No. 24-171

# In The
# Supreme Court of the United States

COX COMMUNICATIONS, INC., ET AL.,
*Petitioners*,

v.

SONY MUSIC ENTERTAINMENT, ET AL.,
*Respondents*.

On Writ of Certiorari
to the United States Court of Appeals
for the Fourth Circuit

## BRIEF OF THE NATIONAL CENTER ON SEXUAL EXPLOITATION AS AMICUS CURIAE IN SUPPORT OF RESPONDENTS

Hyland Hunt
*Counsel of Record*
Dana Kaersvang*
DEUTSCH HUNT PLLC
300 New Jersey Ave., NW
Suite 300
Washington, DC 20001
(202) 868-6915
hhunt@deutschhunt.com

*Licensed in Colorado

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Cases**

**Statutes**

**Other Authorities**

## INTEREST OF AMICUS CURIAE[1]

The National Center on Sexual Exploitation (NCOSE) exists to build a world where people can live and love without sexual abuse and exploitation. With roots going back more than 60 years, NCOSE is a nonpartisan and nonsectarian non-profit that is leading the fight against all forms of sexual abuse and exploitation, including sex trafficking, child sexual abuse, and the distribution of child sexual abuse material (CSAM).[2] Tackling these issues from every angle, NCOSE's efforts encompass a grassroots network, research institute, training team, global coalition, and embedded litigation center—the NCOSE Law Center. The Law Center promotes and participates in key, precedent-setting cases and advocates in state and federal legislatures to advance policies to prevent sexual harm and aid those who have experienced it.

Technological advances have made NCOSE's work ever more urgent. The modern internet has resulted in an explosion in the amount and brutality of child

---

[1] No counsel for any party authored this brief in whole or in part. Other than amicus curiae or its counsel, the Recording Industry Association of America made a monetary contribution intended to fund the brief's preparation and submission.

[2] While some refer to this material as child pornography, NCOSE uses the term "child sexual abuse material" or "CSAM" because it better captures the harmful nature of the material. *See* Nat'l Ctr. for Missing & Exploited Children, *Child Sexual Abuse Material,* https://tinyurl.com/2nwst88x (explaining the term CSAM "most accurately reflect[s] what is depicted—the sexual abuse and exploitation of children").

sexual abuse material—with almost 30 million incidents of child sexual exploitation reported in 2024 alone. *See* Nat'l Ctr. for Missing & Exploited Children, *2024 CyberTipline Report*, https://tinyurl.com/yk33pkw2 (CyberTipline Report).

The internet doesn't just make child sexual abuse material easier to make and distribute. It also increases the harm. When child sexual abuse material is posted and disseminated online, children are re-victimized as images resurface online. This impedes victims' recovery and causes additional long-term harm.

The NCOSE Law Center seeks to hold platforms accountable when they knowingly profit from the presence of child sexual abuse material on their sites. It is, for example, currently litigating a case seeking to hold Twitter (now X) accountable for refusing to remove a video of child sexual abuse material, despite being put on notice of the specific CSAM by the minor boy depicted and his family, while the images were viewed more than 150,000 times, retweeted more than 2,000 times, and circulated through the boy's school, causing him to become suicidal. *See Doe v. Twitter, Inc.*, 148 F.4th 635, 2025 U.S. App. LEXIS 19406, at *6-*8 (9th Cir. 2025). In an email communication with the boy, Twitter informed him directly that it had reviewed the video depicting him and would not be removing it from the platform. *Id.* at *7. It was not until the Department of Homeland Security got involved that Twitter finally removed the CSAM. *Id.*

The Ninth Circuit nonetheless held that it "does not suffice to state a claim" that "Twitter profits from all the posts on its website, it knew the posts at issue

here contained child pornography, and therefore it knowingly benefited from a child-pornography trafficking venture." *Id.* at *15. The NCOSE Law Center is preparing a petition for certiorari seeking review of that decision.

So why is NCOSE here, in a case about copyright? Simple. Petitioners and their amici have attempted to make this case about something more: a blanket rule that internet platforms or services (of any kind) can never be held liable (in any context) for so-called "inaction," *e.g.*, refusing to terminate a user for engaging in known illicit activities. *See* Pet. Br. 23-27; Br. for X as Amicus Curiae 7-12. Indeed, they contend the Court has *already* adopted such a rule, in *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023), and need only clarify that it applies to copyright. *See, e.g.*, Br. for X as Amicus Curiae 20-22.

But the Court has not done so, and should not do so here. *Twitter* eschewed any universal rules. Different claims (e.g., CSAM distribution, sex trafficking, copyright, data privacy, terrorism, etc.) reflect different common law (and state law) backdrops, congressional policies, and statutory standards. And internet services are not all the same, either.

