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

TEAM 15

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.

APPEAL FROM THE UNITED STATES COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT

BRIEF FOR PETITIONER

[redacted]
Bar No. 123456
[redacted]
Bar No. 789012

[redacted]
[redacted]
[redacted]
[redacted]

ATTORNEYS FOR PETITIONERS

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

QUESTIONS PRESENTED vi

DECISIONS BELOW AND PROVISIONS INVOLVED 1

STATEMENT OF THE CASE 2

SUMMARY OF THE ARGUMENT 4

ARGUMENT 8

I. This Court should reverse the 14th Circuit and find that KISKA violates the private nondelegation doctrine by impermissibly delegating vested legislative and executive powers on a private entity 9

A. KISA is indeed a private entity for the purposes of performing its mandated tasks under KISKA 13

B. KISKA impermissibly delegates Congress's powers of the purse on a private entity because it fails to subordinate KISA's funding mechanisms 16

C. KISKA impermissibly delegates executive powers on a private entity because it made KISA impervious to the Presidency's oversight 21

II. This Court should reverse the 14th Circuit and find that Rule ONE's age verification requirements infringe on the First Amendment 27

A. Rule ONE's age verification requirement chills First Amendment rights 27

B. Rule ONE is a content-based restriction that must be evaluated under the heightened strict scrutiny standard 30

C. Rule ONE fails strict scrutiny 32

1. Rule ONE is not narrowly tailored. 32

CONCLUSION 37

APPENDIX 38

TABLE OF AUTHORITIES

CASES

United States Supreme Court

303 Creative LLC v. Elenis,
600 U.S. 570 (2023) 28

A.L.A. Schechter Poultry Corp. v. United States,
295 U.S. 495 (1935) 10, 20

Ashcroft v. ACLU,
542 U.S. 656 (2004) 27, 32,35

Banks v. Mayor & Controller of City of New York,
74 U.S. 16 (1868) 16

Biden v. Nebraska,
143 S. Ct. 2355 (2023) 19, 24

Bowsher v. Synar,
478 U.S. 714 (1986) 11, 22, 24, 25

Buckley v. Valeo,
424 U.S. 1 (1976) 22

Carter v. Carter Coal Co.,
298 U.S. 238 (1936) 10, 12

Clinton v. City of New York,
524 U.S. 417 (1998) 10, 11, 20, 21

Collins v. Yellen,
594 U.S. 220 (2021) 11, 20

Department of Transportation v. Assciation of Amtrak Railroads,
575 U.S. 43 (2015) 9, 10, 13, 14, 22

Dombrowski v. Pfister,
360 U.S. 479 (1965) 27

Free Enterprise Fund v. Public Company Accounting Oversight Bd.,
561 U.S. 477 (2010) 13, 21, 22

Ginsberg v. New York,
390 U.S. 692 (1968) 31

Gundy v. United States,
588 U.S. 128 (2019) 17, 23

Hampton, Jr., & Co. v. United States,
276 U.S. 394 (1928) 9, 13

Humphrey's Executor v. United States,
295 U.S. 602 (1935) 22, 24

INS v. Chadha,
462 U.S. 919 (1983) 11

Kingsley v. Regents of New York,
360 U.S. 684 (1959) 28

Lebron v. National Railway Passenger Corp.,
513 U.S. 374 (1995) 13

Lowe v. Securities and. Exchange Commission,
472 U.S. 181 (1985) 29

Metropolitan Washington Airports Authority v. Citizens for Abatement of Aircraft Noise, Inc.,
501 U.S. 252 (1991) 11

Miller v. California,
413 U.S. 15 (1973) 32

Minnesota v. Barber,
136 U.S. 313 (1980) 27

Morrison v. Olson,
487 U.S. 654 (1988) 22, 24, 25

Myers v. United States,
272 U.S. 52 (1926) 21, 22

NAACP v. Alabama,
357 U.S. (1958) 27

Panama Refining Co. v. Ryan,
293 U.S. 388 (1935) 20

Reed v. Town of Gilbert,
576 U.S. 156 (2015) 30

Reno v. ACLU,
521 U.S. 844 (1997) 31, 32

Sable Communications of California v. FCC,
492 U.S. 115 (1989) 28, 30, 32

Seila L. LLC v. Consumer Financial Protection Bureau,
591 U.S. 197 (2020) 21, 22

Stanley v. Georgia,
349 U.S. 557 (1969) 28

Sunshine Anthracite Coal Co. v. Adkins,
310 U.S. 381 (1940) 11, 12, 13, 22

United Public Workers of America v. Mitchell,
330 U.S. 75 (1947) 26

United States v. Carolene Products Co.,
304 U.S. 144 (1938) 27, 32

United States v. Playboy Entertainment Group, Inc.,
529 U.S. 803 (2000) 27, 30, 31

United States v. Rahimi,
602 U.S. 680 (2024) 26

Wayman v. Southard,
23 U.S. 1 (1825) 9

West Coast Hotel Co. v. Parrish,
300 U.S. 379 (1937) 27

West Virginia v. Envirnomental Protection Agency,
597 U.S. 697 (2022) 9

Whitman v. American Trucking Associations, Inc.,
531 U.S. 457, 472 (2001) 9, 13

United States Court of Appeals

Alpine Securities Corp. v. Financial. Industry Regulatory Authority,
121 F.4th 1314 (D.C. Cir. 2024) 11, 22

Big Time Vapes, Inc. v. FDA,
963 F.3d 436 (5th Cir. 2020) ..... 17 ,23

Bloomberg L.P. v. Securities and Exchange Commission
45 F.4th 462 (D.C. Cir. 2022) 17, 19

Consumers' Research. Cause Based Commerce, Inc. v. FCC,
109 F.4th 743 (5th Cir. 2024) 16, 17, 19

Free Speech Coal. Inc. v. Paxton,
95 F.4th 263 (5th Cir. 2024) 31

Kerpen v. Metro. Washington Airports Auth.,
907 F.3d 152 (4th Cir. 2018) 10

Kids Internet Association, Inc. v. Pact Against Censorship
R. 7 (14th Circuit 2024) 12, 25

National Horsemen's Benevolent & Protective Association v. Black,
53 F.4th 869 (5th Cir. 2022) 10, 12

National Horsemen's Benevolent & Protective Association v. Black,
107 F.4th 415 (5th Cir. 2024) 13, 14

Oklahoma v. United States,
62 F.4th 221 (6th Cir. 2023) 10

Pittston Co. v. United States,
368 F.3d 385 (4th Cir. 2004) 17, 19

United States v. Frame,
885 F.2d 1119 (3d Cir. 1989) 17, 19

Walmsley v. Federal Trade Commission,
117 F.4th 1032 (8th Cir. 2024) 10, 12

CONSTITUTIONAL PROVISIONS

Article II Section 1 21

Article II Section 2 21

Article III 26

U.S. Const. amend. I 5

STATUTES, REGULATIONS, AND COURT RULES

55 C.F.R. app. § 2 .....8, 31,33, 34, 35

55 C.F.R. app. § 4 37

55 C.F.R. app. § 5 29

55. U.S.C. § 3052.....15,17, 18, 19, 23, 25

55. U.S.C. § 3053..... 18, 23, 24, 26

55. U.S.C. § 3054.....15, 19, 23, 24, 25

55. U.S.C. § 3056.....30

55. U.S.C. § 3057..... 15, 23, 24

55. U.S.C. § 3058..... 15, 24, 25, 26

OTHER SOURCES

2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High,
Identity Theft Resource Center (2024).....33

Agency Finance in the Age of Executive Government,
Christopher C. DeMuth, Sr., Michael S. Greve 24 Geo. Mason L. Rev. 555 (2017).....9

December 2023 Healthcare Data Breach Report,
Steve Adler, The HIPPA Journal (2024).....33

Federalist No. 51,
James Madison.....10

Federalist No. 58,
James Madison.....16

Federalist No. 70,
Alexander Hamilton.....16

Glossary,
United States Department of Commerce (undated) 36

Fragmenting the Unitary Executive: Congressional Delegations of Administrative Authority Outside the Federal Government,
Harold J. Krent 85 Nw. U. L. Rev. 62 (1990) 10

How to Explain Zero-Knowledge Protocols to Your Children,
Jean-Jacques Quisquater, et al. (2001) 36

Reconsidering the Nondelegation Doctrine: Universal Service, the Power to Tax, and the Ratification Doctrine,
Ronald J. Krotoszynski, Jr., 80 Ind. L.J. 239 (2005) 16

Speech, Intent, and the Chilling Effect,
Leslie Kendrick, 54 William & Mary L. Rev. 1633 (2013) 27

Standing in the Age of Data Breaches: A Consumer-Friendly Framework to Pleading Future Injury,
John E. McLoughlin, 88 Brook. L. Rev. 923 (2023) 28

The Cost of Malicious Cyber Activity to the U.S. Economy,
United States Council of Economic Advisors (2018) 34

Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs,
Kenneth A. Bamberger, et al., 37 Berkeley Tech. L.J. (2022) 36

What Is a Database?,
Oracle (2020) 34

Why Data Breaches Spiked in 2023,
Stuart Madnick, Harvard Bus. Rev. (2024) 35

QUESTIONS PRESENTED

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.

