No. 24-171

In the Supreme Court of the United States

COX COMMUNICATIONS, INC., ET AL.,
PETITIONERS

v.

SONY MUSIC ENTERTAINMENT, ET AL.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

BRIEF FOR GRANDE COMMUNICATIONS NETWORKS, LLC, AS AMICUS CURIAE SUPPORTING PETITIONERS

RICHARD L. BROPHY
ZACHARY C. HOWENSTINE
MARK A. THOMAS
ARMSTRONG TEASDALE, LLP
7700 Forsyth Blvd., Ste. 1800
St. Louis, MO 63105

DANIEL L. GEYSER
Counsel of Record
HAYNES AND BOONE, LLP
2801 N. Harwood Street, Ste. 2300
Dallas, TX 75201
(303) 382-6219
daniel.geyser@haynesboone.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Page

Cases—continued:

Statute and rule:

Other Authorities:

In the Supreme Court of the United States

No. 24-171

COX COMMUNICATIONS, INC., ET AL.,
PETITIONERS

v.

SONY MUSIC ENTERTAINMENT, ET AL.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

BRIEF FOR GRANDE COMMUNICATIONS NETWORKS, LLC, AS AMICUS CURIAE SUPPORTING PETITIONERS

INTEREST OF AMICUS CURIAE

Grande Communications is a major internet service provider in Texas.[1] It operates as part of Astound Broadband, which is the nation's sixth largest telecommunications provider, serving eight of the top ten metro markets in the United States. Like other ISPs, Grande provides content-neutral internet service to the general public. Grande has firsthand experience with this issue: it has a pending petition (No. 24-967) raising the same question

[1] Pursuant to Rule 37.6, amicus affirm that no counsel for any party authored this brief in whole or in part, and that no person other than amicus, its members, or its counsel made a monetary contribution intended to fund the preparation or submission of this brief.

presented here. And it has a distinct interest in illustrating the devastating practical and legal consequences of respondents' position.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case asks a question of broad national significance under the Copyright Act: whether ISPs are contributorily liable for supplying content-neutral internet access to arm's-length customers who unilaterally engage in copyright violations.

That question is exceptionally important. It has astounding legal and practical stakes. The Fourth Circuit's decision sharply departs from this Court's precedent. And there is an urgent need for correction: respondents' theory does not resemble any kind of traditional common-law liability. It flunks the tests this Court recognized in *Twitter, Inc.* v. *Taamneh*, 598 U.S. 471 (2023), and *Metro-Goldwyn-Mayer Studios Inc.* v. *Grokster, Ltd.*, 545 U.S. 913 (2005). And it targets not individual incidents but systemic concerns—putting the burden on private ISPs to conjure up entire regulatory schemes to police and enforce unwritten copyright rules (or face crushing liability).

This Court has long recognized the importance of protecting key industries from undue interference and preserving clear, efficient, workable rules for regulated actors. Yet while respondents pitch their position as straightforward, nothing about their proposed scheme is simple or easy. They brush aside the real-world challenges it thrusts upon others, and shrug at the severe hardship it would impose on families, businesses, schools, hospitals, and major institutions. It endangers jobs, livelihoods, health, education, emotional wellbeing, and political engagement. And the upshot of respondents' position

is clear: ISPs will be forced to terminate access to thousands of users (many of whom did nothing wrong) or face intolerable costs—despite the lack of any "duty that would require defendants or other communication-providing services to terminate customers after discovering that the customers were using the service for illicit ends." *Twitter*, 598 U.S. at 501.

This is a major question. It involves considerations of vast economic and political significance. The answer is not found in the Copyright Act (which does not even expressly authorize contributory liability). The consequences are vital to the nation's ISP industry and the public's ability to access broadband—which is essential to every component of modern daily life. An issue of such obvious magnitude is one that Congress would necessarily reserve for itself—as this Court recognized decades earlier. *Sony Corp. of Am.* v. *Universal City Studios, Inc.*, 464 U.S. 417, 431 (1984). And yet respondents seek to impose systemic liability on an entire industry without any plausible hint that Congress itself addressed these difficult questions and resolved the conflicting policy concerns.

