

WILLIAM & MARY LAW SCHOOL
WILLIAM B. SPONG, JR., INVITATIONAL TOURNAMENT
SPRING 2025 PROBLEM

No. 25-1779

In the Supreme Court of the United States

PACT AGAINST CENSORSHIP, INC., ET AL.,

Petitioner,

v.

KIDS INTERNET SAFETY ASSOCIATION, INC., ET AL.,

Respondent.

RECORD ON APPEAL¹

¹ **Limitation on Research:** Competitors may not access any briefs filed in the United States Supreme Court. The problem is frozen in time and competitors may not access or use any cases, filings, opinions, statutes, or other materials dated after September 30, 2024.

United States Court of Appeals
for the Fourteenth Circuit

No. 24-30453

KIDS INTERNET ASS’N, INC.; FEDERAL TRADE COMM’N,

Defendants-Appellants,

versus

PACT AGAINST CENSORSHIP, INC.; JANE DOE; JOHN DOE; SWEET STUDIOS, L.L.C.,

Plaintiffs-Appellees.

Appeal from the United States District Court
for the District of Wythe
USDC No. 5:22-cv-7997

Before BARBOUR, MARSHALL, and WASHINGTON, *Circuit Judges.*

BUSHROD WASHINGTON, *Circuit Judge:*

This case arises from from the federal government’s attempts to keep children safe from the online pornography industry. In 2023, Congress created and tasked a private entity—appellant Kids Internet Safety Association, Inc.—with divising and enforcing rules that would require online companies to ensure children’s safety. Shortly after, this private entity passed a rule requiring certain commercial pornographic websites to “age verify” users. Appellees, a coalition of members of the adult entertainment industry, sought to enjoin the rule *and* the continued operation of KISA. Appellees alleged two violations of the

Constitution: first, that Congress violated the private nondelegation doctrine when creating KISA and granting it essentially unfettered power and, second, that the age verification rule violates the First Amendment.

The district court found that Congress’s delegation of authority to KISA was proper, but granted the injunction because it was likely that the Appellees would succeed on their the First Amendment claim. We AFFIRM the nondelegation decision, but because we see no free speech violation, we REVERSE the injunction.

I. BACKGROUND

Factual History

A. Keeping the Internet Safe for Kids Act

In response to growing criticism that our government was doing too little to protect children from being bombarded with inappropriate, offensive, and, at times, obscene sexual material on the internet, Congress passed the Keeping the Internet Safe for Kids Act (KIKSA), which became effective in January 2023.² KISKA aimed to “provide a comprehensive regulatory scheme to keep the Internet accessible and safe for American youth.” 55 U.S.C. § 3050. Because “Internet issues evolve at a rapid rate,” Congress did not think it wise to lay down a strict set of rules in the Act. H. Rep. No. 92-544, at 1 (2022) (Conf. Rep.). Instead, in KISKA Congress created a private entity separate from Congress whose purpose is “to monitor and assure children’s safety online.” 55 U.S.C. § 3054(a). Much like another of Congress’s recent creations, the Horseracing Integrity and Safety Authority, the Kids’ Internet Safety Association, Inc. (KISA)—is a “private, independent, self-regulatory nonprofit corporation,” subject to the “oversight” of the Federal Trade Commission. §§ 3051(a), 3052(a), 3053. In short, Congress is delegating its power by

² For purposes of the competition, we have created federal legislation and an accompanying regulation. The relevant portions of the legislation and regulation are found in the appendix.

creating private companies to oversee and control certain industries within the control of the Federal Trade Commission.

KISA has the ability to make rules regulating the Internet industry as it relates to child access and safety and the ability to enforce those rules. In addition, KISA holds the power to enforce its rules through liberal investigation powers and through the imposition of civil sanctions or the filing of civil actions for injunctive relief. § 3054(c).

Congress also provides KISA with a supervisor, the Federal Trade Commission. The FTC can do a little rulemaking of its own and “abrogate, add to, and modify” KISA’s rules. § 3053(e). Further, the FTC can ask—at any time—to review *de novo* any enforcement actions that KISA brings before an ALJ. § 3058.³

B. Rule ONE

By the end of February 2023, KISA had a governing board of citizens from around the country, and it got to work straight away. In its first few meetings, KISA considered the deleterious effects that easy access to pornography has on minors. Experts at these meetings testified to a host of horrors: Early exposure to pornography results in a higher likelihood of later engagement with “deviant pornography.” Children who frequently consumed adult media were increasingly likely to suffer from “gender dysphoria, insecurities and dissatisfactions about body image, depression, and aggression.” Higher use of pornography also correlated with a drop in grades.

Taking these findings, KISA passed the regulation at issue today—the regulation popularly known as “Rule ONE.” Rule ONE requires certain websites and commercial entities to use “reasonable age verification measures . . . to verify” that only adults access explicit material. The rule applies to “any commercial entity that knowingly and intentionally publishes and distributes material on an Internet

³ To date, the FTC has exercised its authority to review and enforcement action only once. In that case, the FTC engaged in a thorough review before declining to take any action.

website, including a social media platform, more than one-tenth of which is sexual material harmful to minors.” 55 C.F.R. § 1. Rule ONE also provides that reasonable verification measures include government-issued ID, or another reasonable method that uses transactional data. *Id.* § 3. Further, Rule ONE states that no entity performing age verification may “retain any identifying information of the individual.” *Id.* § 2(b).

KISA maintains authority to punish violators of Rule ONE by filing for injunctive relief; issuing up to \$10,000 of fines per day of noncompliance with the rule itself; and fining violators up to \$250,000 for every time a minor accessed a site because of a site’s noncompliance. *Id.* § 4.

The release of this rule in June 2023 sent the adult film industry and its patrons into a frenzy. Jane and John Doe averred that they had stopped visiting sites that required such intrusive identifying information because of the number of instances where seemingly safe websites, such as hospitals and schools, have been hacked and personal information was stolen. Jane Doe, in particular, noted that she believes there is nothing wrong with her interest in obtaining adult information from these sites, but she is fearful that there would be backlash from her community if anyone were to identify her. In fact, the internet is her preferred platform because she need not worry about bumping into an acquaintance, as she might if she sought these materials in a brick-and-mortar store. The industry itself well knew the effect of similar laws passed on a state level. *See, e.g.,* Marc Novicoff, *A Simple Law Is Doing the Impossible. It’s Making the Online Porn Industry Retreat*, POLITICO (Aug. 8, 2023, 4:30 PM) (“[T]raffic in Louisiana has dropped 80 percent.”). They feared results would likely replicate nationally. Thus, with their livelihood (and, as they see it, liberty) at stake, the industry took action by filing this lawsuit.