DECISIONS BELOW

The 14th Circuit's opinion is reported at 345 F.4th 1. (14th Cir. 2024).

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

Article I of the United States Constitution:

- Section 1: All legislative Powers herein granted shall be vested in a Congress of the United States. U.S. Const. Art. I. § 1.

Article II of the United States Constitution:

- Section 1: The executive Power shall be vested in a President of the United States of America. U.S. Const. Art. II § 1.
- Section 2: He shall…appoint…all other Officers of the United States, whose Appointments are not herein otherwise provided for, and which shall be established by Law: but the Congress may by Law vest the Appointment of such inferior Officers, as they think proper, in the President alone, in the Courts of Law, or in the Heads of Departments. U.S. Const. Art. II § 2.

Article III of the United States Constitution:

- Section 1: The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. U.S. Const. Art. III § 1.

First Amendment to the Constitution:

- "Congress shall make no law . . . abridging the freedom of speech, or of the press; or . . . to petition the Government for a redress of grievances." U.S. Const. Amend I.

STATEMENT OF THE CASE

A. Statement of the Facts

To restrict the amount of pornographic material available on the internet available to minors, Congress enacted the passed the Keeping the Internet Safe for Kids Act ("KISKA") which, in 2023, resulted in the creation of an entity called Kids Internet Safety Association, Inc. ("KISA" or "Respondents"). R. 2. KISA is a "private, independent, self-regulatory nonprofit corporation. R. 2 Congress used KISKA to design KISA in a manner conducive to self-directed operations. R. 2. Indeed, it expressly declined to constrain KISA within a strict set of rules. R. 2. Instead, it empowered it to govern the rapidly changing challenges of the internet landscape on its own. R. 2. Accordingly, through KISKA, Congress delegated both broad rulemaking authority and expansive enforcement powers to KISA. R. 3.

KISA's first act was to pass a regulation popularly known as "Rule ONE." R. 3. Rule ONE imposed age verification requirements on a vast audience. R. 3-4. It compelled any kind of commercial entity that "knowingly and intentionally" published and distributed material on the internet to implement measures to verify their user's government-issued ID (or suitable alternatives) when the material they published and distributed contained an amount of explicit material amounting to 10% of the total. R. 3-4. Persons subject to Rule ONE were not allowed to retain any personal data they acquired through these verification methods. R. 4. Rule ONE allows KISA to impose heavy fines on noncompliant persons: up to $10,000 per every day of noncompliance and up to $ 250,000 for every time a minor accessed a noncompliant's website during the period of noncompliance and was exposed to explicit material. R. 4.

Petitioners Pact Against Censorship, comprising both private individuals and business representatives of the entities subject to Rule ONE enforcement, gathered evidence that Rule

ONE's expansive jurisdiction would affect even sites whose content is largely inoffensive to Rule ONE's purpose, such as websites primarily focused on promoting job and educational opportunities. R. 4. They also gathered expert evidence to reveal the significant flaws in Rule ONE's age verificiation scheme – such as the ease with which age verification measures can be circumvented, even by children. R. 5. These experts pointed out, for example, that even children as young as 6 are able to circumvent commercial security measures. R. 5. Conversely, there was some testimony that internet filtering and blocking software could prevent juvenile access to explicit material on the internet. R. 5.

On the strength of this evidence, these individuals and business representatives filed suit in federal court. R. 5.

B. Procedural History

Pact Against Censorship filed suit against Respondents in the United States District Court for the District of Wythe on August 15, 2023. R. 5. They sought a permanent injunction against both Rule ONE and KISA's continued authority over their activities on the internet, on the grounds that KISA's powers violated the private nondelegation doctrine and that Rule ONE violated their First Amendment Rights. R. 5. They further asked the district court for a preliminary injunction. R. 5. Pact Against Censorship did not prevail in its private nondelegation arguments, but did convince the district court that Rule ONE violated the First Amendment. R. 5. This appeal results from Respondents' challenge to the district court's First Amendment ruling and from Pact Against Censorship's cross-appeal of its private nondelegation decision. R. 5.

SUMMARY OF THE ARGUMENT

Parties raise two questions before this Court: (1) Whether Congress violated the private nondelegation doctrine in granting the Kids Internet Safety Association ("KISA") its enforcement powers; (2) Whether a law requiring pornographic websites to verify ages infringes on the First Amendment. We submit our answers to each in turn.

Question 1: Yes. Congress violated the private nondelegation doctrine

The private nondelegation doctrine emerges logically from the Constitution's Vesting Clauses. These establish the separation of powers inherent in the United States constitutional order. Only the Congress may legislate. Only the Presidency may enforce the law. Only the Supreme Court may interpret the law and settle disputes.

It follows that only an entity within this arrangement can exercise these powers. It also follows that no entity outside this arrangement can exercise these powers. This Court has always ruled accordingly, viewing private assumption of constitutional powers with deep suspicion if not outright hostility since the earliest days of the Republic.

That said, mindful of the reality of modern administration, this Court has allowed private entities to exercise vested powers only in very limited circumstances. Congress can subdelegate a vested powers on a private entity through a government agency, so long as there is little question that the entity is subordinate to the agency's specific power over its use of the vested power.

KISKA unquestionably subdelegates vested powers onto KISA. KISA is unquestionably a private entity, over which the FTC is supposed to maintain control. But the FTC's control over KISA's exercise of these subdelegated powers is only nominal and entirely inadequate to keep KISA in a subordinate position.

KISKA grants KISA an unfettered power to borrow money without giving the FTC the power to limit either the amounts or the provenance of these monies. KISKA also grants KISA expansive law enforcement powers, but makes its leadership and governance wholly impervious to both the Presidency and the FTC's participation.

As a result, KISA is that creature which the Founders most feared—an entity combinging powers of the purse and powers of the sword, but wholly unaccountable to the people. No reasonable person would conclude that KISA is subordinate to the FTC. Therefore, Congress violated the private nondelegation doctrine when it granted KISA its enforcement powers.

Question 2: Yes. Requiring porn sites to verify ages violates the First Amendment

The First Amendment provides "Congress shall make no law . . . abridging the freedom of speech, or of the press; or . . . to petition the Government for a redress of grievances." U.S. CONST. amend I.

As pertinent here, a law infringes on the First Amendment when (1) it dissuades citizens from exercising a fundamental right by (2) facially discriminating against the exercise of said right (3) without being narrowly tailored to achieve a compelling governmental interest. As all of these requirements have been met in this case, the appellate court's denial of injunctive relief to the Petitioners should be reversed.

To begin, citizens have a First Amendment free speech right to access pornographic materials. Moreover, First Amendment free speech extends to the right to create and maintain websites featuring constitutionally protected speech. Relatedly, speech has been unconstitutionally chilled when a law Here, First Amendment rights have been chilled. Specifically, Rule ONE has intimidated patrons of online pornography providers into no longer accessing the materials out of fear that their private viewing habits will be made public. Additionally, this chilling effect has

implications that impact the free speech rights of the website hosts whose platforms feature sexually explicit content. As more adults sacrifice their free speech rights in favor of privacy, fewer will visit webpages that require them to input identifying information such as their driver's license or credit card number. In turn, more website hosts will be forced to cease operations due to a lack of traffic. Further, even if the websites do not see a material decline in viewership, they will be coerced into exhausting time and capital obtaining and maintaining age verification data systems and software. As these website hosts have a constitutional right to disseminate the speech promoted on their forums, their First Amendment right has been unconstitutionally chilled by these burdens.

Further, the First Amendment right to freedom of the press has been limited here. The legislature took care to specify that Rule ONE does not apply to bona fide news organizations or news reporters. However, the freedom of the press is not the freedom of established newscasting agencies. Each individual has the right to make protected speech public. Thus, to require sole proprietors to age verification procedures in order to continue exercising their fundamental right is impermissible.

Moreover, and perhaps most concerningly, the right to petition the Government for redress has been iced out entirely. Rule ONE states that the law gives KISA the right to compel binding arbitration with respect to commercial entities that violate the age-verification mandate. This act of the government effectively stripping away citizens' right to seek redress in a court of law is chilling in that it forces compliance with a demonstrably unconstitutional law.

Secondly, a content-based restriction is defined as a limitation on a First Amendment right that targets speech based solely on its substance. Here, Rule ONE is a content-based restriction. Specifically, Rule ONE expressly targets pornographic material. Furthermore, where a restriction is content based, it must be evaluated under the heightened standard of strict scrutiny.

