UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

FREE SPEECH COALITION, INC., AYLO PREMIUM LTD, AYLO FREESITES LTD, WEBGROUP CZECH REPUBLIC, A.S., NKL ASSOCIATES, S.R.O., SONESTA TECHNOLOGIES, S.R.O., SONESTA MEDIA, S.R.O., YELLOW PRODUCTION, S.R.O., PAPER STREET MEDIA, LLC, NEPTUNE MEDIA, LLC, MEDIAME SRL, MIDUS HOLDINGS, INC.,

Plaintiffs,

v.

TODD ROKITA, in his official capacity as the Attorney General of the State of Indiana,

Defendant.

Case No. 1:24-cv-980

STATEWIDE RELIEF SOUGHT

DEMAND FOR JURY TRIAL

COMPLAINT

Plaintiffs, by and through their attorneys, bring this Complaint against Defendant Attorney General Todd Rokita ("Defendant") to enjoin the enforcement of a newly passed law targeting the free speech rights of internet platforms and individuals that goes into effect July 1, 2024, as it violates both the Constitution of the United States and the federal Communications Decency Act.

NATURE OF THE ACTION

1. On March 13, 2023, the Indiana governor signed into law Senate Bill 17 ("the Act"), which goes into effect July 1, 2024. The Act joins a long tradition of unconstitutional—and ultimately failed—governmental attempts to regulate and censor free speech on the internet. The Act in effect requires Plaintiffs to block access to their websites in Indiana wholesale, unless they implement a system that requires all visitors to transmit their personal information to verify that they are at least eighteen years old. The Act's requirements are enforceable by the Indiana

Attorney General. The requirements are unconstitutional and violate the federal Communications Decency Act. Plaintiffs thus seek to enjoin the Attorney General from enforcing the unconstitutional and preempted Act.

2. Pursuant to 42 U.S.C. §§ 1983, 1988 and 28 U.S.C. §§ 2201-02, Plaintiffs seek injunctive and declaratory relief to vindicate rights, privileges, and immunities secured by the Constitution and laws of the United States. The Act violates the First, Eighth, Fifth, and Fourteenth Amendments to the United States Constitution, as well as section 230 of the Communications Decency Act.

3. The Act violates the First Amendment in two fundamental ways.

4. *First*, the Act's age verification requirement is a content- and speaker-based restriction that fails strict scrutiny. Despite impinging on the rights of adults to access protected speech, it fails strict scrutiny by employing the *least* effective and yet also the *most* restrictive means of accomplishing Indiana's stated purpose of allegedly protecting minors. Indeed, minors can use proxy servers, virtual private networks ("VPNs"), the "Tor" browser, and numerous other circumventions to bypass the Act's verification requirements with ease; the law excludes search engines and most social media sites even though they pose a *greater* risk of exposure to adult content; and protected speech will be chilled as adults refuse to risk exposing their personal information that could lead to financial or reputational harm. In contrast, content filtering at the browser and/or the device level allows anyone wishing to implement that technology on minors' devices to block access to any unwanted site, including adult sites, without impairing free speech rights or privacy. But such far more effective and far less restrictive means don't really matter to Indiana, whose true aim is not to protect minors but to squelch constitutionally protected free speech that the State disfavors.

5. *Second*, under the heightened scrutiny required by the First Amendment, the Act is incurably vague as to its fundamental requirements, providing neither a coherent standard for assessing to which websites it applies, nor adequate guidance on what "age verification" entails.

6. The Act further violates the Supremacy Clause by violating section 230 of the Communications Decency Act, which prohibits treating website operators as if they were responsible for alleged harm caused by content created and uploaded by third parties.

7. The Act violates the Fourteenth Amendment in multiple ways, too. First, the Act's indecipherable vagueness violates the basic tenets of procedural due process. Second, by destroying Plaintiffs' protected property right in the goodwill of Indiana viewers without a rational basis, it violates the substantive component of the Due Process Clause. Third, because of its arbitrary exceptions for search engines and most social media sites, it violates the Equal Protection Clause, even under rational basis review. Finally, the Act violates the Takings Clause of the Fifth Amendment, depriving Plaintiffs of their private property interests in their businesses without just compensation by forcing platforms to adopt age verification protocols they cannot afford and will cause a mass exodus of customers.

8. The Act also violates the Excessive Fines Clause of the Eighth Amendment, because it imposes fines that are grossly disproportionate to the unproven, fabricated harms it purports to protect against.