In seeking the injunction, PAC submitted evidence that most sites that would be subject to the law offer significant amounts of non-objectionable material, including discussion boards about business, job and educational opportunities. PAC submitted expert affidavits, one of which explained how easy it is

with a computer to be anonymous even when age verification is required. Another explained how children can bypass security measures and referred to a news report from 2022, where a 6-year-old child spent over 16,000 dollars on in-app purchases.⁴ Some experts testified that internet filtering and blocking software could be effective methods of preventing juvenile access to adult materials.

Procedural History

On August 15, 2023, the plaintiffs filed this suit to permanently enjoin Rule ONE *and* KISA from operation. Appellee Pact Against Censorship, Inc. (“PAC”) operates as the largest trade association for the American adult entertainment industry. The remaining three plaintiffs are PAC members—two performers and one studio. The district court assured their standing, and neither we nor the parties dispute this. *See Speech First, Inc. v. Fenves*, 979 F.3d 319, 330 (5th Cir. 2020) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)).

PAC moved for a preliminary injunction. After full briefing and argument, the District of Wythe held (1) that KISA does not violate the private nondelegation doctrine because the FTC sufficiently supervises it *but* (2) that Rule ONE violated the First Amendment, in part, because it affected more speech than it needed. Thus, the district court granted the injunction.

KISA, the appellant, appealed the lower court decision on the free speech claim, and PAC, the appellee cross-appealed on the nondelegation issue.

II. STANDARD OF REVIEW

Preliminary injunctions are “extraordinary remedies” granted upon a clear showing that the plaintiff is entitled to relief. *Winter v. Nat. Res. Def. Counsel*, 555 U.S. 7, 24 (2008). We ordinarily review preliminary injunctions for abuse of discretion, but we review *de novo* “decisions grounded in erroneous legal principles.” *Mock v. Garland*, 75 F.4th 563, 577 (5th Cir. 2023) (citations omitted). Because the

⁴ <https://abc13.com/ipad-games-parent-permission-video-game-spending-unauthorized-purchase/12591434/>

parties have stipulated to three of the four preliminary injunction factors, we need only decide whether PAC has demonstrated a “substantial likelihood of success on the merits.” *Id.*

III. KISA SURVIVES THE PRIVATE NONDELEGATION DOCTRINE

We must now determine whether KISA’s enforcement power violates the private nondelegation doctrine.

“Private nondelegation” is a constitutional doctrine that bars the government from giving “unchecked” power to private parties. *Oklahoma v. United States*, 62 F.4th 221, 228 (6th Cir. 2023). A central purpose of this doctrine is to assure “accountability” in the exercise of government. *See Nat’l Horseman’s Benevolent and Protective Ass’n v. Black*, 53 F.4th 869, 880 (5th Cir. 2022) (*Black I*). The Supreme Court, however, does not forbid *all* delegations—merely unchecked ones. *See, e.g., Sunshine Anthracite Coal Co. v. Adkins*, 310 U.S. 381, 388 (1940) (private individuals permitted to help set wages for coal workers because they “function[ed] subordinately to” a governmental body).

Thus, the central question is whether KISA properly operates subordinately to the Federal Trade Commission. In contemplating the answer, it is important to be cognizant that the circuits have split over a private nondelegation doctrine challenge to the Horseracing Safety and Integrity Act—the Act after which Congress (nearly identically) modeled KISA. *Compare Oklahoma*, 62 F.4th at 221 (upholding the Act’s enforcement provision), *with Nat’l Horseman’s Benevolent and Protective Ass’n v. Black*, 107 F.4th 415 (5th Cir. 2024) (*Black II*) (invalidating the Act’s enforcement provision).

The split seems to occur over what counts as subordination. As the Sixth Circuit wrote, that “the FTC *could* subordinate every aspect of . . . enforcement” means the private party is constitutionally supervised. *Oklahoma*, 62 F.4th at 231. The Fifth Circuit, however, felt that the FTC’s ability to control enforcement could only happen in reviewing the private party’s actions, which meant a good deal of enforcement had already occurred without supervision. *See Black II*, at 432–33.

Here, section 3053(e) of KISKA permits the FTC to “abrogate, add to, or modify” KISA’s rules. This means that, as the Sixth Circuit recognized, the FTC can add certain pre-enforcement standards to KISA’s rules. *See Oklahoma*, 62 F.4th at 231. This provides adequate control over KISA’s pre-enforcement decisions.

Further, KISKA gives the FTC full authority to review and completely overrule KISA’s enforcement actions. 55 U.S.C. § 3058. This is a potent power. Thus, KISA’s adjudication decisions “are not final until the FTC has the opportunity to review them.” *Oklahoma*, 62 F.4th at 231. As we can learn from cases concerning the power to write rules, the government permissibly delegates power when it retains control over the final product. *See Cospito v. Heckler*, 742 F.2d 72 (3d Cir. 1984); *Todd & Co., Inc. v. SEC*, 557 F.2d 1008 (3d Cir. 1977).

IV. RULE ONE SURVIVES FIRST AMENDMENT RATIONAL-BASIS REVIEW

The First Amendment states that the government “shall make no law . . . abridging the freedom of speech.” U.S. Const. amend. I. PAC argues that Rule ONE abridges such freedom—not because the regulation prevents *children* from participating in pornographic activity, but because the regulation dissuades *adults* from participating in that constitutionally protected conduct. In essence, PAC fears that people will be too shy to wander into the seedier side of the Web when the First Amendment should let them be so bold. The First Amendment, however, does not share PAC’s fears. Because the government has such a strong interest in “the welfare of children,” the Constitution permits the government to heavily regulate “the distribution *to minors* of materials obscene *for minors*.” *Free Speech Coal., Inc. v. Paxton*, 95 F.4th 263, 269 (5th Cir. 2024) (citations omitted). And Rule ONE falls into this form of permissible regulation.

A. Rational Basis Review Is the Proper Standard

We begin this analysis by determining the appropriate standard of review. The lower court held, without much rationale, that strict scrutiny applies to Rule ONE’s regulation. Relying on Supreme Court

cases like *Reno v. ACLU*, 521 U.S. 844 (1997), and *Ashcroft v. ACLU*, 542 U.S. 656 (2004) (*Ashcroft II*), PAC argues that those cases control *this* case. We disagree.

Despite PAC’s insistence to the contrary, the question of what standard applies defies simple resolution. In fact, circuits have split on it. Although a few circuits have applied strict scrutiny while assessing age verification laws, the Fifth Circuit has recently reviewed a law similar to Rule ONE under rational basis review. *Compare ACLU v. Mukasey*, 534 F.3d 181, 190 (6th Cir. 2008), *with Paxton*, 95 F.4th at 269. Thus, we feel it imperative to properly consider the issue and refrain from merely reciting unexamined dogma. After surveying the briefs and relevant opinions, we opt to apply—as we must by law—rational basis.