All of these differences (and many more) matter to the scope of secondary liability—*i.e.*, liability imposed on party A for facilitating or assisting the wrongdoing of party B. NCOSE writes to urge the Court to decline the invitation to transplant *Twitter* into the copyright sphere. And similarly to make clear that its ruling here on the scope of contributory infringement is specific to the copyright context and does not extend to other contexts, not presented here, like the

enforcement of laws designed to prevent and redress the sexual exploitation of children.

## INTRODUCTION AND SUMMARY OF ARGUMENT

It would seem to go without saying that the Court has not already decided this case. But Petitioners and their *amici* insist that it has all but done so in a decision interpreting the scope of secondary liability under an antiterrorism statute, *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023). Specifically, they contend that *Twitter* set a rule that internet platforms can never be liable for what they call "inaction," *i.e.*, refusing to terminate users engaged (repeatedly) in known unlawful conduct. Not so.

*Twitter* itself disclaimed any intent to be setting a rule for all wrongs in any context. Nor could it have been so broad. It was applying a specific common law framework directed by Congress that (1) does not define the full scope of aiding and abetting common law; (2) does not itself set an ironclad no-liability-for-inaction rule (much less hold that it is "inaction" for an internet platform to continue to provide services to users it knows are using the services for illicit ends); and (3) is distinct from contributory infringement and other forms of secondary liability applicable at common law or under distinct federal statutes.

Even a brief examination of secondary liability outside of the terrorism context, including in copyright law, reveals key differences among the governing background common law principles and federal statutes. Inaction is sometimes culpable. Congress's enactments limiting liability for internet platforms in some contexts—and providing distinct causes of action in others—only reinforce that "no

liability for inaction" is not the right legal backdrop across the board. Plus, internet services differ from one another in ways that matter for assessing culpability. Petitioners' attempt to fashion blanket rules from a context-specific case would sweep all of these divergent federal standards aside.

The downside risk of adopting a blanket no-liability-for-inaction rule—and lack of fit—are at their zenith in the area of federal laws designed to protect children from sexual exploitation. A complex web of background common law principles, state law claims, and federal statutes govern these claims. The result is a divergence among lower court opinions addressing when and why internet platforms should be held accountable for facilitating child sex trafficking and the distribution of CSAM. The scope of that liability should be resolved in a case that presents that question—not pretermitted by the transplantation of inapt "rules" from a wholly different context. However the Court resolves the copyright question here, it should not import or adopt a purported blanket no-liability-for-inaction rule for internet platforms.

## ARGUMENT

### I. No per se rule immunizes internet platforms from secondary liability in every context where they facilitate known wrongdoing by refusing to exercise their authority to stop it.

Rules for secondary liability are nuanced and context dependent, informed by a host of different common law histories, statutory standards, and federal policies. Petitioners would sweep all of this aside in favor of blanket rules that govern liability for

internet services "[w]hatever the context, formulation, or label" of a claim. Pet. Br. 23. The distinct rules and standards applicable to different contexts cannot be blinked aside so easily.

### A. *Twitter* did not create a blanket rule applicable to all secondary liability involving internet services.

Declaring that "[c]ontributory infringement *is* aiding-and-abetting liability," Pet. Br. 2 (emphasis added), Petitioners argue that this Court's *Twitter* decision elucidates "common-law rules" for "aiding-and-abetting" that define contributory infringement liability. *See* Pet. Br. 26, 27-28, 30. Petitioners' *amici* make the point even more forcefully, contending that all the Court need do here is "clarify that [*Twitter*] applies to copyright." Br. for X as Amicus Curiae 20 (capitalization normalized); *see also* Br. for Google et al. as Amici Curiae 18-19.

Both erroneously understand *Twitter* to create two key "rules": Never, in any context, can there be liability absent "*active*" conduct "with the purpose of bringing about the wrong," meaning there can be no liability for what Petitioners call "failure to terminate a customer" for using the service for illicit ends. Pet. Br. 23-24. And "[p]roviding general-use technologies to the public is not culpable conduct," full stop, Pet. Br. 28.

As Respondents explain, this grasping at straws misunderstands what this case is about. Not inaction, or the mere provision of services to the general public, but a conscious choice to continue providing services to "specific users they *knew* were habitually using their services" to infringe because of the revenue they gained from those subscribers. Resp. Br. 33-34.

But even on its own terms, Petitioners' argument misunderstands *Twitter*. The Court in *Twitter* did not set out ironclad rules for all aiding and abetting liability (never mind all secondary liability) related to any internet service in all contexts. The Court disclaimed any such intent: "the concepts of aiding and abetting and substantial assistance do not lend themselves to crisp, bright-line distinctions." *Twitter*, 598 U.S. at 506. Other contexts in which internet platforms could be held secondarily liable for knowingly assisting, contributing to, or facilitating their users' wrongdoing raise distinct issues.