Finally, strict scrutiny requires that a statute be narrowly tailored to achieve a compelling governmental interest. The interest of the government in keeping minors safe from the threat of emotional, psychological, and developmental harms that stem from exposure to adult content at a young age is undoubtedly compelling. Relatedly, a law is narrowly tailored when it is the least restrictive means of achieving the underlying goal of the legislation. Here, Rule ONE is not narrowly tailored to achieve any interest, let alone one so critical. Specifically, age verification as mandated by the law is fraught with risk and has not been demonstrated to effectively curtail minors' access to pornography. Moreover, less restrictive means of protecting children from sexually explicit materials exist. Additionally, the potential for civil sanctions against website hosts for exercising a right guaranteed by the Constitution further reveals the lack of narrow tailoring.

Accordingly, Rule ONE infringes on the First Amendment.

Conclusion:

For the reasons set forth above, Petitioners ask that this Court reverse the 14th Circuit, rule that the Keeping the Internet Safe for Kids Act violates the private nondelegation doctrine, that Rule ONE violates the First Amendment, and grant them the injunctive relief they seek.

ARGUMENT

Parties raise two questions before this Court: (1) Whether Congress violated the private nondelegation doctrine in granting the Kids Internet Safety Association ("KISA") its enforcement powers; (2) Whether a law requiring pornographic websites to verify ages infringes on the First Amendment.

Regarding the first question: KISA is unquestionably a private entity upon whom Congress has unquestionably granted enormous vested powers, and a private entity over which neither the FTC, nor the Presidency, can exercise meaningful specific oversight. As a result, KISA consolidates significant and unfettered legislative and executive powers, making the private nondelegation doctrine a welcome and necessary corrective to the impermissible delegation of vested powers that Congress effectuated through the Keeping the Internet safe for Kids Act ("KISKA").

Regarding the second question: significantly, Rule ONE as written does not just apply to websites that have a primary purpose of distributing sexually provocative content. 55 C.F.R. app. § 2(a). Rule ONE considers any online media provider featuring content, at least one-tenth of which is sexual in nature, to be sufficiently lascivious such that age verification is required. *Id.* Thus, what is truly at issue here is whether requiring citizens to sacrifice personal privacy to exercise rights granted to them by the Constitution is a violation of that very same document.

I. This Court should reverse the 14th Circuit and find that KISKA violates the private nondelegation doctrine by impermissibly delegating vested legislative and executive powers on a private entity

The nondelegation doctrine means quite clearly that no entity other than the constitutionally vested government branch can assume a power which the Vesting Clauses confer strictly and exclusively to that branch, regardless of whether such conferral may be authorized by legislation. *Department of Transportation v. Assciation of Amtrak Railroads*, 575 U.S. 43, 67 (2015) (THOMAS, C. concurring). Indeed, the plain text of the Vesting clauses permit no delegation of those powers. *Whitman v. Am. Trucking Associations*, 531 U.S. 457, 472 (2001). Arising from this first principle, the nondelegation doctrine is one of the judiciary's original, most powerful, and ultimate checks on the expansion of a purportedly limited government and on its encroachment on the rights and liberties of the American people. See *West Virginia v. Envirnomental Protection Agency*, 597 U.S. 697, 739 (2022) (GORSUCH, N. concurring).

That said, mindful of the complexities of modern administration, this Court has allowed Congress to delegate some lawmaking authority, such that many *de jure* branch-specific powers are nowadays *de facto* distributed. See Christopher C. DeMuth, Sr., Michael S. Greve, *Agency Finance in the Age of Executive Government*, 24 Geo. Mason L. Rev. 555 (2017). But this Court has been pellucid ever since the earliest days of the Republic. These delegations are only permissible insofar as they faclititate Congress's efforts to "secure the exact effect intended by its acts of legislation" and do not insulate the government from accountability to the citizenry. *J.W. Hampton, Jr., & Co. v. United States*, 276 U.S. 394, 406 (1928) (in line with the original reasoning of *Wayman v. Southard*, 23 U.S. 1, 42-43 (1825)).

Delegating governmental powers to private entities is a particular instance that this Court and the Circuits have consistently viewed as conflicting with the Constitutional order[1]. The courts' firm stance on the matter is faithful to the Founders' original concern that the size, scope, and – most importantly – the actions of the federal government be limited by its accountability to the citizenry. See *Federalist No. 51* ("[a] dependence on the people is, no doubt, the primary control on the government[.]"). As a result, not only is delegation of government powers vested by the Constitution in a specific branch of government to private entities "unknown to our law" and "utterly inconsistent with the constitutional prerogatives and duties of Congress[,]" *A. L. A. Schechter Poultry Corp. v. United States*, 295 U.S. 495, 537 (1935), it is without "even a fig leaf of justification," *Amtrak Railroads* at 62 (ALITO, J., concurring) and "delegation in its most obnoxious form[,]" *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936).

This Court has rightly been hostile to the delegation of core government powers to private entities outside the constitutional order because it undermines the latter's carefully engineered separation of powers. *Clinton v. City of New York*, 524 U.S. 417, 449 (1998) (KENNEDY, A. concurring). Consider the following example. Via their appointment power, Presidents can shape the implementation of federal policy through their selection of officials. However, by assigning governmental responsibilities to private entities, Congress can remove them from the scope of the President's appointment powers, aggrandizing itself at the expense of the President's appointment power and weaken the Executive Branch's overall control over the administration of laws. See Harold J. Krent, *Fragmenting the Unitary Executive: Congressional Delegations of Administrative*

[1] E.g. *Amtrak Railroads* at 62 (ALITO, S. concurring); *Kerpen v. Metro. Washington Airports Auth.*, 907 F.3d 152, 161–62 (4th Cir. 2018); *Nat'l Horsemen's Benevolent & Protective Ass'n v. Black*, 53 F.4th 869, 880 (5th Cir. 2022); *Oklahoma v. United States*, 62 F.4th 221, 228 (6th Cir. 2023); and *Walmsley v. Federal Trade Commission*, 117 F.4th 1032, 1038 (8th Cir. 2024)

Authority Outside the Federal Government, 85 Nw. U. L. Rev. 72-74 (1990). Under the current constitutional order, the three political branches do not have free hand to reallocate vested powers and responsibilities: "[t]he Constitution's structure requires a stability which transcends the convenience of the moment." *Clinton* at 449 (KENNEDY, A. concurring)[2]. Definitionally, private delegation of a core government function pulls it out of the constitutional order, thereby undermining the all-important separation of powers by weakening a branch's ability to vigorously assert its proper authority while simultaneously weaking the citizenry's ultimate control over the government via the ballot box. See *id* at 452. And few threats to liberty are more dangerous than the existence of a "fourth branch" that operates without accountability to the to the people. *Collins v. Yellen*, 594 U.S. 220, 278–79 (2021) (GORSUCH, N. concurring in part).

That said, private delegation can be permissible under a narrow set of circumstaces. Congress can allow executive agencies to subdelegate vested powers onto private entities when these private entities are merely aiding a government agency and that government agency still retains the discretion to approve, disapprove, or modify the private entity's use of the specific subdelegated power. *Sunshine Anthracite Coal Co. v. Adkins*, 310 U.S. 381, 388 (1940). But general oversight – however otherwise granular and powerful – is not enough. See *Nat'l Horsemen's Benevolent & Protective Ass'n v. Black*, 107 F.4th 415, 428-429 (5th Cir. 2024). For a delegation of governmental authority to a private entity to be constitutional, the private entity must act only "as an aid" to an accountable government agency that retains the ultimate authority to "approve[ ], disapprove[ ], or modif[y]" the private entity's actions and decisions on delegated matters. *Alpine Securities Corp. v. Financial. Industry Regulatory Authority*, 121 F.4th 1314, 1325

[2] Referencing *Metropolitan Washington Airports Authority v. Citizens for Abatement of Aircraft Noise, Inc.*, 501 U.S. 252, 276–277 (1991); *Bowsher v. Synar*, 478 U.S. 714, 736 (1986); *INS v. Chadha*, 462 U.S. 919, 944–945, 958–959 (1983)

(D.C. Cir. 2024)[3]. Absent this power of specific control – and absent the private nondelegation doctrine – the private entity would be able to exercise power over the liberty and private property of the citizenry with only the most tenuous accountability before the public—an "intolerable and unconstitutional interference" with their rights and liberties under the ordained constitutional order. *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936).

As a result, the private nondelegation doctrine means that Congress may delegate its powers only if it maintains control over how the receipient of these powers exercises them and that recipient remains subordinate to the government. See *Sunshine Anthracite Coal Co. v. Adkins*, 310 U.S. 381, 388 (1940). All circuits are in agreement that the power to control a subdelegated power cannot exist without the ability to control the exercise – and, ultimately, the removal – of that power. See e.g. *Nat'l Horsemen's Benevolent & Protective Ass'n v. Black*, 53 F.4th 869, 888–89 (5th Cir. 2022). The Fourteenth Circuit is no exception: "the government permissibly delegates power when it retains control over the final product." *Kids Internet Association, Inc. v. Pact Against Censorship* at 7 (14th Circuit 2024).