9. Accordingly, Plaintiffs seek to have the Indiana Attorney General enjoined from enforcing the Act—both preliminarily, pending the hearing and determination of this action, and permanently. Plaintiffs also seek declaratory relief, as well as damages, costs, and attorneys' fees.

JURISDICTION AND VENUE

10. This case presents federal questions within this Court's jurisdiction pursuant to Article III of the United States Constitution and 28 U.S.C. §§ 1331 and 1343(3). Plaintiffs bring this action pursuant to 42 U.S.C. §§ 1983 and 1988 (deprivation of rights, privileges, and immunities secured by the Constitution and federal law) and 28 U.S.C. §§ 2201-02 (declaratory judgment as to an actual controversy).

11. Venue is proper pursuant to 28 U.S.C. § 1391(b). The challenged law was passed in Indianapolis, Indiana, which is also where the Attorney General performs his official duties.

PARTIES

12. Defendant Todd Rokita a person within the meaning of Section 1983 of Title 42 of the United States Code; and he currently serves as the Attorney General of the State of Indiana. The Office of the Attorney General is in Indianapolis, Indiana. The Act expressly authorizes "[t]he attorney general [to] bring an action under this chapter to obtain … against an adult oriented website, accessible by an Indiana resident, that does not implement or properly use a reasonable age verification method: (1) An injunction to enjoin future violations of this chapter. (2) A civil penalty of not more than two hundred fifty thousand dollars ($250,000). (3) The attorney general's reasonable costs." I.C. 24-4-23 § 15. The Attorney General of Indiana is thus directly responsible for the enforcement of the Act.

13. Plaintiff Free Speech Coalition, Inc. ("FSC") is a not-for-profit trade association organized under the laws of California with its principal place of business in Canoga Park, California. FSC assists filmmakers, producers, distributors, wholesalers, retailers, internet providers, performers, and other creative artists located throughout North America in the exercise of their First Amendment rights and in the vigorous defense of those rights against censorship.

Founded in 1991, the Free Speech Coalition represents hundreds of businesses and individuals involved in the production, distribution, sale, and presentation of constitutionally-protected adult content disseminated to consenting adults via the internet. FSC sues on its own behalf and on behalf of its members to vindicate its own constitutional rights, its members' constitutional rights, and the rights of its members' owners, officers, employees, and current and prospective readers, viewers, and customers. Many of FSC's members are individual adult performers gravely concerned about the consequences of the Act, but who fear for their safety should they come forward publicly to challenge the Act in court. FSC's members would directly benefit from an injunction enjoining the enforcement of the Act. The potential harm to FSC's members caused by the recent enactment of state age-verification statutes has caused significant concern among its members. FSC has diverted resources away from its normal day-to-day activity, which has impaired its ability to perform its usual functions. Over the last year, both FSC's Executive Director and Director of Public Affairs have had to devote more than half their time to tracking legislative developments, meeting with FSC members to discuss risks relating to age-verification statutes, meeting with litigation attorneys and advisors, and otherwise engaging in activities to minimize the risk to its members from the age-verification statutes that states, in particular Indiana, have recently enacted.

14. Plaintiff Aylo Premium Ltd, is a limited liability company organized under the laws of the Republic of Cyprus, with its principal place of business in Nicosia, Cyprus, that operates SpiceVids.com ("SpiceVids"), a subscription-based website offering high quality adult content uploaded, owned, copyrighted, and controlled by third party content creators. Aylo Premium Ltd also operates the website Brazzers.com ("Brazzers"), a subscription-based website offering high quality adult content in which Aylo Premium Ltd holds all the intellectual property rights. For

shoots with adult performers, Aylo Premium Ltd writes the scripts, hires the production team, and does the pre- and post-production work. Aylo Premium Ltd uploads Brazzers content both to Brazzers.com and to the websites of other Plaintiffs, including Pornhub.com, xvideos.com, xnxx.com, and SpiceVids. In addition, Aylo Premium Ltd operates the website FakeTaxi.com ("FakeTaxi"), a subscription-based website offering high quality adult content that is produced and owned by Plaintiff Yellow Production, s.r.o., discussed below. Aylo Premium Ltd opposes the restrictions the Act would place on its ability to reach its audience.

15. Plaintiff Aylo Freesites Ltd, is a limited liability company organized under the laws of the Republic of Cyprus, with its principal place of business in Nicosia, Cyprus, that operates Pornhub.com ("Pornhub"), a popular free adult entertainment website that hosts content uploaded, owned, copyrighted, and controlled by third party content creators. Aylo Freesites Ltd opposes the restrictions the Act would place on the ability of its third party content creators to reach their audience.