The *Twitter* decision unsurprisingly did not consider these other contexts. It is not the Court's practice to set forth bright line rules governing situations that are not before it. *See Bostock v. Clayton Cnty.*, 590 U.S. 644, 681 (2020) ("[N]one of these other laws are before us; we have not had the benefit of adversarial testing about the meaning of their terms, and we do not prejudge any such question today."). As Justice Jackson explained, "[g]eneral principles are not … universal," and the *Twitter* decision's "common-law propositions … do not necessarily translate to other contexts." *Twitter*, 598 U.S. at 507 (Jackson, J., concurring).

Consistent with the Court's focus on the specific question before it, the *Twitter* decision is limited in at least three ways.

**1.** *Twitter* addressed the context of aiding and abetting terrorism where Congress specified a particular governing framework.

Aiding and abetting law varies substantially by context. *See infra* Section I.B.1. The Court did not need to conduct an all-contexts survey because the

statute at issue in *Twitter* directed use of a single framework: the decision in *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983). *See* Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, §2(a)(5), 130 Stat. 852, 852 (2016).

The *Halberstam* decision, on which *Twitter* relied, recognized that it was not setting the outer bounds of aiding and abetting liability, noting that "[t]ort law is not … sufficiently well developed or refined to provide immediate answers to all the serious questions." *Halberstam*, 705 F.2d at 489. Among the open questions it acknowledged, but found no need to address, was the scope of circumstances where "silence and inaction alone can qualify as 'substantial assistance.'" *Id.* at 485 n.14. Although *Halberstam* elucidates some general principles of aiding and abetting liability—as does *Twitter*, applying *Halberstam*'s framework—it does not set out the doctrine's full metes and bounds. And depending on the context, *Halberstam* does not necessarily provide the proper framework for evaluating aiding and abetting claims, especially where Congress did not direct its use.

**2.** Even under the framework applied in *Twitter*, the two "rules" Petitioners attempt to divine are not ironclad.

Action is not an essential element of liability. "[I]naction can be culpable in the face of some independent duty to act." *Twitter*, 598 U.S. at 489. The Court recognized that "there may be situations" where "a duty exists" that "would require … communication-providing services to terminate customers after discovering that the customers were using the service for illicit ends." *Id.* at 501. The Court

also recognized the possibility that a "failure to stop ISIS from using these platforms" could be "culpable" on a "strong showing of assistance and scienter." *Id.* at 500. But it found that showing lacking on the allegations before it. *See, e.g.*, *id.* at 505.

As for the purported "rule" that providing services to the public can never be culpable, the Court noted that even a "provider of routine services" may aid and abet a "foreseeable terror attack" if it provides services "in an unusual way" or provides particularly "dangerous wares." *Id.* at 502. Thus, neither of the two "rules" Petitioners cite are in fact inflexible "rules," even within the *Twitter* framework.

**3.** Given that *Twitter* does not govern all aiding and abetting liability, it *a fortiori* cannot be read to govern all secondary liability claims involving internet services. Aiding and abetting is *one* "method by which courts create secondary liability in persons other than the violator of [a] statute." *Cent. Bank, N.A. v. First Interstate Bank, N.A.*, 511 U.S. 164, 184 (1994) (citation omitted), *superseded in part by statute*, 15 U.S.C. § 78t(f). It is not the only method. Other forms of secondary liability are similar, but not identical.

In *Twitter*, the Court interpreted a statute that expressly imposed liability on "any person who aids and abets, by knowingly providing substantial assistance," 18 U.S.C. § 2333(d)(2), thereby bringing "the old soil" with those common-law terms, *Twitter*, 598 U.S. at 484. Other federal statutes impose secondary liability using different terms. *See, e.g.*, 18 U.S.C. § 1591(e) (defining "participation in a [sex trafficking] venture" as "knowingly assisting, supporting, or facilitating a violation" of the sex

trafficking laws); *see infra* Section I.B.2. They therefore do not bring the same "old soil" examined in *Twitter*.

In other contexts, as for copyright, secondary liability is a creature of its own distinct federal common law. *See MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005). This law has its own standard, imposing liability on a party that "induces, causes or materially contributes to the infringing conduct of another." *See Gershwin Publ'g Corp. v. Columbia Artists Mgmt.*, 443 F.2d 1159, 1162 (2d Cir. 1971); *Grokster*, 545 U.S. at 930 (citing *Gershwin* for the contributory infringement standard). As explained below, secondary liability under other statutes or doctrines not addressed in *Twitter* reflects distinct federal policies and interests that must be considered in assessing the scope of liability for internet platforms and services. The Court should decline Petitioners' invitation to transplant *Twitter*'s guideposts into a context where they don't belong.

### B. The scope of secondary liability involving internet services differs by context.

The blanket secondary liability shield proposed by Petitioners cannot be found in *Twitter* because it cannot be squared with the law. The common law of aiding and abetting varies by context. Statutory standards and federal policies for other types of secondary liability vary, too—including for copyright. On top of that, different internet services work differently. There is no one-size-fits-all answer—much less one-size-fits-all immunity for internet platforms.