Here, the Keeping the Internet Safe for Kids Act ("KISKA") impermissibly delegates core government powers to a private entity without endowing the Federal Trade Commission ("FTC") sufficiently specific power to approve, disapprove, or modify the Kids Internet Safety Association's ("KISA") use of those powers. KISA is unquestionably a private entity and the Act endows it with independent powers of the purse and a variety of independent enforcement powers. Therefore, KISA cannot be said to be subordinate to the government either in its subdelegated

[3] Referencing multiple cases from this Court and different circuits, e.g. *Adkins* at 388; *Association of American R.R.s v. Department of Transp.*, 896 F.3d 539, 546 (D.C. Cir. 2018); *National Horsemen's Benevolent & Protective Ass'n v. Black*, 53 F.4th 869, 880 (5th Cir. 2022); *Walmsley at* 1039–1040

exercise of core legislative powers or in its subdelegated exercise of core executive powers. Independent legislative power exclusively belongs to Congress. See *Whitman* at 472. Independent executive power belongs to the Presidency. *Free Enterprise Fund v. Public Company Accounting Oversight Bd.*, 561 U.S. 477, 496–497 (2010). KISKA therefore impermissibly delegates core government powers on a private entity, thereby standing in clear violation of the private nondelegation doctrine.

A. KISA is indeed a private entity for the purposes of performing its mandated tasks under KISKA

Whether an entity who is subdelegated to exercise a core government power is indeed private for the purposes of exercising that power is a key threshold question in a nondelegation analysis. See generally *Amtrak Railroads*. That is because delegations to public entities are reviewed under the broad 'intelligible principle' standard, *J.W. Hampton* at 409, whereas delegations to private entities must pass through the much more rigorous gauntlet of substantive subordination to a government body. *National Horsemen's II* at 424 (quoting *Adkins* at 388). The distinction between a private and a public entity is a fact-intensive question and the same entity can be considered private or public depending on the specific power it is purporting to exercise. See *Amtrak Railroads* at 55 and *Lebron v. National Railway Passenger Corp.*, 513 U.S. 374, 394 (1995) (both holding that a government's private or public status is qualified by the purpose of the specific analysis at issue in each case).

This Court's analysis of Amtrak Railroads in *Amtrak Railroads* provides the seminal roadmap for what constitutes a public entity. 575 U.S. 43, 51–53. This Court first considered Amtrak's organizational structure, finding that eight out of nine members of its Board of Directors were members of the executive appointed at various moments by the President and confirmed by

the Senate. *Id* at 51. Next, it found that Amtrak was subjected to stringent and granular annual reporting obligations directly to both Congress and the President. *Id* at 52. Lastly, it found that Amtrak was substantially dependent on federal funding to exercise its subdelegated powers. *Id* at 53. The combination of these factors led this Court to conclude that, for the rulemaking and enforcement purposes stemming from its ability to develop and issue metrics and standards to evaluate the performance of intercity passenger trains, Amtrak was operated as a public entity. *Id* at 53-54.

Conversely, the 5th Circuit laid out the seminal analysis to determine whetner an entity is considered a private entity while exercising its subdelegated power. *National Horsemen's II*. Since the issue at hand was the subdelegation of executive powers on a private entity (the Horseracing Integrity and Safety Authority, or HISA), the 5th Circuit gave careful consideration to whether it held substantive independent power over their use**.** It found that HISA's ostensible controlling authority, the FTC, did not reserve the right to direct HISA to investigate, issue subpoenas, conduct searches, press charges, or issue sanctions or file lawsuits against a covered entity. *Id* at 429. Indeed, HISA could exercise these powers with unfettered discretion – the FTC's prior approval was not required. This substantial lack of oversight and control over HISA's exercise of subdelegated executive powers led the 5th Circuit to the inescapable conclusion that HISA was indeed a private entity in this context. *Id* at 429-430.

Here, KISA is unquestionably a private entity for the purposes of exercising both its subdelegated legislative powers of the purse and its subdelegated enforcement powers. A more specific analysis on the lack of meaningful and substantive oversight over these powers follows below, but there are sufficient elements for a threshold analysis to conclude, like the Fourteenth Circuit did, that KISA is a private entity and that, therefore, questions regarding the permissibility

of KISKA's subdelegation of these powers to a private entity are proper.

KISKA creates an entity who exercises its powers in a manner much more similar to HISA than to Amtrak. Unlike Amtrak, KISA's Board of Directors, as well as the membership of its various standing and nominating committees, are not members of Congress or the Executive branch, but rather private individuals. § 3052(b)(1)(A-B); § 3052(c)(1)(B)(i-ii); § 3052(c)(2)(B)(i-ii); § 3052(d)(1)(A-B). It has no regular reporting obligations to the FTC. And it is entirely independent of federal funding – which it does not receive. § 3052(f).

Instead, KISA can investigate, issue subpoenas, sanctions or file lawsuits against a covered entity at its own discretion. § 3054 (h); § 3054(j). The FTC has no express power to direct KISA to do so, maintaining only a power to review KISA's imposition of civil sanctions. § 3058(a). Much like HISA, KISA can exercise these enforcement powers with only tenuous restriction from its ostensibly controlling government authority – in this case, the FTC's sole generic requirement that the rules for civil sanctions following violations of KISA's promulgated rules be established in advance. § 3057(b)(1).

As a result, KISA can reliably be viewed as a private entity for the purposes of this case and the question of whether KISKA violates the private nondelegation doctrine is properly addressed to this Court.

B. KISKA impermissibly delegates Congress's powers of the purse on a private entity because it fails to subordinate KISA's funding mechanisms

The power of the purse is the most fundamental prerogative of the legislature. It is the paramount power of Congress[4]. *Banks v. Mayor & Controller of City of New York*, 74 U.S. 16, 23, 19 L. Ed. 57 (1868). By controlling funding, Congress controls the lifeblood of the federal government and – by extension – is able to control its size, scope, and level of interaction with the rights and liberties of the American citizenry. See *Federalist No. 58* ("that powerful instrument by which we behold…an infant and humble representation of the people… finally reducing, as far as it seems to have wished, all the overgrown prerogatives of the other branches of the government."). Indeed, the Great Compromise of 1787[5] was reached when the framers agreed on this very point—that no entity other than Congress should have the ability to fund an indefinite expansion of its dominion. Ronald J. Krotoszynski, Jr., *Reconsidering the Nondelegation Doctrine: Universal Service, the Power to Tax, and the Ratification Doctrine*, 80 Ind. L.J. 239, 243–44 (2005).

Mindful of the importance of the power to fund to the constitutional order, the courts have permitted private entity's self-funding mechanisms to pass unchallenged only when these are statutorily and specifically placed under government control or the entity's revenue collecting powers are only ministerial in nature. E.g. *Consumers' Rsch. Cause Based Commerce, Inc. v. FCC*, 109 F.4th 743, 770-71 (5th Cir. 2024) (where the federal regulations giving the private entity the power to borrow money mandated that they only borrow it from a specific creditor and required

[4] According to the Founders, "'the most complete and effectual weapon with which any constitution can arm the immediate representatives of the people…for carrying into effect every just and salutary measure." The *Federalist No. 58* (James Madison).

[5] Also known as the Connecticut Compromise, where a deal between the large states and the smaller states regarding the vesting of powers in the House of Representatives was reached. Ronald J. Krotoszynski, Jr., Reconsidering the Nondelegation Doctrine: Universal Service, the Power to Tax, and the Ratification Doctrine, 80 Ind. L.J. 239, 243 (2005)

the entity to submit a monthly itemization of costs); *United States v. Frame*, 885 F.2d 1119, 1129 (3d Cir. 1989) (where all of the private entity's budgets became effective only upon final approval of the Secretary of Agriculture); and *Pittston Co. v. United States*, 368 F.3d 385, 395 (4th Cir. 2004) (where the private entity was only allowed to collect premiums in the amount specified by statute).

Self-funding private entities that carry out tasks on behalf of the government do currently exist. But even the self-regulating private entity to which KISA compares itself, the Financial Industry Regulatory Authority ("FINRA"), which funds itself primarily through the fees it collects from the entities subject to its purview, cannot set and charge fees without the Securities and Exchange Commission's authorization. *Bloomberg L.P. v. Sec. & Exch. Comm'n*, 45 F.4th 462, 476 (D.C. Cir. 2022). Moreover, that authorization cannot occur without FINRA showing that a proposed fee would not violate the statute pursuant to which it was created. *Id.* The law is clear: when a private entity's fees are approved with no real challenge, the courts have swiftly found an unconstitutional delegation of Congress's funding powers. E.g. *Consumers' Rsch. Cause Based Commerce* at 770-71 (finding that even *de jure* approval authority over a private entity's subdelegated powers was unlawful when it was unaccompanied by evidence of *de facto* review).

Here, KISA's funding mechanism as described in § 3052(f)(1-3) is unquestionably not subject to the FTC's power of approval, disapproval, or modification.