1. Supreme Court Precedent

As the Fifth Circuit explained, Supreme Court precedent requires us to apply rational basis. In 1968, the Court upheld a law aimed at keeping obscenity out of the hands of children—even though that law burdened adults. *Ginsberg v. New York*, 390 U.S. 629, 634, 643 (1968) (lawful to restrict material that although not obscene for adults was obscene for children) There, the Court upheld New York’s law because one could “rationally conclude” that the law satisfied the legitimate interest “to protect the welfare of the child.” *Id.* at 640-41. Thus, under a fair reading of *Ginsberg*, the government can restrict children’s access to materials obscene for children on a rational basis review even where such restrictions may inconvenience an adult’s lawful and protected access to those same materials. As the Fifth Circuit wrote, “the statute at issue in *Ginsberg* necessarily implicated, and intruded upon, the privacy of those adults seeking to purchase ‘girlie magazines.’ But the Court still applied rational-basis scrutiny.” *Paxton*, 95 F.4th at 271. Rule ONE seeks to take material obscene for children, as defined in 55 C.F.R. §§ 1(6)(A)-(C), and prevent children from accessing it. Thus, rational basis should apply.

2. *Ginsberg* Remains Good Law

The cases relied on by PAC are distinguished from *Ginsberg*. In applying strict scrutiny when invalidating two provisions in the Communications Decency Act of 1996, the Supreme Court noted that the CDA was materially different than “the statute upheld in *Ginsberg*” in a number of ways. *Reno*, 521 U.S. at 865-68. And it is. The CDA (1) did not permit parental consent, (2) extended past commercial transactions, and (3) prohibited some material that was simply not obscene for minors. *Id.*

Further, and perhaps more importantly, the *Reno* Court felt “*existing technology*” in 1997 failed to accurately distinguish minors from adults. *Id.* at 876 (emphasis added). However, present technology as defined by the facts of this case *does* contain some verifiable technology. Rule ONE permits the use of state driver’s licenses, and studies have shown that the average age verification platform is 91% effective at screening out minors’ fake IDs. Thus, we are in a substantially different technological world than the world of *Reno*.

Next, we turn to *Ashcroft II*. There, the Court held that the Child Online Protection Act likely “failed” strict scrutiny. *Ashcroft II*, 542 U.S. at 660. The Court was not asked whether strict scrutiny was the proper standard; it merely ruled on the issue the parties presented: whether COPA would survive strict scrutiny.” *See Paxton*, 95 F.4th at 274.

B. Rule ONE Is Rationally Related to Protecting Children’s Welfare

Rational basis review simply requires that it not be “irrational” for a legislature to think it could achieve a legitimate interest through its proffered ends. Here, all agree that children’s welfare is a legitimate—even “*compelling*”—interest. *Sable Comm’cs. of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989). Having found the validity of the ends, the remaining question is whether the means and ends rationally relate. They do. The record teems with KISA’s evidence that early access to pornography harms children. Further, Rule ONE follows through on that evidence by prohibiting minors’ access to those harms.

This Court has long recognized the government’s ability to protect minors from obscenity. Given the dangers afoot today—and our children’s easy access to such dangers—we find no reason to depart from the Court’s protections for our children. Accordingly, we hold that there is little likelihood that PAC will be successful in its quest to have Rule ONE declared unconstitutional.

For the foregoing reasons, we AFFIRM the district court’s holding as to the non-delegation issue and REVERSE the district court’s holding on the First Amendment challenge. Accordingly, this case is remanded to the district court with instructions to vacate the injunction.

MARSHALL, *Circuit Judge*, dissenting:

KIKSA strikes a double blow to the liberty of the American people. First, it allows a private entity to lord the powers of state. Second, it uses those powers to impermissibly chill the speech of millions of American adults. Whatever the wisdom of KISA and its actions, the Constitution does not simply disappear because someone has stumbled upon a good policy. Rather, our charter document demands a faithful adherence to its basic structure and liberties.

Thus, I would have reversed the lower court’s private nondelegation decision, and I would have affirmed the lower court’s free speech decision. I therefore respectfully dissent.

I. KISA’S ENFORCEMENT POWERS VIOLATE THE PRIVATE NONDELEGATION DOCTRINE

Today’s majority first errs in its private nondelegation doctrine decision. It holds that the FTC’s possible power of review suffices for actual supervision. What the majority overlooks is that the Constitution requires that only those “in” whom the Constitution has vested power exercise that power. *See* U.S. Const. art. I, § 1; art. II, § 2; art. III, § 1. Without that simple requirement, the government could let anyone wield power without consequence. To avoid that, I would call Congress’s delegation of enforcement authority to KISA unconstitutional.

A. The FTC's Direct Review Is Unmeaningful

The proper test, as the majority stated, is whether the private entity “functions subordinately” to a government agency that has “authority and surveillance” over the private entity.

Like the Horseracing Act, the Keeping the Internet Safe for Kids Act plainly grants enforcement power to a private entity. The “plain terms” dictate this result. *See Black II*, 107 F.4th at 429. It is KISA who has the power to launch investigations, to levy sanctions, and to file suits. *See* 55 U.S.C. § 3054. KISKA merely grants the FTC *review* of KISA's decisions. *See id.* § 3058.

Although I concede that this review power *does* permit the FTC to unilaterally reverse KISA, such potential power, especially such power that is exercised so sparingly, is simply not enough control to prevent a private party from abusing its power. The Fifth Circuit correctly analogizes this to the role of the police officer. *Black II*, 107 F.4th at 431. Although officers' day-to-day decisions to pull people over are reviewable, this does not mean the officer *ceases to enforce*, nor does it assure that the police officer has not exceeded his authority. *Id.*

Moreover, at least *one* of KISA's enforcement powers fails to have *any* FTC restraint. 55 U.S.C. § 3054(j)(1)-(2) permits KISA to file civil suits against “technological companies” for violations of KISA regulations. The power to file civil suits is so profound that the Supreme Court has said it cannot be delegated from the executive. *See Buckley v. Valeo*, 424 U.S. 1, 138 (1976).

B. The FTC's Power to “Modify” KISA Fails to Supervise

In its brief, defendants claim that the FTC's power to “modify” KISA rules further provides an adequate level of supervision. Just as it did in amendments to the Horseracing Integrity and Safety Act, Congress permitted the FTC to “abrogate, add to, or modify the rules of the Kids Internet Safety Association.” 55 U.S.C. § 3053(e). KISA claims that this grant could authorize it to cure the defect with

the FTC's *post*-enforcement power. In short, they claim that the FTC could *require* KISA to "preclear" any enforcement action. *Black II*, 107 F.4th at 432.