**1.** The scope of "aiding and abetting" liability is not uniform across tort law. *See* Richard C. Mason, *Civil Liability for Aiding and Abetting*, 61 Bus. Lawyer 1135, 1137 (2006) (describing the "doctrine's many variations"); Sarah L. Swan, *Aiding and Abetting Matters*, 12 J. Tort L. 255, 258 (2019); *see also, e.g.*, Nelson S. Ebaugh, *Why You Should Understand the Five Tests of Civil Aiding and Abetting in Texas*, 78 Tex. Bar J. 362 (2015) (describing five distinct tests under Texas law). A full discussion of this variation would be far afield from this case. The crucial point here is that inaction is sometimes culpable.

Courts "have started to embrace and expand the idea that a failure to act can, in some circumstances, constitute substantial aid for the purposes of aiding and abetting liability." Swan, *supra*, at 258. Spectators—silent or not—have been held liable because "the presence of appreciative others is a large contributor to the existence of the wrong." *Id.* at 276; *see also Halberstam*, 705 F.2d at 485 n.14 (describing a case where a police officer's silence encouraged his partner to physically attack someone). Similarly, "silence and inaction in the face of knowledge [of] fraud" could culpably assist the fraud, even sometimes in circumstances where the aider and abettor does not have a duty to disclose. *Halberstam*, 705 F.2d at 485 n.14; Mason, *supra*, at 1157-58.[3] The failure to stop wrongdoing may also be culpable in

[3] *Halberstam* discussed securities fraud cases. 705 F.2d at 485 n.14. The Court subsequently held that there is no private cause of action for aiding and abetting in that context. *Cent. Bank*, 511 U.S. at 177. But the same principles apply in other contexts involving fraud and business torts. Mason, *supra*, at 1136-37.

some scenarios where the aider and abettor has the authority to stop the wrongdoer. Swan, *supra*, at 272-74 (describing cases involving supervisors who fail to take any action to correct supervisees' known harassing behavior).

Liability for failure to stop wrongdoing does not rest on a finding that the person with authority consciously wanted the tort to occur; most States impose no such requirement. *Id.* at 278 & n.155. Rather, the reasoning rests on the principle that the refusal to take action regarding known wrongdoing may cause the wrongdoer to believe that the wrong is tolerated, thereby encouraging the behavior. *See id.* at 272-74. This reasoning fits with common experience, where we distinguish between the failure to stop something and the refusal to stop it. Why? Refusal—especially by someone who had the authority and capacity to halt known wrongdoing and did nothing—sends a message about the (non)wrongfulness of the conduct; failure doesn't. It is all the more culpable when someone refuses to stop wrongdoing because they profit from it.[4] In short, not all "inaction" is treated the same, even under the general law of aiding and abetting. Context matters.

**2.** Broadening the lens to federal law that imposes or recognizes similar—but not identical—forms of

---

[4] The dynamic where horrific wrongdoing drives revenue is sadly ever-present in the context of internet-facilitated sexual exploitation of children. *See infra* Section II.A. Given the revenue at stake, if so-called "inaction" were shielded wholesale from liability as Petitioners urge, the upshot would be to incentivize internet platforms to amplify child sexual exploitation rather than to take the simple steps available to them to shut it down.

secondary liability, context matters even more. There are several contexts where issues might arise regarding an internet platform or service provider's liability for facilitating or assisting wrongdoing. Among them are terrorism (as in *Twitter*), copyright (as here), distribution of child sexual abuse material, sex trafficking, data privacy, and no doubt many others. Each area has its own unique set of federal statutes, policies, and interests, which collectively defeat any attempt to set a for-all-contexts rule that "inaction" can never support secondary liability.

**a.** Start with copyright. This brief will leave extensive discussion of the federal common law of contributory infringement and the standards reflected in the Digital Millenium Copyright Act (DMCA) to the copyright experts. *See, e.g.*, Resp. Br. 22-28; Br. for Am. Intellectual Property L. Ass'n as Amicus Curiae 6-12. It suffices here to note that contributory infringement has developed as a distinct body of law that has long recognized that contributory liability is triggered by providing a tool or service that can be used to infringe, "with the expectation that it would be used" to infringe. *See Henry v. A.B. Dick Co.*, 224 U.S. 1, 48-49 (1912).