Nondelegation questions are generally answered via careful statutory analysis. *Big Time Vapes, Inc. v. FDA*, 963 F.3d 436, 443 (5th Cir. 2020) (quoting *Gundy v. United States*, 588 U.S. 128, 129). KISA's funding mechanisms are set out in U.S.C. § 3052(f)(1-2). § 3052(f)(1)(A) provides that "initial funding to establish [KISA] and underwrite its operations before the program effective date shall be provided by loans obtained by the association." § 3052(f)(1)(B) provides

that "[KISA] may borrow funds toward the funding of its operations." § 3052(f)(2), meanwhile, states that "[f]ees and fines imposed by [KISA] shall be allocated toward funding of [KISA] and its activities," in accordance with § 3052(f)(1)(C)(ii)(I), which states that "[KISA] shall assess a fee equal to the allocation made and shall collect such fee according to such rules as the Association may promulgate," and § 3052(f)(1)(C)(ii)(II), which states that "Technological companies as described above shall be required to remit such fees to [KISA]." As it pertains to funding, FTC oversight over KISA is set out, instead, in § 3053(a), which lists the subject matters that trigger a requirement for the FTC's approval of any related KISA rules, but also in § 3053(e), which states more generally that the FTC "may abrogate, add to, and modify" KISA's promulgated rules as it finds "necessary and appropriate."

It should be apparent to even a cursory reading of these provisions that the FTC holds no authority whatsoever to approve, disapprove, or KISA's main funding mechanisms. Nowhere in KISKA is the FTC tasked with that responsibility, either explicitly or implicitly. Moreover, KISA's borrowing powers are not included in § 3053(a)'s list of subject matters triggering KISA review. Lastly, the FTC is not required to submit any budgetary report or account of its financing and expenses to the FTC. The well-worn canon of statutory construction, that *expressio unius est exclusio alterius*, leads to the inescapable conclusion that these funding mechanisms are not subject to any kind of FTC oversight.

Nor can KISA argue that § 3053(e)'s allocation to the FTC of a general power to review any rule promulgated by KISA gives it the power to review KISA's funding mechanisms. The reason is simple: U.S.C. § 3052(f)(1)(A-B) are not a rules promulgated by KISA. For one, they logically and chronologically precede KISA's establishment, and so viewing them as rules promulgated by KISA is absurd. For another, KISKA fails to explicitly require KISA to submit

any decision to borrow money for the FTC's approval, when it otherwise does so frequently when the words 'promulgated rules' appear in a provision. See e.g. § 3054(c)(1)(A) ("[KISA] shall develop uniform procedures and rules") and § 3054(c)(2) ("The procedures and rules developed under paragraph (1)(A) shall be subject to approval by the [FTC]"). Again, *expressio unius est exclusio alterius* leads to the unavoidable conclusion that these funding mechanisms are are not subject to any kind of FTC oversight. Lastly, and most importantly, § 3052(f)(1)(A-B) are rules that emanate directly from Congress—and only Congress has the power the architecture of legislation. *Biden v. Nebraska*, 143 S. Ct. 2355, 2368 (2023).

KISKA therefore endows KISA with unfettered power to fund its enforcement activities. Unlike the private entity in *Consumers' Rsch. Cause Based Commerce,* it can borrow unlimited sums from unrestricted sources and can refuse to account for any of it in front of its ostensible supervisor. 109 F.4th at 770-71. Unlike one in *Frame,* it has total and unreviewable discretion to establish its own operating budgets. 885 F.2d at 1129. Also unlike the one in *Pittston,* it has total and unreviewable discretion to require companies subject to its purview to remit whatever fees it desires. 368 F.3d at 395.

Its comparison to FINRA also fails. KISA does not have to show its ostensible supervisor that any of its funding mechanisms comply with any kind of framework legislation. FINRA, instead, must. *Bloomberg* at 476. Instead, KISA's funding enjoys an independence from government supervision far greater than the mere 'rubber stamp' the 5th Circuit invalidated in *Consumers' Rsch. Cause Based Commerce* at 770-71. The necessary conclusion is that KISKA gives KISA unprecedented autonomy in all senses of the word.

This Court has long recognized the dangers of allowing a private entity to hold such unfettered powers, otherwise exclusively vested in a specific branch of government. See *Panama Refining Co. v. Ryan*, 293 U.S. 388, 430 (1935)*; Schechter* at 541–42. Unfettered power of the purse outside the control of government is especially noxious to the Constitutional order. As Justice Kennedy wrote: "Money is the instrument of policy and policy affects the lives of citizens. The individual loses liberty in a real sense if that instrument is not subject to traditional constitutional constraints." *Clinton* at 451. Justice Gorsuch concurred that in such cases:

> The chain of dependence between those who govern and those who endow them with power is broken. Few things could be more perilous to liberty than some "fourth branch" that does not answer even to the one executive official who *is* accountable to the body politic.

Collins at 278–79 (internal citations omitted). As currently written, KISKA decidedly breaks this chain of dependence. No entity with KISA's autonomy in terms of funding can plausibly be said to be under the supervision or control of any other entity while it exercises such a fundamental government power. Should KISA's unaccountable funding mechanisms be allowed to stand, this Court would pave the way for just that fourth branch of government, who would encroach upon the rights and liberties of the people without any basis in the Constitution – a power with no accountable body.

To prevent this specter from materializing, and since the Keeping the Internet Safe for Kids Act clearly allows a private entity to assume and exercise Congress's core powers of the purse without the slightest oversight, this Court should reverse the Fourteenth Circuit and rule that the Keeping the Internet Safe for Kids Act violates the private nondelegation doctrine and impermissibly delegates powers strictly and exclusively vested in Congress to a private entity.

C. KISKA impermissibly delegates executive powers on a private entity because it made KISA impervious to the Presidency's oversight

The Constitution vests the power to enforce the laws of the United States in the Presidency. Art. II, § 1; Art. II, § 3. And independent executive power is only properly exercised by the Presidency. *Free Enterprise Fund* at 496–497. The Constitution vests ultimate responsibility for the actions of the Executive branch in the person of the President, which necessarily implies the impermissibility of defraying a President's power to supervise officers of the executive branch to the point of futility. *Id* (referencing *Clinton* at 712–713 (BREYER, J. concurring)). Such responsibility is fundamental to the proper functioning of the ordained Constitutional order. As Alexander Hamilton noted in his arguments in favor of an energetic and accountable executive:

> …the plurality of the Executive tends to deprive the people of the two greatest securities they can have for the faithful exercise of any delegated power, first, the restraints of public opinion, which lose their efficacy, as well on account of the division of the censure attendant on bad measures among a number, as on account of the uncertainty on whom it ought to fall; and, secondly, the opportunity of discovering with facility and clearness the misconduct of the persons they trust, in order either to their removal from office or to their actual punishment in cases which admit of it.

Federalist No. 70. Scarred by the weakness and ineffectiveness of the Articles of Confideration during the Revolution, and persuaded by arguments like Hamilton's, the Founders coalesced around the idea of a strong executive with the sole responsibility of exercising independent executive power. *Myers v. United States*, 272 U.S. 52, 116–17 (1926).

In recent years, this Court has reaffirmed that the power to appoint and remove officers of the executive branch is inextricable from the President's sole responsibility for independent executive authority. *Seila L. LLC v. Consumer Fin. Prot. Bureau*, 591 U.S. 197, 204 (2020) (referencing *Free Enterprise Fund* and holding that a power which "follows from the text of Article II" and which has been settled since "the First Congress"). Indeed, throughout its long tenure, this Court has recognized only two exceptions to such power. *Id.* Government bodies with

quasi-judicial and quasi-legislative functions can be insulated from the executive since they are not properly part of it. *Humphrey's Executor v. United States*, 295 U.S. 602, 628 (1935). And Congress is allowed to circumscribe the executive branch's ability to remove inferior executive officers in a limited fashion, such as requiring that they be removed only for 'good cause,' provided that ultimate power of removal remain within the executive branch and that its exercise require no Congressional approval. *Morrison v. Olson*, 487 U.S. 654, 691–94 (1988). Narrow exceptions indeed. In fact, the general rule of law remains that Congress, nor any entity for that matter, may draw away from the executive the right to participate in the exercise of its constitutionally vested powers. *Bowsher v. Synar*, 478 U.S. 714, 724 (1986).

Such powers do not only include the power to appoint and remove executive officers, but also include the discretion to exercise many of the enforcement powers at issue in this case. These are: initiating and conducting civil litigation to vindicate public rights (*Buckley v. Valeo*, 424 U.S. 1, 138 (1976)); setting enforcement priorities and determining what penalties to impose on private parties (*Seila L.* at 225); the ability to impose those penalties, especially if monetary (*id* at 219); and the power to start, stop, or alter a regulatory Board's individual investigations (*Free Enterprise Fund* at 504). These powers – as this Court has reiterated time and again – cannot be exercised outside of the ultimate supervision of the President. *Amtrak Railroads* at 62 (2015) (ALITO, J. concurring); see also *Seila L.* at 204; *Free Enterprise Fund* at 496-497; and *Myers* at 116-117. A private entity can only exercise them when, as discussed above: it remains subordinate to the government, see *Adkins* at 388; and the government maintains ultimate authority "approve[ ], disapprove[ ], or modif[y]" the private entity's actions and decisions on delegated matters. *Alpine Securities* at 1325.