Nor are respondents correct that the DMCA's safe harbor is an answer. That provision confirms on its face that Congress was preserving any and all defenses and not deciding whether ISPs might be passively liable for copyright infringement on their networks. See 17 U.S.C. 512(*l*); S. Rep. No. 190, 105th Cong., 2d Sess. 19 (1998). Congress does not resolve major questions in provisions that explicitly dodge an issue.

At bottom, this is a policy question for the political branches. It falls plainly outside the common-law footprint (which otherwise rejects respondents' theory).[2] It needs a regulatory framework with settled rules, clear enforcement mechanisms, and unambiguous legislative guidance. It should not be announced in scattershot fashion by district-court judges on an ad-hoc basis—a process that will wreak havoc on the public and the entire ISP industry for potentially decades.

Because this kind of major question should be resolved by Congress alone, the Fourth Circuit's decision is wrong and this Court should reverse.

ARGUMENT

A. Respondents' Position Flouts The Major-Questions Doctrine And This Court's Express Guidance In This Very Context

This case presents a fundamental question of surpassing importance under the Copyright Act: whether an ISP is liable for contributory infringement by providing content-neutral service to known infringing subscribers. That question can be resolved under a straightforward application of this Court's settled rules for contributory

---

[2] Indeed, this Court has twice summarized the dispositive legal rule in a manner that should have directly resolved this case: "passive assistance" is not "active abetting," and "a contrary holding would effectively hold any sort of communication provider liable for any sort of wrongdoing merely for knowing that the wrongdoers were using its services and failing to stop them. That conclusion would run roughshod over the typical limits on tort liability and take aiding and abetting far beyond its essential culpability moorings." *Twitter*, 598 U.S. at 500, 503; see also *Grokster*, 545 U.S. at 937 & 939 n.12 ("in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses").

infringement and secondary liability. But if those settled rules leave any room for doubt, the major-questions doctrine is dispositive.

Under that doctrine, courts presume that Congress reserves for itself policy questions of staggering "'magnitude and consequence.'" *Biden* v. *Nebraska*, 600 U.S. 477, 504 (2023). That describes this case exactly. This case dictates whether an entire industry is on the hook for the wrongful acts of unrelated third parties. The decision below threatens this key national industry in a profound way. It dictates how that industry can operate and provide service to millions of subscribers—with the answer affecting the wellbeing of thousands of individuals, families, businesses, and institutions. This question is not even plausibly addressed by the Copyright Act, and it is inconceivable to think Congress left these mission-critical questions to the ad-hoc decisionmaking of random juries and scattered district courts.

The question implicates matters of overriding economic and social significance—and yet the answer is found nowhere in the text of any enacted federal law. If respondents wish to craft a new industrywide scheme, their proper audience is Congress.

1. This question implicates considerations of vast economic and political significance that Congress would necessarily reserve for itself

At its irreducible core, this case asks whether ISPs are liable for their subscribers' copyright violations.

That is an obvious major question. It affects a critical national industry and millions of stakeholders. The Fourth Circuit's decision ignores the serious costs of cutting off service, the untenable task of forcing ISPs to regulate this sensitive issue, and the profound problem of asking ISPs and courts to craft an unwritten regulatory

scheme without any legislative guidance—a strong indication that Congress nowhere authorized this staggering liability.

Respondents may be content to leave it up to district courts and juries to implement a pseudo-administrative regime on an ad-hoc basis. But that is no way to structure industrywide rules for questions of such serious legal and practical importance. This Court has long recognized—in *this* setting—that the judiciary will not "expand the protections afforded by the copyright without explicit legislative guidance." *Sony Corp. of Am.* v. *Universal City Studios, Inc.*, 464 U.S. 417, 431 (1984). There is no such guidance here. Respondents are fundamentally wrong to invite a systemic upheaval without Congress's input.

a. First and foremost, respondents wrongly ignore the sensitive and difficult policy questions inherent in cutting off internet access—including the grave and obvious hardship for tens of thousands of users, and the unfairness of punishing an entire household, business, school, hospital, hotel, facility, dorm, etc., for a single individual's misfeasance.