The DMCA's safe harbor illustrates this truth. If the background rule were as Petitioners propose—that failure to terminate known repeat infringers could never be a basis for liability—it would be passing strange for the DMCA safe harbor to hinge,

in part, on "reasonably implement[ing]" a repeat-infringer termination policy. 17 U.S.C. § 512(i).[5]

Although safe harbor qualification is a distinct issue from contributory infringement liability, if refusing to terminate infringers could *never* generate liability, Congress would hardly have needed to provide a liability shield that turns on reasonably stopping known infringers. *See* Resp. Br. 38-41. At a bare minimum, the safe harbor indicates that an internet platform's so-called "inaction" in the face of known repeat infringement matters to the contributory infringement analysis. For some types of internet services, moreover, including one that hosts user-generated content (like YouTube), the safe harbor turns in part on the service's "right and ability to control" the infringing activity and its expeditious take down of known infringing material. 17 U.S.C. § 512(c). This likewise reinforces that "inaction"—e.g., refusing to take down known wrongful material—does not automatically and entirely remove an entity from the realm of secondary liability.

**b.** Turning to federal laws about internet platforms more generally, Congress has shielded some internet platforms ("interactive computer services") from some liability—liability based on their being "treated as the publisher or speaker of any information provided by" third parties. 47 U.S.C.

---

[5] DMCA safe harbor requirements vary depending on the type of online services provided, but the repeat-infringer policy applies across the board. *See id.* § 512(a)-(d), (i); U.S. Copyright Office, *Section 512 of Title 17*, https://tinyurl.com/68thya5e.

§ 230.[6] Here again, the existence of some statutory immunity reinforces the background rules whereby internet platforms otherwise could be liable for their "inaction" regarding third-party content—*i.e.*, refusal to take it down, or stated another way, continuing to distribute it.

Section 230's history confirms that Petitioner's blanket "action" requirement cannot be imported wholesale to every situation. The "specific background legal principles" against which Congress enacted § 230 were not aiding and abetting precepts, but rather doctrines governing when one party could be liable for a another party's content. *Malwarebytes, Inc. v. Enigma Software Grp. USA, L.L.C.*, 141 S. Ct. 13, 14 (2020) (Thomas, J., statement respecting denial of certiorari). That law distinguished between publishers (who "could be strictly liable for transmitting illegal content") and distributors of third-party content (who were liable only if they knew or constructively knew of the illegal content). *Id.* Under this law, both publishers and distributors could be liable for what Petitioners would call "inaction"; publishers if they failed to correct a defamatory statement and distributors if they failed to remove known illegal content from their newsstands.

Responding to a state case that held an internet bulletin board liable as a "publisher" for information that it had failed to remove simply because the

---

[6] Section 230 does not "limit or expand any law pertaining to intellectual property." *Id.* § 230(e)(2). The discussion here thus does not pertain to copyright. But that divergence yet again reinforces why liability rules cannot be generalized to all internet platform liability connected to users' wrongdoing.

bulletin board engaged in some content moderation, *Malwarebytes*, 141 S. Ct. at 14 (Thomas, J., statement respecting denial of certiorari), Congress enacted § 230 to encourage internet platforms to "block[] and screen[] … offensive material" without concern that merely doing so would render them "publishers," 47 U.S.C. § 230(c). It is best understood to provide that "if a company unknowingly leaves up illegal third-party content, it is protected from publisher liability." *Malwarebytes*, 141 S. Ct. at 15 (Thomas, J., statement respecting denial of certiorari).

But publisher liability is not all liability. There are myriad circumstances where internet platforms are subject to liability, and not immunized by § 230, for failures to act (*i.e.*, negligence), even though user-uploaded content may be involved in some way. For example, in NCOSE's *Doe* case, the Ninth Circuit held that § 230 did not apply to a claim of negligence per se based on Twitter's failure to report known child sexual abuse material to the National Center for Missing and Exploited Children. *Doe*, 148 F.4th 635, 2025 U.S. App. LEXIS 19406, at *22-24. Internet platforms can also be subject to liability, and not immunized, for defective product designs. *See e.g.*, *id.* at *16-18 (claim for defective CSAM reporting infrastructure); *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1091 (9th Cir. 2021) (holding Snapchat not entitled to § 230 immunity for claim that filter showing the speed a user was traveling encouraged reckless driving).

Section 230, moreover, contains express exceptions that raise additional, context-specific issues, including exceptions related to child sexual abuse material and sex trafficking. As discussed below, there is a nuanced interplay between

background liability rules, § 230, and federal statutes prohibiting the sexual exploitation of children that requires case-by-case, claim-by-claim consideration. *See infra* Part II.

Another exception is the § 230 carve-out for violations of the "Electronic Communications Privacy Act of 1986 … or any similar State law." 47 U.S.C. § 230(e)(4). That raises the possibility of internet platform liability for "disclos[ing]" communications that were unlawfully intercepted or recorded by others, 18 U.S.C. § 2520(a)—another distinct standard that raises distinct questions. Does refusing to take down a user's posted video of a known illegally recorded phone call count? That question should be answered in a case that presents it—not resolved by application of some purported blanket no-liability-for-inaction rule.