Here, KISA's unfettered discretion to exercise its broad enforcement powers, as described

in § 3054 and 5 U.S.C. § 3057, is unquestionably not subordinate to the FTC, who holds no authority whatsoever to approve, disapprove, or modify KISA's ability to exercise these powers.

Once again, since this case presents a nondelegation question, a careful statutory analysis is required. *Big Time Vapes* at 443 (quoting *Gundy* at 129). Under KISKA, KISA is governed by a variety of Boards and committees. At the apex sits the Board of Directors comprised by nine members. § 3052(b)(1). Per § 3052(b)(1)(A), five of the nine must be "independent members selected from outside the technological industry" and, per § 3052(b)(1)(B)(i), four members must be "selected from the various technological constituencies." § 3052(c) requires KISA to create two further standing committees a majority of whose members must again be "independent members selected from outside the technological industry" and a minority be "selected from the various technological constituencies." § 3052(c)(1-2). The exact numbers of members these two standing committees can comprise is unknown. But initial members of the Board are appointed by a special nominating committee. § 3052(c)(3)(A). The nominating committee is comprised of "seven independent members selected from business, sports, and academia" initially set forth in KISA's governing corporate documents. § 3052(d)(1)(A-B). Thereafter, vacancies in the nominating committee are filled by the Board of Directors. § 3052(d)(1)(C).

Meanwhile, KISKA endows KISA with a variety of powers to enforce the implementation of the rules it promulgates. KISA's power to initiate civil suits and impose penalties is established in § 3054(j)(1); its power to set enforcement priorities in § 3054(g)(1)(ii); its power to create a variety of civil penalties for technology companies in § 3054(i) and § 3057(b)(1); and its power to start investigations in § 3054(h). FTC oversight over KISA's use of these powers is set out, instead, in § 3053(a), which lists the subject matters that trigger a requirement for the FTC's approval of any related KISA rules, but also in § 3053(e), which states more generally that the

FTC "may abrogate, add to, and modify" KISA's promulgated rules as it finds "necessary and appropriate." It is also set up in § 3057(b)(2), which grants the FTC power to review proposed modifications of rules pertaining KISA's rules regarding the imposition of civil sanctions, as well as § 3058, which requires KISA to submit any final decision regarding a civil sanction to review by an administrative judge, whose findings may themselves be reviewed by the FTC, per § 3058(c)(1).

Again, it should be clear from even a cursory reading of KISA's governance and enumerated enforcement powers under KISKA that KISKA positions KISA well outside the control and supervision of the executive branch. For one, governance is entrusted not to executive officers, but entirely to private individuals. Moreover, the controlling Board of Directors is allowed to select members of the committee tasked with selecting members of the Board of Directors. The FTC maintains no meaningful power to review this arrangement because, as discussed above, this arrangement is not prescribed by rules promulgated by KISA, subject to the FTC's general powers of review under § 3053(e), but is instead prescribed by legislation – and only legislation can alter it. *Biden v. Nebraska* at 2368. As a result, the executive branch is clearly prevented from participating in the appointment and removal of individuals tasked with exercising executive powers—a clear violation of the separation of powers. *Bowsher* at 724.

Nor can KISA's governance find relief from this Court's prohibition against impermissible removals of executive powers by invoking the narrow exceptions described in *Humphrey's Executor* and *Morrison*. Though KISKA does endow KISA with some quasi-legislative and quasi-judiciary powers, see e.g. § 3054(c)(1)(A) and § 3054(g) (which respectively grant KISA the power to develop rules and procedures governing private company's access to the internet and issue guidance pertaining the interpretations of its own rules), these are not central to its purpose.

What is central to its purpose is the classic executive task of implementing and enforcing "standards of safety for children online and rules of the road for adults interacting with children online" as prescribed by legislation issued by Congress. § 3052(a). Moreover, KISA's governance does not merely circumscribe the removal of executive officers for 'good cause,' a limitation permitted in *Morrison*. It entirely precludes the President from removing private individuals tasked with exercising core executive powers—an obvious violation of the separation of powers as set forth in *Bowsher*.

Indeed, as KISKA is currently written KISA's ability to exercise executive powers is effectively free from meaningful review of any kind. § 3054(g)(1)(ii) allows KISA to to set enforcement priorities, but § 3054(g)(2) only requires that KISA submit them to the FTC. It does not mandate that the FTC approve them before they can take effect – according to § 3054(g)(3), they take effect on the same date they are submitted. More concerning yet, KISA's investigative and subpoena powers under § 3054(h) are unreviewable. KISKA currently contains no provisions requiring that KISA receive any form of approval before beginning an investigation or issuing a subpoena, nor any mechanism for the FTC to do so specifically without first altering KISKA's architecture.

The 14th Circuit rightly notes that the FTC does retain the unilateral authority to overturn KISA's imposition of civil penalties under § 3058. *Kids Internet Ass'n, Inc. v. Pact Against Censorship* at 7 (14th Circuit 2024). But it overstates its significance to the question of KISA's subordination to the FTC. Not only does § 3058 apply only and specifically to final decisions regarding the imposition of civil penalties – and not, as the 14th Circuit states incorrectly, to "all enforcement actions." *Id.* § 3058(c)(1), which establishes that unilateral authority, only applies to decisions that an administrative judge makes regarding KISA's imposition of civil penalties, and

under § 3058(c)(3)(A)(ii), the FTC's review is constrained by what is "proper and based on the record" and is not, therefore, totally discretionary.

The FTC does retain a substantial power under § 3053(e) to "abrogate, add to, and modify" the rules governing KISA's behavior as it finds "necessary and appropriate." But that power is irrelevant to the case currently before this Court. Article III of the Constitution vests this Court with the power to review laws are they presently arise before it in an actual case and controversy. *United Public Workers of America v. Mitchell*, 330 U.S. 75, 89 (1947). Before this Court is a frozen statute, and this court of gravity should decide the question it raises as they clearly stand before it, without regard to hazy hypothetical alternatives. *United States v. Rahimi*, 602 U.S. 680, 713 (2024) (GORSUCH, J. concurring). Accordingly, the FTC's ability to augment KISA's accountability or to remedy the separation of powers issues raised by KISKA's current architecture in the future is irrelevant to this case.

Instead, for the reasons stated above, there is only one certain conclusion. Because its governance is entirely impervious to the FTC and the President's participation and KISKA doest not establish express review mechanisms for the vested executive powers that KISA exercises, the Keeping the Internet Safe for Kids Act confers on a private entity the unfettered ability to exercise core executive powers with an utter lack of accountability. This is hostile to the ordained constitutional order. As a result, this Court should should reverse the 14th Circuit and rule that Congtress violated the private nondelegation doctrine when it gave KISA it's enforcement powers.

II. This Court should reverse the 14th Circuit and find that Rule ONE's age verification requirements infringe on the First Amendment

As relevant here, when a statute is being challenged for a constitutional violation, it is the duty of the court to analyze whether the law "impairs or destroys constitutional rights" and whether there exists a substantial nexus between the purpose of the law and the means by which said end are legislated to be achieved. *Minnesota v. Barber*, 136 U.S. 313, 320 (1980); *West Coast Hotel Co. v. Parrish*, 300 U.S. 379, 391 (1937). Where a fundamental right has been violated or encroached upon, courts scrutinize the constitutionality of the statute under heightened scrutiny. *United States v. Carolene Products Co.*, 304 U.S. 144, 153 n.4 (1938) (acknowledging a "narrower scope for the presumption of constitutionality when legislation appears on its face to be within a specific prohibition of the Constitution, such as those of the first ten Amendments").

As more fully elaborated below, Rule ONE's age verification requirement infringes upon the First Amendment because: (1) Rule ONE's age verification requirement chills First Amendment rights; (2) Rule ONE is a content-based restriction that must be evaluated under the heightened strict scrutiny standard; and (3) Rule ONE fails strict scrutiny.

a. Rule ONE's age verification requirement chills First Amendment rights

First Amendment rights have been chilled when a law discourages, deters, or disempowers citizens from exercising them. *See Dombrowski v. Pfister*, 380 U.S. 479, 487 (1965); *see also* Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 William & Mary L. Rev. 1633, 1649 (2013). Moreover, where a law "chills" protected speech, a constitutional violation has occurred. *See NAACP v. Alabama*, 357 U.S. 449, 462-66 (1958); *United States v. Playboy Entertainment Group Inc.*, 529 U.S. 803, 812 (2000) ("[t]he distinction between laws burdening and laws banning speech is but a matter of degree"); *Ashcroft v. ACLU*, 542 U.S. 656, 666 (2004).