But this will not do! Congress did not permit the FTC to add new jobs for itself. Instead, Congress required each entity to "implement and enforce" KISKA only "*within the scope of their powers and responsibilities under this chapter.*" 55 U.S.C. § 3054(a)(1) (emphasis added). No court can or should allow an agency to alter the face of a statute simply to save it, and no court has. In fact, the Supreme Court recently prevented the Secretary of Education from usurping powers under her statutory authority to "modify" the HEROES Act. *Biden v. Nebraska*, 143 S. Ct. 2355, 2368 (2023).

Finally, I want to acknowledge the Sixth Circuit's and majority's argument that the FTC could regulate KISKA, not by requiring pre-approval, but by creating rules modifying *how* KISA enforces. For example, the Sixth Circuit posits that the FTC could prohibit KISA from issuing "overbroad subpoenas and search warrants." *Oklahoma*, 62 F.4th at 231. But this does not resolve the problem! A private nondelegation doctrine violation does not simply go away because the private actor acts *nicely* with his government power.

C. KISA Does Not Analogize to Other Valid Enforcement Schemes

Finally, KISA analogizes itself to Financial Industry Regulatory Authority (FINRA), a private enforcement entity that has enjoyed court approval for many years. FINRA comes from the Maloney Act, on which both KISKA and the Horseracing Safety and Integrity Act are modeled. But "modeled after" does not mean "identical to."

It is true that courts have recognized the validity of FINRA and other self-regulatory organizations. *See, e.g., R.H. Johnson & Co. v. SEC*, 198 F.2d 690, 695 (2d Cir. 1952); *First Jersey Secs. Ins. v. Bergen*, 605 F.2d 690, 697 (3d Cir. 1979). But the attributes which make FINRA and the SEC's relationship work do not show up in KISA and the FTC's relationship. The SEC *shares* enforcement power with FINRA,

and the SEC alone has the power to subpoena. Further, the “SEC can also revoke FINRA’s ability to enforce its rules.” 15 U.S.C. § 78(s)(g). Moreover, the SEC can fire members of FINRA and bar members from FINRA. And what can the FTC do over KISA? None of *these* things. For this reason, KISA is not an entity subordinate to the FTC. Thus, I would reverse the lower court and protect Americans from powers with no accountability.

II. RULE ONE INFRINGES ON FREE SPEECH

In upholding Rule ONE, the majority has threatened the protected expression of millions of Americans. The First Amendment guards against such abridgment of “the freedom of speech.” U.S. Const. amend. I. Yet, despite this almost absolute protection, the majority would “reduce the adult population” to consuming “only what is fit for children.” *Butler v. Michigan*, 352 U.S. 380, 383 (1957). This type of overreach is exactly why Rule ONE should be subject to strict scrutiny.

A. Strict Scrutiny Applies

The First Amendment protects expressive speech and conduct from intrusive government overreach. *Hurley v. Irish-Am. Gay, Lesbian and Bisexual Group of Boston*, 515 U.S. 557, 570 (1995). The core principle of that right is that government cannot restrict expression “because of its message, its ideas, its subject matter, or its content.” *Nat’l Institute of Family and Life Advocates v. Becerra*, 585 U.S. 755, 766 (2018). When conduct or speech falls outside the ambit of the First Amendment, it receives rational basis review. *Ginsberg v. New York*, 390 U.S. 629, 641 (1968) (upholding a law prohibiting sale to children of material obscene for children). Children’s speech and conduct can get this treatment, but the government cannot so burden a child’s speech that it has “the potential to chill, or burden, speech outside [the] boundaries” of that group. *Counterman v. Colorado*, 600 U.S. 66, 75 (2023).

1. Precedent Requires Strict Scrutiny

The lower court cited two of at least four Supreme Court cases that dictate the application of strict scrutiny. The district court properly applied strict scrutiny because as in *Reno*, where “[the statute] effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another,” here KISA suppresses access to speech that adults have a constitutional right to receive, while also suppressing access to speech that both adults and children have a constitutional right to receive. *See Reno*, 521 U.S. at 874; *see also Ashcroft II*, 542 U.S. at 665. Despite the majority’s attempts to suggest otherwise, each of these cases involve laws promulgated for children’s welfare, and in each adults win their freedom of speech back.

2. *Ginsberg* Says Nothing to the Contrary

Nothing in *Ginsberg* requires that we apply rational basis to this case. The majority believes otherwise because *Ginsberg* upheld a regulation that, by implication, would chill adults’ access to speech. The case’s true force, however, is “its recognition of a state’s power to regulate minors in ways it could not regulate adults.” *Free Speech*, 95 F.4th at 293 (Higginbotham, J., dissenting in part and concurring in part). Further, *Ginsberg* did not challenge an *adult’s* ability to access protected speech; rather, the petitioner there argued that the law burdened *children*. *Id.* at 636.

B. Rule ONE Fails Strict Scrutiny

To satisfy strict scrutiny, the government must demonstrate that the law furthers a compelling interest in the most narrowly tailored way, and the regulation must be the “least restrictive means possible to achieve the state’s interest.” *Sable*, 492 U.S. at 126; *The Florida Star v. B.J.F.*, 491 U.S. 524, 540 (1989). Rule ONE is underinclusive because it fails to ban all the material which would, in fact, prevent children from accessing obscene materials. For every major pornographic website that the law bans, there is a website that teens can flock to that contains at least some pornographic material. *See*

Paxton, 95 F.4th at 301. Moreover, the prevalence of VPNs—and Rule ONE’s lack of attempt to deal with them—also allows children to circumvent the rules. See *Free Speech Coalition, Inc. v. Rokita*, No. 1:24-cv-00980-RLY-MG, 2024 WL 3228197, at * 10, 15 (S.D. Ind. June 28, 2024) (published). Finally, PAC offered, and the district court accepted, that two less restrictive alternatives to Rule ONE exist: (1) requiring Internet providers to block content until adults “opt out” and (2) “content filtering” that places adult controls on children’s devices. The presence of these alternatives alone is fatal to Rule ONE. Thus, for the sake of our fundamental freedoms, I dissent.

Supreme Court of the United States

No. 25-1779

PACT AGAINST CENSORSHIP, INC.

Petitioner

v.

KIDS INTERNET SAFETY ASSOCIATION, INC.

Respondent

O R D E R

The Court GRANTS the petition for certiorari review of *Kids Internet Safety Ass'n, Inc. v. Pact Against Censorship, Inc.*, 345 F.4th 1 (14th Cir. 2024). The questions before the Court are as follows:

- 1) Whether Congress violated the private nondelegation doctrine in granting the Kids Internet Safety Association its enforcement powers.
- 2) Whether a law requiring pornographic websites to verify ages infringes on the First Amendment.