This is not a full accounting of all the different contexts in which questions could arise about internet platform liability for refusing to take down illicit conduct or refusing to terminate users that the platform knows are using its service for illicit ends. The list could go on and on. Each context must be judged by its own distinct federal standards.[7]

**3.** An additional contextual variable makes blanket rules unworkable: not all internet companies are the same merely because they "provid[e] their services to the public writ large." *Twitter*, 598 U.S. at

---

[7] Different contexts could raise different constitutional questions, too. For example, whatever the weight of any First Amendment interest in maintaining access to internet service generally, CSAM is "fully outside the protection of the First Amendment." *United States v. Stevens*, 559 U.S. 460, 471 (2010).

499. Petitioners here run an internet service provider that supplies a household's internet connection. Pet. App. 6a.[8] That is a distinct service from an interactive computer service that hosts, curates, and promotes user-created content (as with social media); a search engine; a website that displays its own content alongside user-submitted content; a hosting service that stores material for user-created websites; or any number of infinite variations on these possibilities. Depending on the context and the specific claim at issue, these variations matter when assessing secondary liability.

Other specifics about the internet service at issue may matter, too. *Twitter* considered "three of the largest and most ubiquitous platforms on the internet: Facebook, YouTube, and Twitter." *Twitter*, 598 U.S. at 479. The platforms' size and general use were factors in the Court's analysis, *id.* at 500, in part because the case turned on "failing to detect" a number of terrorism-related posts rather than the refusal to take down known illegal content. *Id.* at 481, 489. In other cases, the narrowly tailored nature of the platform's service might increase the foreseeable risk of wrongdoing and tighten the connection between the service and the illicit conduct. *See id.* at 502.

Some internet services, such as Pornhub, are focused on distributing user-created sexual content, raising obvious concerns of distributing CSAM. *See Doe v. MG Freesites, Ltd.*, 676 F. Supp. 3d 1136, 1145

---

[8] Of course, the conduct at issue here is not Petitioners' basic provision of services to the public, but their refusal to terminate specific customers that they knew were repeat infringers. *See* Resp. Br. 1.

(N.D. Ala. 2022). Others are primarily used to connect individuals for in-person or virtual encounters, presenting obvious concerns for facilitating sex trafficking. *See, e.g.*, *A.M. v. Omegle.com*, 614 F. Supp. 3d 814, 817 (D. Or. 2022) (holding that claims could proceed against a service that "pairs strangers from around the world for one-on-one chats" that paired an 11-year-old girl with an adult man who forced the girl "to send pornographic images and videos of herself to him, [and] perform for [him] and his friends"). Where the case involves a purported failure to detect unlawful material (as opposed to knowing refusal to take it down), these differences in platform purpose and function may be significant factors. All of these internet platforms provide services to the general public (perhaps subject to age restrictions), but they vary significantly in their scope, structure, and operation—again reinforcing the inaptness of blanket rules.

## II. Internet platforms' attempt to rewrite *Twitter* to apply in every context would impair efforts to protect children from the irreparable harm of sexual exploitation.

The spread of child sexual abuse material online is an "ongoing public health crisis" and successfully addressing it "requires action" by "online service providers" among others. U.S. Dep't of Justice, *Report to Congress, The National Strategy for Child Exploitation Prevention & Interdiction*, at i (2023), https://tinyurl.com/3npdz2tu. If Petitioners and their amici successfully establish an all-contexts rule that they can never be liable for anything that can be characterized as "inaction," internet platforms could sit on their hands while knowingly profiting from

criminal child sexual abuse material—despite federal statutes and background legal principles that mandate the contrary result. The Court need not, of course, resolve that question here. But that's the point. So-called blanket "rules" about internet-related liability cannot be transplanted from context to context without case-specific and context-dependent analysis.

### A. No general immunity-for-inaction rule should apply where sites knowingly use automated features to amplify and profit from child sexual abuse material.

The "toll" on survivors caused by child sexual abuse material circulating online "cannot be overstated." *Doe v. Mindgeek U.S. Inc.*, 702 F. Supp. 3d 937, 943 (C.D. Cal. 2023). Images may circulate through the victims' schools, leading to harrowing stories of "harassment, [and] vicious bullying," and causing children to skip school or became suicidal. *Doe v. Twitter, Inc.*, No. 3:21-cv-00485, 1st Am. Compl., Dkt. No. 39, ¶ 106 (N.D. Cal.). Not only that, offender communities have been known to "discuss, track, and follow victims of CSAM as they grow up" by searching for victims online and "work[ing] together to hunt these children." U.S. Dep't of Justice, *Child Sexual Abuse Material*, at 7, https://tinyurl.com/mwzfyddh.