The freedom of adults to avail oneself to pornography pursuant to their First Amendment free speech right has long been established through precedential case law. *Stanley v. Georgia*, 349 U.S. 557, 566 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house . . . what films he may watch."); *Kingsley v. Regents of the Univ. of N.Y.*, 360 U.S. 684, 685 (1959) (holding a statute prohibiting the exhibition of films portraying "acts of sexual immorality" unconstitutional). Further, the First Amendment extends to protect the right of website hosts to portray legally protected speech on their platforms. *See 303 Creative LLC v. Elenis*, 600 U.S. 570, 587 (2023) (affirming First Amendment right of website developer to portray protected speech despite said speech being disfavored by the government before holding law compelling additional website features to be unconstitutional).

Here, the free speech right of adults to view pornography has been chilled. Specifically, several adults state they no longer access sexually explicit materials out of fear that their private viewing predilections would be made public due to the age verification requirement. R. at 4; 17. This view is not misinformed. Unfortunately, it is almost certain that at least one internet site falls within this law's purview will suffer a data breach within the next year. *See* John E. McLoughlin, *Standing in the Age of Data Breaches: A Consumer-Friendly Framework to Pleading Future Injury*, 88 BROOK. L. REV. 923, 923 (2023). Citizens' hands are bound. They are effectively being forced to either surrender their First Amendment free speech right, or accept a level of personal risk that has not yet been quantified by law's proponents. This is the very definition of an impermissible chilling.

Significantly, even where speech may be harmful to minors, it is still protected for adult enjoyment. *Sable Commc'ns of Cal., Inc., v. FCC,* 492 U.S. 115, 126-28 (1989). Thus, this is a demonstrable burden to the exercise of constitutional rights. Put simply, the end does not justify

the means. The government impermissibly seeks to protect children by making it more difficult for adults to access material that has been held as protected speech.

Further, the free speech right of website hosts to make such content available has been chilled. Even more concerningly, the right of website hosts whose primary offerings do not even include pornography are restricted. Rule ONE stands to obstruct that which is not sexually explicit in nature in an attempt to curtail unfavorable speech. The age verification requirement extends to *all* commercial internet websites distributing media featuring content at least one-tenth of which is sexual in nature. This distinction, however, is without a difference. Whether the totality of a website's material is sexually salacious or just a small percentage, protected speech is just that – protected. Rule ONE discourages website hosts from exercising their rights by forcing them to expend time and resources verifying the age of its users in violation of such users' First Amendment rights. This, too, is an unlawful infringement.

Moreover, individuals' First Amendment right to freedom of press has been chilled. Specifically, while the law asserts that it does not apply to bona-fide news organizations, such is an impermissible narrowing of the freedom of the press. *See Lowe v. Sec. Exch. Comm'n*, 472 U.S. 181, 204-211 (1985) (holding freedom of the press permitted a financial advisor to publish an investment advisory newsletter); *but see* 55 C.F.R. app. § 5. The freedom of the press refers to the right of individuals to make information and beliefs publicly available. *Id.* By forcing independent journalists to participate in age verification on their platforms that feature content more than one-tenth of which is sexual in nature, Rule One chills their right to freely publish protected speech even when pornography is a secondary offering of the site.

Finally, Rule ONE impermissibly chills the First Amendment right to petition the Government for a redress of grievances. Specifically, Rule One forces commercial entities to

submit to binding arbitration for violation of the law. § 3056(b)(6). This is especially concerning because, as demonstrated above, the law has disintegrated several First Amendment rights held by multiple groups of people.

b. Rule ONE is a content-based restriction that must be evaluated under the heightened strict scrutiny standard

As held by this Court, a statute regulating speech is a content-based restriction when it facially discriminates against a designated category of speech. *Reed v. Town of Gilbert*, 576 U.S. 156, 156 (2015). Moreover, a law facially discriminates when it explicitly names the speech being prohibited. Finally, content-based restrictions must be examined for constitutionality under the strict scrutiny standard. *Playboy*, 529 U.S. at 812.

For example, in *Playboy*, the plaintiffs challenged the enforcement of Telecommunications Act of 1996 Section 505, which restricted "sexually explicit adult programming" on cable television. *Id.* at 811. Moreover, in addition to applying to a specific category of speech, Section 505 hindered media companies whose distributions were "primarily sexually oriented[.]" *Id.* at 812. As relevant here, the government's justification for the restriction of the speech and regulation of the companies was to prevent access to sexually explicit materials by minor children. *Id.* at 803. Notably, this Court held Section 505 to be a content-based restriction. *Id.* at 812 (holding the "essence" of a content-based regulation to be its "focus . . . on the content of the speech and the direct impact that speech has on its listeners). Further, Section 505 was evaluated under the heightened standard of strict scrutiny before being held unconstitutional under its framework due to the classification of the restriction as content based. *Id.* at 813 (citing *Sable*, 492 U.S. at 126).

Here, Rule ONE is a content-based restriction necessitating strict scrutiny. Specifically, the rule constricts adults' First Amendment right to access and distribute pornographic material by virtue of its substance. Significantly, Rule ONE is even more restrictive than Section 505

mentioned above. *Playboy* at 812. As noted, Section 505 applied to website hosts whose content was "primarily" sexually explicit. Even more prohibitively, Rule ONE applies to commercial entities that "knowingly and intentionally [publish] or [distribute] materials on the internet" of which "more than one-tenth . . . is sexual in nature." 55 C.F.R. app. § 2(a). Regardless of the principal business of the corporation or entity, Rule ONE seeks to abridge all access to pornography. Thus, Rule ONE is a content-based restriction that must be evaluated under the heightened strict scrutiny standard.

Inasmuch as Respondents may argue that rational-basis review should apply pursuant to either *Ginsberg v. New York* or *Free Speech Coal. Inc. v. Paxton*, such a view is misguided. 390 U.S. 629 (1968); 95 F.4th 263, 269 (5th Cir. 2024) (internal citations omitted).

First, this Court in *Ginsberg* takes care to specifically note that the statute at issue had no implications on the free speech rights of adults. *Id.* at 634-35. Children do not have a right to access adult content due precisely to the reasons underlying Rule ONE. The law in *Ginsberg* did not burden the class of citizens who hold the right because it did not require them to surrender control of sensitive, personal information to access the content. Here, Rule ONE burdens the right of adult citizens. Specifically, it requires them to insert information into online databases without full assurance that such their privacy will not be compromised. This law burdening adults' First Amendment right *requires* strict scrutiny. *Reno v. ACLU*, 521 U.S. 844, 874 (1997) (reasoning prohibition of constitutional First Amendment rights requires that no less restrictive means could meet a compelling governmental interest).

Second, *Paxton* is distinguishable from this case in that *Paxton* focused specifically on speech that the legislature had designated as obscene for children. Such is not the case here. Rule One is not restricted to material exclusively obscene for minors. It applies to all material deemed

sexually harmful for children, the very definition of which, according to the law, *is material which is obscene for adults. See Miller v. California,* 413 U.S. 15, 26-33 (1973) (delineating three-part framework for determining obscenity). Thus, by making pornographic material synonymous with obscenity, Rule ONE has permitted the government to restrict a First Amendment right.

For all of these reasons, Rule ONE is a content-based restriction that must be evaluated under the heightened strict scrutiny standard.

c. Rule ONE fails strict scrutiny

To survive strict scrutiny, the government must demonstrate the challenged statute was (1) narrowly tailored to fulfill a (2) compelling governmental interest. *Sable*, 492 at 126; *Carolene Products Co.*, 304 U.S. at 153 n.4.

The protection of children from materials that are developmentally inappropriate and damaging is a compelling governmental interest. However, as more fully elaborated below, Rule One has not been narrowly tailored to meet this well-founded, significant concern.

i. Rule ONE is not narrowly tailored

A rule is narrowly tailored when it is the least restrictive means to achieve a compelling governmental interest. *Ashcroft*, 542 U.S. at 666 ("[t]he purpose . . . is to ensure the speech is restricted no further than necessary to achieve the goal, for it is important to ensure that legitimate speech is not chilled or punished"); *Reno v. ACLU,* 521 U.S. at 869 (holding legislation not narrowly tailored and thus unconstitutional because the "statute's denial of adult access to [pornographic materials] . . . far exceeds that which is necessary to limit the access of minors to such messages[.]"). Further, if the rule does not fulfill the overall purpose of its enactment, it is not narrowly tailored. *Reno v. ACLU,* 521 U.S. at 876. If the government may achieve its compelling interests without infringing upon the First Amendment rights of its citizens, it must do

so. Additionally, if a compelling interest obliges constitutional infringement, the government must demonstrate a narrow tailoring to overcome a ruling of unconstitutionality. *Id.* at 879.