APPENDIX

FROM TITLE 55 OF THE CODE OF FEDERAL REGULATIONS ("RULE ONE")

SECTION 1. DEFINITIONS

- (1) "Commercial entity" includes a corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized business entity.
- (2) "Distribute" means to issue, sell, give, provide, deliver, transfer, transmit, circulate, or disseminate by any means.
- (3) "Minor" means an individual younger than 18 years of age.
- (4) "News-gathering organization" includes:
 - (A) an employee of a newspaper, news publication, or news source, printed or on an online or mobile platform, of current news and public interest, who is acting within the course and scope of that employment and can provide documentation of that employment with the newspaper, news publication, or news source;
 - (B) an employee of a radio broadcast station, television broadcast station, cable television operator, or wire service who is acting within the course and scope of that employment and can provide documentation of that employment;
- (5) "Publish" means to communicate or make information available to another person or entity on a publicly available Internet website.
- (6) "Sexual material harmful to minors" includes any material that:
 - (A) the average person applying contemporary community standards would find, taking the material as a whole and with respect to minors, is designed to appeal to or pander to the prurient interest;
 - (B) in a manner patently offensive with respect to minors, exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated displays or depictions of:
 - (i) a person's pubic hair, anus, or genitals or the nipple of the female breast;
 - (ii) touching, caressing, or fondling of nipples, breasts, buttocks, anuses, or genitals; or
 - (iii) sexual intercourse, masturbation, sodomy, bestiality, oral copulation, flagellation, excretory functions, exhibitions, or any other sexual act; and
 - (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.
- (7) "Transactional data" means a sequence of information that documents an exchange, agreement, or transfer between an individual, commercial entity, or third party used for the purpose of satisfying a request or event. The term includes records from mortgage, education, and employment entities.

SECTION 2. PUBLICATION OF MATERIALS HARMFUL TO MINORS.

- (a) A commercial entity that knowingly and intentionally publishes or distributes material on an Internet website, including a social media platform, more than one-tenth of which is sexual material harmful to minors, shall use reasonable age verification methods as described by Section 3 to verify that an individual attempting to access the material is 18 years of age or older.
- (b) A commercial entity that performs the age verification required by Subsection (a) or a third party that performs the age verification required by Subsection (a) may not retain any identifying information of the individual.

SECTION 3. REASONABLE AGE VERIFICATION METHODS.

- (a) A commercial entity that knowingly and intentionally publishes or distributes material on an Internet website or a third party that performs age verification under this chapter shall require an individual to comply with a commercial age verification system that verifies age using:
 - (1) government-issued identification; or
 - (2) a commercially reasonable method that relies on public or private transactional data to verify the age of an individual

SECTION 4. CIVIL PENALTY; INJUNCTION

- (a) If the Kids Internet Safety Authority, Inc., believes that an entity is knowingly violating or has knowingly violated this Rule, the Authority may bring a suit for injunctive relief or civil penalties.
- (b) A civil penalty imposed under this Rule for a violation of Section 2 or Section 3 may be in equal in an amount equal to not more than the total, if applicable, of:
 - (1) \$10,000 per day that the entity operates an Internet website in violation of the age verification requirements of this Rule;
 - (2) \$10,000 per instance when the entity retains identifying information in violation of Section 129B.002(b); and
 - (3) if, because of the entity's violation of the age verification requirements of this chapter, one or more minors accesses sexual material harmful to minors, an additional amount of not more than \$250,000.
- (c) The amount of a civil penalty under this section shall be based on:
 - (1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of the violation;
 - (2) the history of previous violations;
 - (3) the amount necessary to deter a future violation;
 - (4) the economic effect of a penalty on the entity on whom the penalty will be imposed;
 - (5) the entity's knowledge that the act constituted a violation of this chapter; and
 - (6) any other matter that justice may require.
- (d) The Kids Internet Safety Association, Inc., may recover reasonable and necessary attorney's fees and costs incurred in an action under this Rule.

KEEPING THE INTERNET SAFE FOR KIDS ACT
Codified in Title 55 of the United States Code

55 U.S.C. § 3050. PURPOSE

- a. The purpose of this Act is to provide a comprehensive regulatory scheme to keep the Internet accessible and safe for American youth.

55 U.S.C. § 3051. DEFINITIONS.

1. Association. The term “Association” means the Kids Internet Safety Association, Inc., designated by section 3052(a).
2. Commission. The term “Commission” means the Federal Trade Commission.
3. Technological Industry. The term “technological industry” refers to the sector of the economy that develops, researches, and distributes advancements in computers and other electronics.
4. Technological Company. The term “technological company” refers to a business that operates in the technological industry—especially internet-based companies.
5. Technological Constituency. The term “technological constituency” refers to an individualized interests (such as web designers or executives) within the technological industry.

55 U.S.C. § 3052. RECOGNITION OF THE KIDS INTERNET SAFETY ASSOCIATION

- a. In general. The private, independent, self-regulatory, nonprofit corporation, to be known as the “Kids Internet Safety Association”, is recognized for purposes of developing and implementing standards of safety for children online and rules of the road for adults interacting with children online.
- b. Board of Directors.
 1. Membership. The Association shall be governed a board of directors (in this section referred to as the “Board”) comprised of nine members as follows:
 - A. Independent members. Five members of the Board shall be independent members selected from outside the technological industry.
 - B. Industry members.
 - i. In general. Four members of the Board shall be industry members selected from among the various technological constituencies
 - ii. Representation of technological constituencies. The members shall be representative of the various technological constituencies and shall include not more than one industry member from any one technological constituency.
 2. Chair. The chair of the Board shall be an independent member described in paragraph (1)(A).
 - A. Bylaws. The Board of the Association shall be governed by bylaws for the operation of the Association with respect to—
 - i. The administrative structure and employees of the Association;
 - ii. The establishment of standing committees;

- C. Vacancies. After the initial committee members are appointed in accordance with subparagraph (B), vacancies shall be filled by the Board pursuant to rules established by the Association.
 - 2. Chair. The chair of the nominating committee shall be selected by the nominating committee from among the members of the nominating committee.
 - 3. Selection of members of the Board and standing committees
 - A. Initial members. The nominating committee shall select the initial members of the Board and the standing committees described in subsection (c).
 - B. Subsequent members. The nominating committee shall recommend individuals to fill any vacancy on the Board or on such standing committees.
- e. Conflicts of interest. Persons with a present financial interest in any entity regulated herein may not serve on the Board. Financial interest does not include receiving a paycheck for work performed as an employee.
- f. Funding
 - 1. Initial Funding.
 - A. In general. Initial funding to establish the Association and underwrite its operations before the program effective date shall be provided by loans obtained by the Association.
 - B. Borrowing. The Association may borrow funds toward the funding of its operations.
 - C. Annual calculation of amounts required
 - i. In general. Not later than the date that is 90 days before the program effective date, and not later than November 1 each year thereafter, the Association shall determine and provide to each technological company engaged in internet activity or business the amount of contribution or fees required.
 - ii. Assessment and collection
 - I. In general. The Association shall assess a fee equal to the allocation made and shall collect such fee according to such rules as the Association may promulgate.
 - II. Remittance of fees. Technological companies as described above shall be required to remit such fees to the Association.
 - 2. Fees and fines. Fees and fines imposed by the Association shall be allocated toward funding of the Association and its activities.
 - 3. Rule of construction. Nothing in this chapter shall be construed to require—
 - A. the appropriation of any amount to the Association; or
 - B. the Federal Government to guarantee the debts of the Association.
- g. Quorum
 - 1. For all items where Board approval is required, the Association shall have present a majority of independent members.