But platforms profit from this material. Advertising revenue is driven by web traffic and there is an "'insatiable demand'" for CSAM that "drives web traffic." *Fleites v. MindGeek S.A.R.L.*, No. 2:21-cv-04920, 2025 U.S. Dist. LEXIS 190592, at *11 (C.D. Cal. Sep. 26, 2025) (quoting National Center for Missing and Exploited Children report). In 2024

alone, the National Center for Missing and Exploited Children documented "29.2 million separate incidents of child sexual exploitation" reported to its CyberTipline. CyberTipline Report, *supra*.

Both general-use platforms and those dedicated to the sharing of pornographic material display advertisements on pages with CSAM. Both have automated features to assist users in locating this material. Allegations in litigation against Reddit, for example, note that it "highlights subreddits that feature child pornography to sell advertising on those pages." *Does v. Reddit, Inc.*, 51 F.4th 1137, 1140, 1145 (9th Cir. 2022). Third-party "advertising tools have listed several subreddits dedicated to child pornography as some of the most popular pages on the platform, which encourages advertisers to buy ad space on those pages." *Id.* at 1140. And Reddit is not alone. *See Doe*, 148 F.4th 635, 2025 U.S. App. LEXIS 19406, at *8, *19-20 (discussing allegations that Twitter linked advertising to posts sharing CSAM and suggested hashtags associated with CSAM to make it easier to find).

Popular porn-sharing sites likewise display ads around CSAM videos and tag the videos with words indicating their heinous nature to help users find them. *See Doe v. WebGroup Czech Republic*, No. 2:21-cv-02428, Compl., Dkt. No. 1, ¶¶ 52, 66, 116 (C.D. Cal.) (complaint documenting use of tags including "toddler," "elementary," "7th grader," and "not 18" by owner of two porn-sharing sites, both ranked in the top ten most visited sites on the internet); *Does 1-9 v. Murphy*, No. 7:20-cv-00947, 5th Am. Compl., Dkt. No. 193, ¶¶ 60, 63 (D.S.C.) (complaint cataloging

Pornhub's use of tags including "underage," "rape" and "hidden camera").

This profit motive is powerful. According to the Federal Trade Commission, "Pornhub's operators turned a blind eye to the proliferation of videos depicting the sexual abuse of children on its sites so it could profit off this exploitation." Federal Trade Comm'n, *FTC Takes Action Against Operators of Pornhub and other Pornographic Sites for Deceiving Users About Efforts to Crack Down on Child Sexual Abuse Material and Nonconsensual Sexual Content* (Sept. 3, 2025), https://tinyurl.com/24ke64mf (describing consent order). Other platforms may also "turn[] a blind eye to illegal revenue-generating content." *Doe*, 148 F.4th 635, 2025 U.S. App. LEXIS 19406, at *15-16; *Reddit*, 51 F.4th at 1145 (discussing allegations that Reddit "fails to remove child pornography" reported by users because it enjoys the resulting revenue).

In many cases, sites have actual knowledge of specific posts sharing CSAM but do not remove them. In *Doe v. Twitter,* for example, the platform told the victim that it had "reviewed" a video displaying CSAM of two 13-year-old boys and refused to remove the video. *Doe*, 148 F.4th 635, 2025 U.S. App. LEXIS 19406, at *7. The video only came down after the Department of Homeland Security got involved almost a week later. *Id.*

### B. Federal law does not create or allow blanket immunity for internet platforms' inaction in response to child sexual exploitation.

Congress "never intended to provide legal protection to websites that … facilitate traffickers in

advertising the sale of unlawful sex acts with sex trafficking victims," and it "clarif[ied]" the law to make sure that it would "not provide such protection to such websites," *MG Freesites,* 676 F. Supp. 3d at 1154 (quoting Pub. L. No. 115-164, § 2(1), (3), 132 Stat. 1253, 1253 (2018)).

Specifically, Congress has created two relevant private rights of action. One applies to claims seeking damages for violations of the federal criminal prohibition on sex trafficking, 18 U.S.C. § 1591. *See* 47 U.S.C. § 230(e)(5). The secondary liability standard for violations of the anti-sex-trafficking statute—benefitting from "participation in a venture" that has committed an act of sex trafficking, 18 U.S.C. § 1591(a)(2)—is distinct from the "aiding and abetting" standard considered in *Twitter*. Specifically, someone "participates in a [sex trafficking] venture" if they "knowingly assist[], support[], or facilitat[e]" any violation of § 1591(a), including child sex trafficking. Section 230 expressly exempts such claims from any immunity otherwise conferred by that statute. 47 U.S.C. § 230(e)(5). Congress enacted this exception in the Allow States and Victims to Fight Online Sex Trafficking Act, calling out certain websites' "reckless[ness]" and their inaction, having "done nothing to prevent the trafficking of children." Pub. L. No. 115-164, § 2(2), 132 Stat. at 1253.