Here, Rule ONE is not narrowly tailored. Specifically, it requires website hosts to procure software that has been proven to be inefficient at protecting the interests of both children and adults. While online technology has evolved, the concerns underlying the implications of Rule One's requirements have remained constant. *Id.* at 847. As noted above, Rule ONE requires all commercial entities whose websites feature content, more than one-tenth of which is sexually explicit, to procure technological means of verifying users' age. 55 C.F.R. app. § 2(a). The security risks associated with this mandate are deeply striking. Nearly eleven percent of all public corporations suffered at least one data breach in 2023. *2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High*, Identity Theft Resource Center (Jan. 25, 2024) https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/. For example, in the healthcare sector, over 133 million patient records were inappropriately accessed across over 700 data breaches in that same year, which was an increase from a gargantuan 52 million records breached in the year before. Steve Adler, *December 2023 Healthcare Data Breach Report*, The HIPPA Journal (Jan. 18, 2024) https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/. If the records that are often regarded as the most private and personal can be accessed by third parties through systems that are generally considered to be secure, it not unreasonable to infer that such will be the case at even higher rates on social media sites that are typically held as less trustworthy than healthcare providers.

That the law prohibits companies from retaining long term any identifying information is of no consequence. Even when databases cannot be breached, data *systems* may. A database refers

to the actual information that will need to be held by the website hosts in order to engage in internet activity under the law (e.g., driver's license number and date of birth). A database system is the overall structure managing said data, and is often provided by a third party (e.g., Microsoft SQL or Oracle). *What Is a Database?*, Oracle (Nov. 24, 2020), https://www.oracle.com/database/what-is-database/. Thus, even if the websites being bound by Rule ONE do not retain the information of users, it is entirely possible that a third party to the transaction could suffer a data breach.

The fact that Rule ONE expressly bars third parties from retaining records is also inconsequential. While the law also prohibits third parties from retaining any identification, the law is so vague that compliance is almost impossible. 55 C.F.R. app. § 2(b). The law ambiguously states they may not retain the information, but gives no further guidance. *Id.* For example, as it is unknown how long the age verification process takes, companies will have to hold on to users' personal information at least until they have received confirmation that a particular person is eighteen or older. A data breach may likely occur within this time frame, compromising the confidential information of countless private individuals. In this scenario, the commercial entity or third party is in a lose-lose situation. Either they unlawfully retain the records such that age may be verified and the patron can legally use their site, or they dispose of the records, potentially circumventing the verification process, which would also be in violation of Rule One.

Further, the United States Council of Economic Advisors found that online attacks compromising confidential information cost the American public between $57 and $109 billion in 2016. CEA, The Cost of Malicious Cyber Activity to the U.S. Economy (2018). Adjusted for inflation, the total swells to $75 to $143 billion dollars today. Moreover, the total number of data breaches reported increased markedly in 2023 – a trend that has yet to decline or stagnate. Stuart

Madnick, *Why Data Breaches Spiked in 2023*, Harvard Bus. Rev. (February 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.

Notwithstanding this current unsatisfactory state of affairs, the government is requiring virtually *all* websites to obtain similar or identical intrusive, demonstrably unsecure software or to use existing software to mine even more personal information from patrons. 55 C.F.R. app. § 2. Naturally, there is a positive correlation between how much personal data is entered into online databases and how frequently such databases are breached. If more information is able to be compromised, it will be. This could potentially lead to a shuttering of entire websites – a complete erasure of forums created precisely for American adults to exercise their First Amendment rights. As discussed above, this will certainly lead to fewer adults engaging with the websites, regardless of whether they intend to engage with sexually explicit content. R. at 4. This would mean fewer opportunities for adults to access *any* speech, not just that which the government has identified as being unfit for minor children.

Significantly, as reasoned by this Court, at least one less restrictive alternative exists to this policy restricting social media and other sites whose primary purpose is not the distribution of pornography. *Ashcroft*, 542 U.S. at 671. Rather than requiring all websites to require personal, identifying information from users just to access the site, the policy could filter out pornographic content from websites who do not primarily distribute it. *Id.* If a user is accessing a site, ninety percent of which has content that is not sexually explicit, it can be reasonably assumed that said user is not seeking out such content with a particular fervor. This policy as written, due to its overbroadness, does not protect the right of adults to access materials featuring content that is outside of the bounds of what the government is attempting to regulate here.

Of note, a less restrictive policy exists that would ameliorate privacy concerns of adults who wish to access pornographic material online. *See* Kenneth A. Bamberger, et al., *Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs*, 37 Berkeley Tech. L.J. 1 (2022). According to the National Institute of Standards and Technology's Computer Security Resource Center, a zero-knowledge proof ("ZKP") is defined as a "cryptographic scheme where a prover is able to convince a verifier that a statement is true, without providing any more information than that single bit." United States Government Department of Commerce, Glossary https://csrc.nist.gov/glossary/term/zero_knowledge_proof (last visited Jan. 19, 2025). In the case at hand, the ZKP would be utilized to enable website users to certify that they have reached the age of majority, without having to input confidential information such as a credit card or driver's license number. Generally, ZKPs work by requiring the prover to complete a series of tasks that may only be done successfully if the information they are asserting to the verifier as true actually is so. *See* Kenneth A. Bamberger, et al., *Verification Dilemmas in Law* at 41-43. They do so by transforming an assertion that must be verified digitally (e.g., that a website user is over eighteen years old) into a mathematical proof that requires no other knowledge than that very fact (such as the knowledge of a particular user's credit card number associated with a social security number or birthday). *Id.* at 31. This proof may only be satisfied if the assertion to be verified may be done so using accurate information not disclosed to the verifier. *See* Kenneth A. Bamberger, et al., *Verification Dilemmas in Law* at 31; Jean-Jacques Quisquater, et al., *How to Explain Zero-Knowledge Protocols to Your Children* (Conf. on the Theory and Application of Cryptology, 2001), https://rdcu.be/d6O95. Thus, a less restrictive alternative to age verification via the surrender of personal information does exist. The government has failed to meet its burden to narrowly tailor Rule ONE.

Further, the government has failed to demonstrate that requiring identification such as a credit card or driver's license would bar minors' access to adult material. While the appellate court took it upon itself to advance the notion that the average age verification process is "91% effective at screening out minors' fake IDs" without citing any sources repudiating such assertion, that does not address minors who will attempt to access the material with legitimate, valid identification not belonging to them. While age verification on internet platforms *may* be able to identify fraudulent identification, it surely is unable to identify when a user types in the information of a third party so that they may gain access to the site. Put differently, while age verification software may be able search governmental databases to confirm the existence of an adult, it cannot confirm that such adult is the one inputting the information into the software to begin with. Thus, the policy as written, is not tailored *at all* to achieve any governmental interest, compelling or otherwise.

Moreover, narrow tailoring is especially imperative here, where civil penalties are being threatened by the legislation. 55 C.F.R. app. § 4. The government's failure to narrowly tailor its restriction is glaring where the liberty interests of its citizens involved. The implications of the government's failure extend beyond the consequence of private citizens not being able to peruse sexual imagery. The government seeks to penalize content providers, even if the overwhelming majority of their content is not sexually charged. 55 C.F.R. app. §§ 2; 4. Under this law, it is entirely possible for content providers to be held civilly liable for not requiring age verification on websites that are not primary providers of pornography. *Id.* This law must be held unconstitutional.

CONCLUSION

For the reasons set forth above, Petitioners request this Court reverse the 14th Circuit, rule that the Keeping the Internet Safe for Kids Act violates the private nondelegation doctrine, that Rule ONE violates the First Amendment, and grant Petitioner the injunctive relief they seek.

APPENDIX

FROM TITLE 55 OF THE CODE OF FEDERAL REGULATINS
("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, transmute, 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;

iii. The procedures for filling vacancies on the Board and the standing committees; term limits for members and termination of membership; and

iv. any other matter the Board considers necessary.

c. Standing Committees.

1. Anti-trafficking and exploitation prevention committee

A. In general. The Association shall establish an anti-trafficking and exploitation prevention standing committee, which shall provide advice and guidance to the Board on the development and maintenance of the Stop Internet Child Trafficking Program.

B. Membership. The anti-trafficking and exploitation prevention standing committee shall be comprised of seven members as follows:

i. Independent members. The majority of the members shall be independent members selected from outside the technological industry.

ii. Industry members. A minority of the members shall be industry members selected to represent the various technological constituencies and shall include not more than one industry member from any one technological constituency.

iii. Qualification. A majority of individuals selected to serve on the anti-trafficking and exploitation prevention standing committee shall have significant, recent experience in law enforcement and computer engineering.

C. Chair. The chair of the anti-trafficking and exploitation prevention standing committee shall be an independent member of the Board described in subsection (b)(1)(A).

2. Computer safety standing committee

A. In general. The Association shall establish a computer safety standing committee, which shall provide advice and guidance to the Board on the development and maintenance of safe computer habits that enhance the mental and physical health of American youth.

B. Membership. The computer safety standing committee shall be comprised of seven members as follows:

i. Independent members. A majority of the members shall be independent members selected from outside the technological industry.

ii. Industry members. A minority of the members shall be industry members selected to represent the various technological constituencies.

C. Chair. The chair of the computer safety standing committee shall be an industry member of the Board described in subsection (b)(1)(B).

d. Nominating committee

1. Membership

A. In general. The nominating committee of the Association shall be comprised of seven independent members selected from business, sports, and academia.

B. Initial membership. The initial nominating committee members shall be set forth in the governing corporate documents of the Association.

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.