Terminating online access is no minor thing. It threatens the jobs of remote workers. It threatens the ability of children to engage in remote learning. It threatens the health of those with connected medical devices. The list is easy to expand. Virtually every component of today's social and economic existence is tied to the internet—and cutting off service threatens massive disruption to work, education, health, learning, entertainment, political engagement, social interaction, and basic wellbeing. It has devastating effects on families and their livelihoods, and can shut down businesses and essential facilities. The costs are patently unreasonable under any metric, and there is no indication, anywhere, that Congress felt this kind of drastic punishment was warranted based on two

alleged infractions often resulting in less than a few dollars of actual harm.[3]

And this says nothing about the deeper unfairness and costs of punishing entire households (or entire facilities) because a single individual happened to download as few as two songs on two separate occasions. It is absolutely common for families, businesses, apartment buildings, universities, etc., to share a single internet connection or account. So take a family: this could mean terminating service to 4-6 people (including parents working from home) simply because one person—or even a transient guest—happened to misuse the connection (often unbeknownst to others). Respondents' position is especially absurd as applied to institutional users—hotels, hospitals, dorms, businesses, barracks, coffee shops, etc. See Pet. Br. 11 (listing 48 such entities—including 10 universities, 9 hotels, 6 apartment buildings, and 3 retail establishments). This would cut off access to countless innocent parties for a single person's misconduct—even if the subscriber itself was completely unaware of that party's actions.

Most families and institutions cannot function today without the internet. Yet respondents say everyone

---

[3] The concrete costs are not hypothetical. See, *e.g.*, K. N. Hampton, et al., *Broadband and Student Performance Gaps*, Mich. State Univ. (Mar. 3, 2020) <https://doi.org/10.25335/BZGY-3V91> (high-school students without home internet access had lower grades and standardized test scores, controlling for socioeconomic factors); J. Van Parys, et al., *Broadband Internet access and health outcomes: Patient and provider responses in Medicare*, 95 Int'l J. Indus. Org. 103072 (expanding home broadband drove 16% of the overall reduction in mortality and readmission rates for elective surgery patients); Kathryn R. Johnson, et al., *Broadband Internet Access, Economic Growth, and Wellbeing*, Nat'l Bureau Econ. Research, Working Paper 32517 (May 2024) <https://www.nber.org/papers/w32517> (increase in broadband access reduces suicide rates).

loses—in devastating ways—whenever anyone associated with any IP address twice engages in even minor acts of infringement. It is bizarre to say an ISP should face jaw-dropping liability for failing to mete out the harshest possible punishment (with predictable collateral damage) based on a two-dollar crime. And it is especially bizarre to presume Congress (without any textual hint) would endorse such a severe result.[4]

b. Even were this extreme punishment warranted, respondents paint the ISPs' task as simple and straightforward, but this stands reality upside-down. Respondents ignore the significant practical challenges that ISPs face in making termination decisions, especially without any clear framework dictating when action is required—or what process and protections subscribers should receive.

The record labels bombard ISPs with millions of alleged infringement notices (Cox Pet. App. 9a; Cox Pet. 10; Sony Opp. 4)—typically sending hundreds of notices each day. Yet there is absolutely no guidance or framework establishing the bounds of liability. Just a few examples:

**How many notices are enough? Two? Ten? More? What if the first notice is doubtful—or the subscriber offers a legitimate excuse or promises not to do it again? Still credit the violation? What if the notices are separated in time (say the second arrives a year after the first? six months? five weeks?)? When, if ever, does the clock reset? What if a notice flags hundreds of downloads in a single session? What if a longtime user uncharacteristically downloads songs on two consecutive days? Terminate im-

[4] Indeed, imagine the public reaction were Congress to write this sentence into the U.S. Code: "Any person or business who twice downloads songs illegally shall be immediately barred from the internet." Respondents' attempt to read such a penalty between the lines is untenable.

mediately? What if two separate users admit responsibility for the two separate notices? Does that still require termination? What if the IP address never receives another notice? If access is terminated, when can it be restored? Ever? Do ISPs have an obligation to notify their competitors so they too can refuse to serve that customer? Can an ISP sign up a customer despite being flagged by a different ISP? Do those past strikes count or not?