16. Plaintiff WebGroup Czech Republic, a.s. ("WebGroup"), is a corporation organized under the laws of the Czech Republic, with its principal place of business in Prague, Czech Republic, that operates xvideos.com ("XVideos"), a popular free adult entertainment website that hosts content uploaded, owned, copyrighted, and controlled by third party content creators. WebGroup opposes the restrictions the Act would place on the ability of its third party content creators to reach their audience.

17. Plaintiff NKL Associates, s.r.o. ("NKL"), is a limited liability company organized under the laws of the Czech Republic, with its principal place of business in Prague, Czech Republic, that operates xnxx.com ("Xnxx"), a popular free adult entertainment website that hosts content uploaded, owned, copyrighted, and controlled by third party content creators. NKL

opposes the restrictions the Act would place on the ability of its third party content creators to reach their audience.

18. Plaintiff Sonesta Technologies, s.r.o. ("Sonesta Tech"), is a limited liability company organized under the laws of the Czech Republic, with its principal place of business in Prague, Czech Republic, that operates the website BangBros.com ("BangBros"), a subscription-based website offering high quality adult content. Sonesta Tech opposes the restrictions the Act would place on its ability to reach its audience.

19. Plaintiff Sonesta Media, s.r.o., ("Sonesta Media") is a limited liability company organized under the laws of the Czech Republic, with its principal place of business in Prague, Czech Republic, that produces, and owns the intellectual property rights to, the content on BangBros.com. It also licenses some of its content to be uploaded to other websites, including Pornhub, XVideos, Xnxx, and SpiceVids. Sonesta Media opposes the restrictions the Act would place on its ability to reach its audience.

20. Plaintiff Yellow Production, s.r.o. ("Yellow Production") is a limited liability company organized under the laws of the Czech Republic, with its principal place of business in Prague, Czech Republic, that produces, and owns the intellectual property rights to, the content on FakeTaxi. It also licenses some of its content to be uploaded to other websites, including Pornhub, Xvideos, Xnxx, and SpiceVids. Yellow Production opposes the restrictions the Act would place on its ability to reach its audience.

21. Plaintiff Paper Street Media, LLC ("Paper Street"), is a limited liability company organized under the laws of Florida, with its principal place in Miami, Florida, that operates the TeamSkeet adult content network, comprised of numerous subscription-based adult websites offering high quality adult content. Paper Street owns the content on its network sites and, for

shoots with adult performers, writes the scripts, hires the production team, and does the pre- and post-production work. Paper Street also makes some of the content available on the TeamSkeet network available to other adult websites, including Pornhub, XVideos, Xnxx, and SpiceVids. Paper Street opposes the restrictions the Act would place on its ability to reach its audience.

22. Plaintiff Neptune Media, LLC ("Neptune Media"), is a limited liability company organized under the laws of Florida, with its principal place of business in Miami, Florida, that operates the MYLF adult content network, comprised of numerous subscription-based adult websites offering high quality adult content. Neptune Media owns the content on its network sites and, for shoots with adult performers, writes the scripts, hires the production team, and does the pre- and post-production work. Neptune Media also makes some of the content available on the MYLF network available to other adult websites, including Pornhub, XVideos, Xnxx, and SpiceVids. Neptune Media opposes the restrictions the Act would place on its ability to reach its audience.

23. Plaintiff MediaME SRL is a limited liability company organized under the laws of Romania, with its principal place of business in Pipera, Romania, that operates the website Porndoe.com, a popular free adult entertainment websites that hosts content uploaded, owned, copyrighted, and controlled by third party content creators. MediaME opposes the restrictions the Act would place on its ability to reach its audience.

24. Plaintiff Midus Holdings, Inc., is a corporation organized under the laws of Florida, with its principal place of business in Coral Springs, Florida, that operates the websites Letsdoeit.com and Superbe.com, each a subscription-based website offering high quality

adult content within the United States. Midus Holdings opposes the restrictions the Act would place on its ability to reach its audience.