The second federal cause of action applies to children who were victims of any crime related to child sex abuse material (as well as for sex trafficking and other crimes). 18 U.S.C. § 2255; *id.* § 2252A. The cause of action (like the crime) reaches not just the creators or original uploaders of CSAM, but also those who knowingly receive or redistribute it online. *Id.*

§ 2252A(a)(2).[9] This cause of action is part of Congress's effort to "stamp[] out the vice of child pornography at all levels in the distribution chain." Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 501(2)(C), 120 Stat 587, 624. Congress has also recently imposed statutory duties requiring internet platforms to act to take down and stop distributing CSAM and other images related to the sexual exploitation of children. *See, e.g.*, 18 U.S.C. § 2258A(a)(1)(A)(i) (requiring certain internet platforms to file reports with the National Center for Missing and Exploited Children "as soon as reasonably possible after obtaining actual knowledge of" apparent or imminent CSAM violations); 47 U.S.C. § 223a (requiring covered platforms to take down intimate visual depictions published without consent, including of minors).

Of course, Congress also provided some immunity in § 230 for internet platforms acting as publishers. *See supra* Section I.B.2.b. But § 230 makes no mention of distributor liability. Although the courts of appeals have generally held that § 230 covers distributor liability—"adopt[ing] this holding as a categorical rule across all contexts"—this Court has never interpreted § 230. *Malwarebytes*, 141 S. Ct. at 15 (Thomas, J., statement respecting denial of certiorari).

There are reasons to doubt that Congress intended that categorical extension of immunity. Among them is Congress's express § 230 exception for "the

---

[9] There is a disagreement in the district courts regarding whether the cause of action also reaches aiders and abettors. *See, e.g.*, *Mandel v. Daskal*, No 23-CV-7352, 2025 U.S. Dist. LEXIS 165967, *11 (E.D.N.Y. Aug. 25, 2025) (describing split).

enforcement of … [chapter] 110 (relating to sexual exploitation of children) of title 18," which contains the private cause of action for CSAM victims, 47 U.S.C. § 230(e)(1) (captioned "No effect on criminal law"), as well as the express exception for sex trafficking claims discussed above.

Lower courts have diverged regarding the question of when websites and internet platforms are subject to liability for knowing distribution of CSAM and profiting from the sexual exploitation of children. In one case against Pornhub involving user-created videos of the rapes of 14- and 16-year-olds, the Northern District of Alabama found that the that the platform was not immune from suit where it profited from "demand for CSAM" and "cater[ed] to this demand by creating tags, categories, and search suggestions that facilitate easy access to CSAM." *MG Freesites*, 676 F. Supp. 3d at 1145.

The Ninth Circuit in NCOSE's *Doe* case, on the other hand, recently held that § 230 shields an internet provider from liability even for the continued distribution of known CSAM. *Doe*, 148 F.4th 635, 2025 U.S. App. LEXIS 19406, at *24. The court recognized that the allegations showed that "Twitter profits from all the posts on its website, it knew the posts at issue here contained child pornography, and therefore it knowingly benefited from a child-pornography trafficking venture." *Id.* at *15. But it nevertheless affirmed dismissal of the sex trafficking claims, concluding that "[u]nder our precedents, that simply does not suffice to state a claim." *Id.*; *see also Doe v. Webgroup Czech Republic*, 767 F. Supp. 3d 1009, 1018, 1020 (C.D. Cal. 2025) (holding website was immune under Ninth Circuit law because

allegations of "creation of advertisement based on data indicating CSAM; sharing of profits with sex trafficking users; use of VPNs to anonymize web traffic and evade law enforcement; and creation of thumbnails, titles, tags, keywords, search terms, and categories indicative of CSAM" were insufficient).

This divide is not, of course, before the Court now. But its existence belies the idea that there can be any one-size-fits-all rule governing internet platform liability for "inaction." The Court should await a case that presents those questions to decide them—not pretermit them through sweeping blanket rules drawn from wholly inapposite contexts.

* * * * *

This case is not about CSAM or child sex trafficking, or the role of internet platforms in either facilitating the wrongdoing or helping to stop the scourge of sexual exploitation. The case should not be about those harms. But the overbroad argument made by Petitioners and their amici risks putting them in the frame. This case should only be about the distinct question of contributory infringement of copyright—not blanket rules governing the liability of internet platforms for facilitating or assisting wrongdoing. However the question presented is resolved, NCOSE urges the Court to make clear that neither *Twitter* nor this case involves general rules immunizing internet platforms from liability for anything that might be called "inaction," regardless of context.

## CONCLUSION

The judgment should be affirmed.

Respectfully submitted,

Hyland Hunt
*Counsel of Record*
Dana Kaersvang*
DEUTSCH HUNT PLLC
300 New Jersey Ave. NW
Suite 300
Washington, DC 20001
(202) 868-6915
hhunt@deutschhunt.com
**Licensed in Colorado*

October 22, 2025