**Respondents' robo-vendors are not infallible. There is a risk of false accusations or simple mistakes. See, *e.g.*, Altice Amicus Br. 15-16 (providing examples). What happens if a subscriber objects or denies the allegation? What opportunity do subscribers have to respond? What process is required? An in-person hearing? Any ability to submit evidence? What investigation is mandated? What notice is sufficient? What proof is required? Who decides whether the label or the subscriber is correct? And how is the ISP supposed to do any of this—given that it cannot monitor any user's activity, has no access to a subscriber's hard drive, has no way of verifying anything, and cannot even determine which individual person was using the targeted IP address (an especially acute problem when dealing with facilities, dorms, hospitals, coffee shops, businesses, etc.)?[5]

**What excuses/explanations are acceptable? Any? Are any second- or third-chances allowed? What if the

[5] Respondents even overlook the technical challenges of matching the correct user with a corresponding IP address. Assignments of IP addresses to subscribers change over time, and it is not always obvious which subscriber is responsible for which action on which date. As a result, ISPs cannot even be perfectly confident that the right person is being served with the right notice. Nor is there any other way around this, given the practical impossibility of monitoring (much less recording) the entirety of all internet activity conducted across a global system. ISPs simply have no way to verify the allegations.

subscriber was hacked? What if the subscriber was unaware how to install a WiFi password? What if the subscriber was clueless about a babysitter's improper use? Or a child's (or her friend's)? What if another incident occurs despite a parent first attempting a mild punishment? No chance to try again? What about honest mistakes? Still terminate?

**What leniency is permitted? Any? And based on what factors? What if a parent had no idea about a child's or spouse's infringement? What if they will lose their job? What if a child will miss school or assignments? What if the family has special medical needs, has connected medical devices, or lives in a rural area and uses telehealth services? Is it fair for the ISP to consider the stakes—including situations where terminating access will devastate a family's livelihood and wellbeing?

**What flexibility is permitted for connections used by dozens or hundreds of users? Does the same "two-strikes-and-you're-out" policy apply? Does it matter if the IP address is exposed to different users at different times (like hotels with guests)? Does it matter what policies those facilities enforce?

**ISPs may face competing directives from state authorities. ISPs, for example, received instructions (from various state actors) not to terminate internet access during the recent pandemic. Yet respondents' theory requires termination anyway. This leaves ISPs in an impossible bind. What are ISPs supposed to do? Ignore the States and risk regulatory action, or follow state directives and risk massive damages? How, if at all, do state directives affect liability? And how can respondents possibly justify countermanding regulatory orders and seeking damages for failing to terminate during such periods?

**What resources are required? Are ISPs supposed to invest in hiring entire staffs and departments to review,

investigate, adjudicate, and resolve hundreds of robo-complaints, all because respondents would rather not do the hard work themselves—or sue the actual infringers?

In short, there is no clear framework dictating when action is required. Respondents' theory (which the Fourth Circuit has now endorsed) effectively demands a pseudo-governmental regulatory body operating privately inside each ISP—with a still-unwritten and still-unknown scheme of detailed regulations. And respondents are quick to demand termination upon receiving a second notice, but they apparently cannot be bothered to spell out the details of their own scheme.

Respondents cannot simply brush these issues aside as someone else's problem. Respondents expect to collect up to $150,000 for each infringed work—and yet there is no statutory framework or legal guidance, anywhere, making clear precisely when an ISP should take action or what action is necessary. ISPs should not be left to fend for themselves, and they should not face crushing liability for not knowing how to resolve competing private disputes about whether infringement actually exists or what remedial actions suffice in response. And yet that is precisely the outcome of the decision below—with ISPs everywhere scrambling to find ways to protect themselves against ad-hoc determinations by individual courts and juries in lawsuits seeking crippling liability.[6]

---

[6] Indeed, under Fourth Circuit precedent, ISPs are left with an impossible choice: terminate access immediately for users who may have done nothing wrong (at a grave cost to individuals, businesses, etc.), or terminate access too late and face crushing liability. And these suits threaten to drive smaller ISPs out of business—harming competition, risking access in rural markets, and defeating Congress's goal of universal broadband coverage. See Altice Amicus Br. 12-19.