55 U.S.C. § 3053. FEDERAL TRADE COMMISSION OVERSIGHT.

- a. In general. The Association shall submit to the Commission, in accordance with such rules as the Commission may prescribe under section 553 of Title 5, any proposed rule, or proposed modification to a rule, of the Association relating to-

1. the bylaws of the Association;
 2. a list of permitted and prohibited content for consumption by minors;
 3. training standards for experts in the field;
 4. standards for technological advancement research;
 5. website safety standards and protocols;
 6. a program for analysis of Internet usage among minors;
 7. a program of research on the effect of consistent Internet usage from birth;
 8. a description of best practices for families;
 9. a schedule of civil sanctions for violations;
 10. a process or procedures for disciplinary hearings; and
 11. a formula or methodology for determining assessments under section 3052(f) of this title.
- b. Publication and Comment
1. In general. The Commission shall—
 - A. publish in the Federal Register each proposed rule or modification submitted under subsection (a); and
 - B. provide an opportunity for public comment.
 2. Approval required. A proposed rule, or a proposed modification to a rule, of the Association shall not take effect unless the proposed rule or modification has been approved by the Commission.
- c. Decision on proposed rule or modification to a rule
1. In general. Not later than 60 days after the date on which a proposed rule or modification is published in the Federal Register, the Commission shall approve or disapprove the proposed rule or modification.
 2. Conditions. The Commission shall approve a proposed rule or modification if the Commission finds that the proposed rule or modification is consistent with—
 - A. this chapter; and
 - B. applicable rules approved by the Commission.
 3. Revision of proposed rule or modification
 - A. In general. In the case of disapproval of a proposed rule or modification under this subsection, not later than 30 days after the issuance of the disapproval, the Commission shall make recommendations to the Association to modify the proposed rule or modification.
 - B. Resubmission. The Association may resubmit for approval by the Commission a proposed rule or modification that incorporates the modifications recommended under subparagraph (A).
- d. Proposed standards and procedures
1. In general. The Association shall submit to the Commission any proposed rule, standard, or procedure developed by the Association to carry out the Anti-trafficking and exploitation committee.
 2. Notice and comment. The Commission shall publish in the Federal Register any such proposed rule, standard, or procedure and provide an opportunity for public comment.
- e. Amendment by Commission of rules of Association. The Commission, by rule in accordance with section 553 of Title 5, may abrogate, add to, and modify the rules of the Association promulgated in accordance with this chapter as the Commission finds necessary

or appropriate to ensure the fair administration of the Association, to conform the rules of the Association to requirements of this chapter and applicable rules approved by the Commission, or otherwise in furtherance of the purposes of this chapter.

55 U.S.C. § 3054. JURISDICTION OF THE COMMISSION AND THE KIDS INTERNET SAFETY ASSOCIATION

a. In general. The Association is created to monitor and assure children's safety online. Beginning on the program effective date, the Commission and the Association, each within the scope of their powers and responsibilities under this chapter, as limited by subsection (j), shall—

1. implement and enforce the Anti-Crime Internet Safety Agenda; and
2. exercise independent and exclusive national authority over the safety, welfare, and integrity of internet access to children.

b. Preemption. The rules of the Association promulgated in accordance with this chapter shall preempt any provision of law or regulation with respect to matters within the jurisdiction of the Association under this chapter. Nothing contained in this chapter shall be construed to limit the authority of the Commission under any other provision of law.

c. Duties

1. In general. The Association--

- A. shall develop uniform procedures and rules authorizing—
 - i. access to relevant technological company websites, metadata, and records as related to child safety on the internet;
 - ii. issuance and enforcement of subpoenas and subpoenas duces tecum; and
 - iii. other investigatory powers; and
- B. with respect to a violation of section 3059, the Association may recommend that the Commission commence an enforcement action.

2. Approval of Commission. The procedures and rules developed under paragraph (1)(A) shall be subject to approval by the Commission in accordance with section 3053 of this title.

d. Registration of technological companies with Association

1. In general. As a condition of participating in internet activity or business that is potentially accessible by children, a technological company shall register with the Association in accordance with rules promulgated by the Association and approved by the Commission in accordance with section 3053 of this title.

2. Agreement with respect to Association rules, standards, and procedures. Registration under this subsection shall include an agreement by the technological company to be subject to and comply with the rules, standards, and procedures developed and approved under subsection (c).

3. Cooperation. A technological company registered under this subsection shall, at all times--

- A. cooperate with the Commission, the Association, all federal and state law enforcement agencies, and any respective designee, during any civil investigation; and
- B. respond truthfully and completely to the best of the knowledge of the technological company if questioned by the Commission, the Association, all federal and state law enforcement agencies, or any respective designee.

4. Failure to comply
 - A. Any failure of a technological company to comply with this subsection shall be a violation of section 3057(a)(2)(G) of this title.
- e. Partnership programs
 - A. Use of Non-Profit Child Protection Organizations. When necessary, the Association is authorized to seek to enter into an agreement with non-profit child protection organizations to assist the Association with investigation and enforcement.
 - B. Negotiations. Any negotiations under this paragraph shall be conducted in good faith and designed to achieve efficient, effective best practices for protecting children and the integrity of technological companies and internet access to all.
 - C. Any agreement under this paragraph shall include a description of the scope of work, performance metrics, reporting obligations, and budgets. Elements of agreement. Any agreement under this paragraph shall include a description of the scope of work, performance metrics, reporting obligations, and budgets
- f. Procedures with respect to rules of Association
 1. Anti-Trafficking and Exploitation
 - A. In general. Recommendations for rules regarding anti-trafficking and exploitation activities shall be developed in accordance with section 3055 of this title.
 - B. Consultation. If the Association partners with a non-profit under subsection (e), the standing committee and partner must consult regularly.
 2. Computer safety. Recommendations for rules regarding computer safety shall be developed by the computer safety standing committee of the Association.
- g. Issuance of guidance
 1. The Association may issue guidance that—
 - A. sets forth—
 - i. an interpretation of an existing rule, standard, or procedure of the Association; or
 - ii. a policy or practice with respect to the administration or enforcement of such an existing rule, standard, or procedure; and
 - B. relates solely to—
 - i. the administration of the Association; or
 - ii. any other matter, as specified by the Commission, by rule, consistent with the public interest and the purposes of this subsection.
 2. Submittal to Commission. The Association shall submit to the Commission any guidance issued under paragraph (1).
 3. Immediate effect. Guidance issued under paragraph (1) shall take effect on the date on which the guidance is submitted to the Commission under paragraph (2).
- h. Subpoena and investigatory authority. The Association shall have subpoena and investigatory authority with respect to civil violations committed under its jurisdiction.
- i. Civil penalties. The Association shall develop a list of civil penalties with respect to the enforcement of rules for technological companies covered under its jurisdiction.
- j. Civil actions

