit card company was inadmissible because employee was acting as a government agent at the time of the search).
[10] Available at https://takeitdown.ncmec.org/

new program through NCMEC, that allows victims to self-report CSAM and have it assigned a numerical hash value. Online platforms that partner with Take It Down then receive those hash values and begin identifying and removing all instances of that CSAM.

This incentive has numerous benefits, for victims and platforms alike. First, victims can report their material once, to a trusted, nonprofit entity that specializes in victim advocacy and support. They wouldn't have to go to each platform individually and make a report, as is required by AB 1394, saving them time and the pain of having to relive their abuse. Second, NCMEC and Take It Down operate across the internet and are not limited by borders. Meaning that an incentive in California law to join Take It Down that results in more companies participating would ultimately result in more CSAM being removed across the world, not just in California. This would benefits thousands, if not millions, of victims the world over. Third, using hash values to identify and remove CSAM is far more efficient than relying on user reports, resulting in quicker actions being taken to limit views and the spread of CSAM. Sexual abuse isn't limited to the taking of a picture or the upload; revictimization occurs every time CSAM is viewed and shared. The faster platforms are able to take action, the faster the abuse stops. Hash values and the system that underpins Take It Down and the CyberTipline are the fastest, most efficient means to removing CSAM.

Our suggested amendments containing this safe harbor were the result of countless hours of discussion amongst our members, with many difficult tradeoffs and considerations involved. For example, reasonable people disagree as to whether the incentive that we proposed crosses the line into state actor territory under the Fourth Amendment, as discussed above. Our members and companies debated this point and did our best to draft it in such a way as to avoid those issues.

We took feedback from the author and amended our language to include their concerns, adding in a timeline for downloading hashes and beginning the process for removing instances of hashed content. We also made clear that if a platform participating in Take It Down received a direct user report, the platform was still under an obligation to respond to that user's report.

In order to provide a true incentive for new and emerging social media platforms to join Take It Down, our suggestion was to create an alternative path to compliance, one that acknowledged the cost and difficulty of engineering a platform to receive and search content via hashes. Our suggestion precluded liability if a platform joined Take It Down and completed all six requirements we developed in consultation with the author.

The language that was instead amended into the bill only reduces penalties, it does not prevent liability. We believe this significantly undercuts the incentive this language provides and makes it less likely that new platforms will avail themselves of this alternative compliance and join Take It Down. This language falls disappointingly short of creating a true incentive and the progress that we had envisioned.

As previously noted, our suggestions, combined with the Fourth Amendment language above, would have removed our opposition and that of our coalition.

Numerous workability issues remain.
AB 1394 continues to suffer from a variety of avoidable problems that will impact its effective implementation. For example, AB 1394 requires platforms to collect personal information such as cell phone numbers and email addresses from victims in order to meet notice and update requirements. The bill counterintuitively does not allow a victim to request these notices and updates to be delivered via an on-platform method. This not only unnecessarily limits options for victims but also makes compliance incredibly difficult. Text and email responses are difficult to scale to potentially thousands of recipients. Automation is likely the only means to do so and will result in notices and updates with little individualized information. Furthermore, the bill's prohibition on utilizing a contact method that is "within the control of the social media company" would also prohibit a platform that controls and operates an email platform from using that email platform.

The bill also requires platforms to contact victims every seven days after their report has been made, regardless of whether a victim wants that regular contact or if there is any update to provide. We believe that creating more flexible compliance will benefit platforms and victims seeking to exercise their new rights under this bill.

These glaring issues have solutions but time has run out on this legislative session to address them. We believe with more time we could reach a consensus with the author and stakeholders and pass a superior bill.

Thank you for your consideration. If you have any questions regarding our opposition to AB 1394 (Wicks), 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
Carl Szabo, NetChoice