The bottom line: Respondents cannot rightfully foist a pseudo-regulatory scheme on private ISPs together with government-like duties to police third-party conduct on their content-neutral service—despite having no direct control over what any subscriber does; no way to limit or monitor their conduct; no way to track or confirm their activity; and no ready means of responding to hundreds of robo-blasts each day from an entity with every incentive to maximize allegations of infringement. Grande is unaware of "any case holding such a company liable for merely failing to block [identified wrongdoers] despite knowing that they used the company's services." *Twitter*, 598 U.S. at 501 n.14; see also *Grokster*, 545 U.S. at 937, 939 n.12. And it is especially difficult to fathom such a duty in the face of practical obstacles as serious as these.

These problems are all the more egregious given that none of this is even necessary. Copyright holders have a clear right to sue those directly responsible for infringing conduct (and the right to force ISPs to reveal the identities of those parties). Respondents may not wish to do that for political or public-relation reasons. See Cox Pet. 8. But that is their choice—and it is on them for refusing to invoke the rights Congress actually provided via statute.

c. As this illustrates, there is a clear danger of presuming Congress (silently) intended the Copyright Act to address these issues at all—and compelling reasons for courts to hesitate before judicially crafting an industry-wide framework for a major policy question that Congress itself did not address. "In a case like this, in which Congress has not plainly marked our course, we must be circumspect in construing the scope of rights created by a legislative enactment which never contemplated such a calculus of interests." *Sony*, 464 U.S. at 431. Indeed, if Congress had "wanted to impose a duty to remove content

on these types of entities," it presumably would have "done so by statute." *Twitter*, 598 U.S. at 501 n.14.

This is a serious question with sensitive and difficult considerations on all sides. It involves industry-wide rules and liability; it implicates massive economic and political stakes; it risks holding private actors responsible for policing the conduct of unrelated third parties in enforcing the separate rights of independent actors. And this scheme looks nothing like an ordinary copyright case (much less traditional common-law secondary liability): it targets an industry-specific regulatory framework dictating how ISPs (as private actors) must govern and enforce federal law on their networks. In sum, "[t]his is no 'everyday exercise of federal power.' It is instead a significant encroachment into the lives—and health—of" countless citizens and a major corporate industry. *NFIB* v. *Department of Labor, OSHA*, 595 U.S. 109, 117 (2022) (internal citation omitted).

Respondents may wish to force the judiciary and ISPs to address these difficult questions without legislative guidance. But this is precisely the kind of "question of deep economic and political significance" that "Congress would likely have intended for itself." *Biden*, 600 U.S. at 506 (internal quotation marks omitted); see also *West Virginia* v. *EPA*, 597 U.S. 697, 723-724 (2022). It calls for a clear and detailed regulatory framework. And while it would be one thing if the common law already provided clear rules in this area, the only rule it does provide forecloses liability: there is no duty targeting passive activity or the failure to take affirmative action when providing a content-neutral service to the public at large. *Twitter*, 598 U.S. at 501 & n.14, 503; see also *Smith & Wesson Brands,*

Inc. v. *Estados Unidos Mexicanos*, 605 U.S. 280, 292-293 (2025).[7]

The Fourth Circuit was mistaken in imposing duties that contravene the common law and are not found in any statute. Its views destabilize the industry and create serious risks for ISPs and their subscribers. If this type of liability should exist, it is Congress's job to say so—balancing the many difficult and sensitive policy questions on all sides. But it is emphatically not the province and duty of the judiciary to conjure up an entire regulatory scheme out of whole cloth.

2. Contrary to respondents' contention, the DMCA did not resolve this issue by refusing to address it

According to respondents, Congress has (somehow) already resolved this major question in the DMCA—where Congress flatly refused to impose secondary liability and explicitly sidestepped the issue.