1. In general. In addition to civil sanctions imposed under section 3057 of this title, the Association may commence a civil action against a technological company that has engaged, is engaged, or is about to engage, in acts or practices constituting a violation of this chapter or any rule established under this chapter in the proper district court of the United States, the United States District Court for the District of Columbia, or the United States courts of any territory or other place subject to the jurisdiction of the United States, to enjoin such acts or practices, to enforce any civil sanctions imposed under that section, and for all other relief to which the Association may be entitled.
 2. Injunctions and restraining orders. With respect to a civil action temporary injunction or restraining order shall be granted without bond.
- k. Limitations on authority
1. Prospective application. The jurisdiction and authority of the Association and the Commission with respect to (1) anti-trafficking and exploitation and (2) computer safety shall be prospective only.
 2. Previous matters
 - A. In general. The Association and the Commission may not investigate, prosecute, adjudicate, or penalize conduct in violation of the anti-trafficking and computer safety programs that occurs before the program effective date.
 - B. State enforcement. With respect to conduct described in subparagraph (A), the applicable State agency shall retain authority until the final resolution of the matter.
 - C. Other laws unaffected. This chapter shall not be construed to modify, impair or restrict the operation of the general laws or regulations, as may be amended from time to time, of the United States, the States and their political subdivisions relating to criminal conduct, computers, technology, or other law.

55 U.S.C. § 3055. Stop Internet Child Trafficking Program

- a. Program required
 1. In general. Not later than the program effective date, and after notice and an opportunity for public comment in accordance with section 3053 of this title, the Association shall establish the Stop Internet Child Trafficking Program.
- b. Considerations in development of program. In developing the regulations, the Association shall take into consideration the following:
 1. The Internet is vital to the economy.
 2. The costs of mental health services for children are high.
 3. It is important to assure children socialize in person as well as online.
 4. Crime prevention includes more than education.
 5. The public lacks awareness of the nature of human trafficking.
 6. The statements of social scientists and other experts about what populations face the greatest risk of human trafficking.
 7. The welfare of the child is paramount
- c. (c) Activities. The following activities shall be carried out under Stop Internet Child Trafficking Program:

1. Standards for anti-trafficking measures control. Not later than 120 days before the program effective date, the Association shall issue, by rule--
 - A. uniform standards for—
 - i. assuring the technological industry can reduce the potential of trafficking; and
 - ii. emergency preparedness accreditation and protocols; and
 - B. a list of websites known to engage in prohibited acts.
- d. Prohibition of Video Chatting. This Association shall make sure that no technological company permits minors from video chatting with strangers in an obscene way.
- e. Agreement possibilities. Under section 3054(e), this is a good opportunity to try to partner with other nonprofits.
- f. Enforcement of this Provision
 - A. Control rules, protocols, etc. When the Association opts to partner with a nonprofit under section 3054(e), the nonprofit shall, in consultation with the standing committee and consistent with international best practices, develop and recommend anti-trafficking control rules, protocols, policies, and guidelines for approval by the Association.
 - B. Results management. The Association shall assure compliance with its anti-trafficking agenda, including independent investigations, charging and adjudication of potential medication control rule violations, and the enforcement of any civil sanctions for such violations. Any final decision or civil sanction of the Association or its partnering nonprofit under this subparagraph shall be the final decision or civil sanction of the Association, subject to review in accordance with section 3058 of this title.
 - C. Testing. The Association shall perform random tests to assure that websites covered under this act comply with standards.
 - D. Certificates of compliance. The Association shall certify which websites most comply with their regulations
2. Anti-trafficking and exploitation standing committee. The standing committee shall regularly consider and pass rules for enforcement consistent with this section and its goals.
- g. Prohibition. Any website caught violating these provisions or the regulations of the Association will be prohibited from operating for an equitable period of time.
- h. Advisory committee study and report
 1. In general. Not later than the program effective date, the Association shall convene an advisory committee comprised of anti-trafficking experts to conduct a study on the use of technology in preventing such crimes.
 2. Report. Not later than three years after the program effective date, the Association shall direct the advisory committee convened under paragraph (1) to submit to the Association a written report on the study conducted under that paragraph that includes recommended changes, if any, to the prohibition in subsection (d).
 3. Modification of prohibition
 - A. In general. After receipt of the report required by paragraph (2), the Association may, by unanimous vote of the Board, modify the prohibition in subsection (d) and, notwithstanding subsection (f), any such modification

shall apply to all States beginning on the date that is three years after the program effective date.

B. Condition. In order for a unanimous vote described in subparagraph (A) to affect a modification of the prohibition in subsection (d), the vote must include unanimous adoption of each of the following findings:

- i. That the modification is warranted.
- ii. That the modification is in the best interests of most children.
- iii. That the modification will not unduly stifle industry.
- iv. That technology is a benefit to our society.

i. Baseline anti-trafficking and exploitation rules.

1. (1) In general. Subject to paragraph (3), the baseline anti-trafficking and exploitation l rules described in paragraph (2) shall--

A. constitute the initial rules of the anti-trafficking and exploitation standing committee; and

B. remain in effect at all times after the program effective date.

2. Baseline anti-trafficking and exploitation control rules described

A. In general. The baseline anti-trafficking and exploitation control rules described in this paragraph are the following:

i. The lists of preferred prevention practices from Jefferson Institute

ii. The World Prevent Abuse Forum Best Practices

iii. Psychologists Association Best Practices

B. Conflict of rules. In the case of a conflict among the rules described in subparagraph (A), the most stringent rule shall apply.

3. Modifications to baseline rules

A. Development by anti-trafficking and exploitation standing committee.

B. Association approval.

55 U.S.C. § 3056. COMPUTER SAFETY PROGRAM

a. (a) Establishment and considerations

1. In general. Not later than the program effective date, and after notice and an opportunity for public comment in accordance with section 3053 of this title, the Association shall establish a computer safety program applicable to all technological companies.

2. Considerations in development of safety program. In the development of the computer safety program, the Association and the Commission shall take into consideration existing safety standards, child development standards, existing laws protecting children, and relevant advances in technology

b. Plans for implementation and enforcement.

1. A uniform set of safety standards and protocols, that may include rules governing oversight and movement of children access to the internet.

2. Programs for data analysis.

3. The undertaking of investigations related to safety violations.

4. Procedures for investigating, charging, and adjudicating violations and for the enforcement of civil sanctions for violations.

5. A schedule of civil sanctions for violations.

6. Disciplinary hearings, which may include binding arbitration, civil sanctions, and research.
 7. Management of violation results.
 8. Programs relating to safety and performance research and education.
- c. In accordance with the registration of technological companies under section 3054(d) of this title, the Association may require technological companies to collect and submit to the database such information as the Association may require to further the goal of increased child welfare.

55 U.S.C. § 3057. RULE VIOLATIONS AND CIVIL ACTIONS

a. Description of rule violations

1. In general. The Association shall issue, by regulation in accordance with section 3053 of this title, a description of safety, performance, and rule violations applicable to technological companies.
2. Elements The description of rule violations established may include the following:
 - A. Failure to cooperate with the Association or an agent of the Association during any investigation.
 - B. Failure to respond truthfully, to the best of a technological company's knowledge, to a question of the Association or an agent of the Association with respect to any matter under the jurisdiction of the Association.
 - C. Attempting to circumvent a regulation of the Association.
 - i.the intentional interference, or an attempt to interfere, with an official or agent of the Association;
 - ii.the procurement or the provision of fraudulent information to the Association or agent; and
 - iii.the intimidation of, or an attempt to intimidate, a potential witness.
 - D. Threatening or seeking to intimidate a person with the intent of discouraging the person from reporting to the Association.
3. The rules and process established under paragraph (1) shall include the following:
 - A. Provisions for notification of safety, performance, and anti-exploitation rule violations;
 - B. Hearing procedures;
 - C. Standards for burden of proof;
 - D. Presumptions;
 - E. Evidentiary rules;
 - F. Appeals;
 - G. Guidelines for confidentiality
 - H. and public reporting of decisions.

b. Civil sanctions

1. In general. The Association shall establish uniform rules, in accordance with section 3053 of this title, imposing civil sanctions against technological companies for safety, performance, and anti-trafficking and exploitation control rule violations.
2. Modifications. The Association may propose a modification to any rule established under this section as the Association considers appropriate, and the proposed

modification shall be submitted to and considered by the Commission in accordance with section 3053 of this title.

55 U.S.C. § 3058. REVIEW OF FINAL DECISIONS OF THE ASSOCIATION

a. Notice of civil sanctions. If the Association imposes a final civil sanction for a violation committed by a covered person pursuant to the rules or standards of the Association, the Association shall promptly submit to the Commission notice of the civil sanction in such form as the Commission may require.

b. Review by administrative law judge

1. In general. With respect to a final civil sanction imposed by the Association, on application by the Commission or a person aggrieved by the civil sanction filed not later than 30 days after the date on which notice under subsection (a) is submitted, the civil sanction shall be subject to de novo review by an administrative law judge.

2. Nature of review

A. In general. In matters reviewed under this subsection, the administrative law judge shall determine whether--

i.a person has engaged in such acts or practices, or has omitted such acts or practices, as the Association has found the person to have engaged in or omitted;

ii.such acts, practices, or omissions are in violation of this chapter or the anti-trafficking and exploitation control or computer safety rules approved by the Commission; or

iii.the final civil sanction of the Association was arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.

B. Conduct of hearing. An administrative law judge shall conduct a hearing under this subsection in such a manner as the Commission may specify by rule, which shall conform to section 556 of Title 5.

3. Decision by administrative law judge

A. In general. With respect to a matter reviewed under this subsection, an administrative law judge--

i.shall render a decision not later than 60 days after the conclusion of the hearing;

ii.may affirm, reverse, modify, set aside, or remand for further proceedings, in whole or in part, the final civil sanction of the Association; and

iii.may make any finding or conclusion that, in the judgment of the administrative law judge, is proper and based on the record.

B. Final decision. A decision under this paragraph shall constitute the decision of the Commission without further proceedings unless a notice or an application for review is timely filed under subsection (c).

c. Review by Commission

1. Notice of review by Commission. The Commission may, on its own motion, review any decision of an administrative law judge issued under subsection (b)(3) by providing written notice to the Association and any interested party not later than 30 days after the date on which the administrative law judge issues the decision.

2. Application for review

A. In general. The Association or a person aggrieved by a decision issued under subsection (b)(3) may petition the Commission for review of such decision by filing an application for review not later than 30 days after the date on which the administrative law judge issues the decision.

B. Effect of denial of application for review. If an application for review under subparagraph (A) is denied, the decision of the administrative law judge shall constitute the decision of the Commission without further proceedings.

C. Discretion of Commission

i. In general. A decision with respect to whether to grant an application for review under subparagraph (A) is subject to the discretion of the Commission.

ii. Matters to be considered. In determining whether to grant such an application for review, the Commission shall consider whether the application makes a reasonable showing that--

I. a prejudicial error was committed in the conduct of the proceeding; or

II. the decision involved--(aa) an erroneous application of the anti-exploitation or computer safety rules approved by the Commission; or (bb) an exercise of discretion or a decision of law or policy that warrants review by the Commission.

3. Nature of review

A. (A) In general. In matters reviewed under this subsection, the Commission may--

i. affirm, reverse, modify, set aside, or remand for further proceedings, in whole or in part, the decision of the administrative law judge; and

ii. make any finding or conclusion that, in the judgement of the Commission, is proper and based on the record.

B. De novo review. The Commission shall review de novo the factual findings and conclusions of law made by the administrative law judge.

C. Consideration of additional evidence

i. Motion by Commission. The Commission may, on its own motion, allow the consideration of additional evidence.

ii. Motion by a party

I. In general. A party may file a motion to consider additional evidence at any time before the issuance of a decision by the Commission, which shall show, with particularity, that--(aa) such additional evidence is material; and (bb) there were reasonable grounds for failure to submit the evidence previously.

II. Procedure. The Commission may--(aa) accept or hear additional evidence; or (bb) remand the proceeding to the administrative law judge for the consideration of additional evidence.

d. Stay of proceedings. Review by an administrative law judge or the Commission under this section shall not operate as a stay of a final civil sanction of the Association unless the administrative law judge or Commission orders such a stay.

55 U.S.C. § 3059

Creating false advertisements to lure unsuspecting persons to a website shall be considered an unfair or deceptive act or practice.