As the government confirmed, the DMCA answers nothing. U.S. Invitation Br. 13-14. It set out an affirmative defense while deliberately punting on whether underlying liability exists. This is confirmed in both the plain text (17 U.S.C. 512(*l*)) and the legislative reports. *E.g.*, S. Rep. No. 190, 105th Cong., 2d Sess. 19, 55 (1998) ("the Committee decided to leave current law in its evolving state"; "[n]ew

[7] To be clear: Grande is not suggesting the Copyright Act precludes all secondary liability—although the Act is silent on the question. *Sony*, 464 U.S. at 434. That ship has sailed after *Sony* and *Grokster*. But Grande is saying that it is extraordinary to presume Congress delegated to the courts the responsibility of crafting an industrywide set of rules for ISPs to enforce on a systemic level—while making the sensitive judgment-calls reserved for Congress in setting this kind of fundamental public policy. That is directly at odds with "[t]he judiciary's reluctance to expand the protections afforded by the copyright without explicit legislative guidance." *Id.* at 431.

section 512 does not define what is actionable copyright infringement in the online environment"; it "does not create any new liabilities for service providers or affect any defense available to a service provider").

Respondents thus stand the DMCA upside-down in saying it somehow "confirmed" contributory liability in this context. No. 24-967 Opp. 20. The DMCA explicitly says otherwise. And respondents are fanciful to think Congress made a judgment in 1998 (in the days of dial-up modems) regarding how theories of contributory liability ought to apply in today's online world. U.S. Invitation Br. 14. Congress refused to balance the conflicting policy concerns back then; there is no license for the judiciary to step in and do Congress's job now.

* * *

This entire case turns on the core question in the ordinary operation of every ISP: whether providing service to "known infringing subscribers" is actionable.

This is an obvious major question. It has astounding economic and political stakes. The answer is found nowhere in the Copyright Act. This Court already established in *this* setting that this is Congress's job—and the judiciary will not "expand the protections afforded by the copyright without explicit legislative guidance." *Sony*, 464 U.S. at 431. Yet there is no remote legislative guidance here. If extraordinary grants of power "are rarely accomplished through 'modest words,' 'vague terms,' or 'subtle device[s]'" (*West Virginia*, 597 U.S. at 723), they certainly are not found in a statute *silent* on secondary liability.

This is a serious policy question. It needs a legal framework with settled rules, clear enforcement mechanisms, and unambiguous legislative directives. There is no basis to impose systemic liability on an entire industry without any hint that Congress itself addressed and resolved these significant questions.

B. Respondents' Aggressive Theory Has No Limiting Principle—Further Undermining The Notion That This Is Plausibly What Congress Intended

Respondents' failure to identify an *actual* legislative framework infects their theory in another debilitating way: because no statute exists, there is no statutory hook to limit their theory's reach.

Indeed, while respondents hint their aggressive theory is limited to copyright alone, their position could rewrite the entire universe of secondary liability—with no principled stopping point (certainly none in any statute). The end result: they risk exposing ISPs and online platforms—and even brick-and-mortar entities—to heretofore unknown liability for all manner of third-party misconduct. This emphatically underscores the prudence in refusing to resolve a significant policy question that Congress nowhere addressed.

1. According to respondents, ISPs are liable because they knew a user infringed and failed to take affirmative steps to terminate service. Yet that same rule could apply to *any* alleged misconduct—criminal or civil, online or offline.

There is no basis for limiting respondents' theory to copyright alone: the Act does not even *address* secondary liability (*Sony*, 464 U.S. at 434),[8] and the Court invoked traditional "common law principles" in reading it into the

---

[8] The only debatable textual hook for secondary liability is found in Section 106, which grants copyright owners exclusive rights "to do and *to authorize*" certain conduct. 17 U.S.C. 106 (emphasis added); see H.R. Rep. No. 1476, 94th Cong., 2d Sess. 61 (1976) (so suggesting). But that limited textual license—"to authorize"—goes beyond any indirect or passive nonfeasance. It describes affirmative action *approving* infringing conduct. That does not describe offering a content-neutral service to the general public while remaining "indifferent" how that service is used. *Twitter*, 598 U.S. at 500.

Act. *E.g.*, *Grokster*, 545 U.S. at 930; *Sony*, 464 U.S. at 435. Yet if liability here is activated merely by alleged knowledge and passive inaction, what would spare ISPs (or any online service) from any other common-law tort? What about reported drug dealing? Terrorism? Fraud? Illicit trades? Unlawful images? Think of speech-related torts alone: libel, tortious interference, false light. If the misconduct is flagged and the platform fails to respond, respondents' theory says the ISP or online service is liable—despite "our legal system generally" *not* "impos[ing] liability for mere omissions, inactions, or nonfeasance." *Twitter*, 598 U.S. at 489.[9]

Nor is there an obvious way to cabin respondents' theory to the online world. Why not apply the same rule to cellphone providers? Payment processors? Apartment complexes? Office buildings? Cf. Pet. Br. 35, 37. Once any business is told a user is leveraging its service to do anything wrong, the decision to continue that general service now apparently leaves the provider on the hook. *Twitter*, 598 U.S. at 489 ("if aiding-and-abetting liability were taken too far, then ordinary merchants could become liable for any misuse of their goods and services"; "those who merely deliver mail or transmit emails could be liable for the tortious messages contained therein"). That would risk targeting any online or offline service whose users happen to engage in misconduct—with no articulable way

[9] This system would also embroil ISPs and online services in constant private disputes. Websites and ISPs cannot possibly determine whether a given post about someone's character or business is false, defamatory, designed to interfere with existing business or contracts, etc. Nor are websites and ISPs situated to investigate and adjudicate private disputes. These are not pseudo-administrative agencies or informal courts. Put simply: Respondents' theory suggests these services should be liable for inaction despite having no obvious way to verify if action is even warranted in the first place.

to cut off liability where it plainly does not belong. See *id.* at 499 (repudiating comparable arguments for same reasons).

2. Unsurprisingly, this Court has already rejected respondents' world of unlimited secondary liability. So much is clear alone from *Twitter*: companies are not liable "merely for knowing" "wrongdoers were using [their] services and failing to stop them." *Twitter*, 598 U.S. at 499-500, 503; *id.* at 501 ("plaintiffs identify no duty that would require defendants or other communication-providing services to terminate customers after discovering that the customers were using the service for illicit ends"). It is clear again from *Smith & Wesson*: secondary liability "requires misfeasance rather than nonfeasance," and a company's "mere[] know[ledge] that 'some bad actors' are taking 'advantage' of its products for criminal purposes" is "not aid[ing] and abet[ting]"—"even if the company could adopt measures to reduce their users' downstream crimes." *Smith & Wesson*, 605 U.S. at 292-293 (quoting *Twitter*, 598 U.S. at 503). And, of course, it is clear from *Sony* and *Grokster*: "mere knowledge" "of actual infringing uses would not be enough"—fault cannot be "merely based on a failure to take affirmative steps to prevent infringement." *Grokster*, 545 U.S. at 937, 939 n.12 (reaffirming "the *Sony* safe harbor").

This Court's decisions are unequivocal: There is no secondary liability based on a third party's unilateral misuse of a general service designed for substantially lawful means. *Grokster*, 545 U.S. at 939 & n.12; accord *Twitter*, 598 U.S. at 499 ("[t]he mere creation of those platforms, however, is not culpable"; "ISIS's ability to benefit from these platforms was merely incidental to defendants' services and general business models"). This protects innovation and eliminates unwarranted burdens on those conducting legitimate activity—while leaving responsibility

solely with those bad actors engaged in actual wrongdoing. *E.g.*, *Grokster*, 545 U.S. at 937, 941.

As it stands today, respondents' position "would run roughshod over the typical limits on tort liability and take aiding and abetting far beyond its essential culpability moorings." *Twitter*, 598 U.S. at 503. If respondents wish to rewrite the law in this area, their appropriate audience is Congress. But this Court should be especially cautious before embracing a doctrine that would expand secondary liability into untold zones—with an unknown blast radius and zero legislative guidance.

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

RICHARD L. BROPHY
ZACHARY C. HOWENSTINE
MARK A. THOMAS
ARMSTRONG TEASDALE, LLP
7700 Forsyth Blvd., Ste. 1800
St. Louis, MO 63105

DANIEL L. GEYSER
Counsel of Record
HAYNES AND BOONE, LLP
2801 N. Harwood Street, Ste. 2300
Dallas, TX 75201
(303) 382-6219
daniel.geyser@haynesboone.com

SEPTEMBER 2025