25. Furthermore, Plaintiffs are supported by at least three Jane Does, who are prepared to join as Plaintiffs if the Court permits them to proceed under pseudonym without disclosing their identities to the State of Indiana. Jane Doe No. 1 is a Oregon-based adult performer who produces, performs, and publishes adult content on websites that will be subject to the Act's age-verification requirements. Jane Doe No. 2 is an Indiana-based sex therapist and social worker who uses pornography in their treatment of patients and provision of sex education as a part of their employment. They will be chilled and burdened from accessing adult content essential to their work if the Act goes into effect. As a result, Jane Doe No. 2 will be impaired in providing treatment to patients, where pornography is helpful for treating sexual issues; taking required desensitization trainings, which include watching pornography, to obtain national licensure; and providing sexual health resources over telehealth appointments. Jane Doe No. 3 is an Indiana-based "cam" performer, who live-streams adult content and interacts with customers on a website that will be subject to the Act's age verification requirements. All will be injured in their ability to share expressive speech and earn a livelihood if the Act becomes effective; none can risk disclosure of their identities to the public or the State. The risk of State retaliation or targeting in response to Does' defense of their First Amendment rights is especially concerning and chilling.

BACKGROUND FACTS

I. The Act

26. During the 2024 legislative session, the Indiana Legislature passed Senate Bill 17, which: (1) amended Title 24, Article 4 of the Indiana Code to add Chapter 23; (2) amended Title 24, Article 4.9, Chapter 2, Section 10; and (3) amended Title 24, Article 5, Chapter 0.5, Section

3—herein referred to as "the Act." The Indiana Governor signed the bill into law on March 13, 2024, which goes into effect July 1, 2024. Chapter 23 of the Act provides in relevant part:

Chapter 23. Age Verification for Adult Oriented Websites

Sec. 1. "Adult oriented website" means a publicly accessible website that publishes material harmful to minors, if at least one-third (1/3) of the images and videos published on the website depict material harmful to minors.

Sec. 2. "Adult oriented website operator" means a person that owns or operates an adult oriented website. The term does not include the following:

(1) A newspaper or news service that publishes news related information through a website.

(2) A cloud service provider.

(3) An Internet provider, an affiliate or subsidiary of an Internet provider, or a search engine that:

(A) solely provides access or connection to a website or other Internet content that is not under the control of that Internet service provider, affiliate or subsidiary, or search engine; and

(B) is not responsible for creating or publishing the content that constitutes material harmful to minors.

Sec. 3. "Material harmful to minors" means matter or a performance described in IC 35-49-2-2.

Sec. 4. "Minor" means a person less than eighteen (18) years of age.

Sec. 5. "Mobile credential" has the meaning set forth in IC 9-13-2-103.4.

Sec. 6. "Person" means a human being, a corporation, a limited liability company, a partnership, an unincorporated association, or a governmental entity.

Sec. 7. "Reasonable age verification method" means a method of determining that an individual seeking to access a website containing material harmful to minors is not a minor by using one (1) or more of the following methods:

(1) A mobile credential.

(2) An independent third party age verification service that compares the identifying information entered by the individual who is seeking access with material that is available from a commercially available data base, or an aggregate of data bases, that is regularly used by government agencies and businesses for the purpose of age and identity verification.

(3) Any commercially reasonable method that relies on public or private transactional data to verify the age of the individual attempting to access the material.

Sec. 8. "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 that relate to a mortgage, education, or employment.

Sec. 9. "Verification information" means all information, data, and documents provided by an individual for the purposes of verification of identity or age under this chapter.

Sec. 10. An adult oriented website operator may not knowingly or intentionally publish an adult oriented website unless the adult oriented website operator uses a reasonable age verification method to prevent a minor from accessing the adult oriented website.

Sec. 11. (a) If:

(1) an adult oriented website operator knowingly or intentionally publishes an adult oriented website in violation of section 10 of this chapter; and

(2) a minor accesses the adult oriented website;

the parent or guardian of the minor who accessed the adult oriented website may bring an action against the adult oriented website operator.

(b) A parent or guardian who prevails in an action described in this section is entitled to:

(1) either:

(A) actual damages; or

(B) damages of up to five thousand dollars ($5,000);

(2) injunctive relief; and

(3) court costs, reasonable attorney's fees, and other reasonable expenses of litigation, including expert witness fees.

Sec. 12. (a) If an adult oriented website operator publishes an adult oriented website in violation of section 10 of this chapter, any person may bring an action to seek injunctive relief.

(b) A person that brings an action for injunctive relief under this section and prevails is entitled to:

(1) injunctive relief; and

(2) court costs, reasonable attorney's fees, and other reasonable expenses of litigation, including expert witness fees.

Sec. 13. (a) This section applies to a person that uses or purports to use a reasonable age verification method to grant or deny access to an adult oriented website.

(b) A person to which this section applies, and any third party verification service used by a person to which this section applies, may not retain identifying information of the person seeking access to an adult oriented website, unless retention of the identifying information is required by a court order.

(c) An individual whose identifying information is retained in Violation of this section may bring an action against the person that unlawfully retained the individual's identifying information. An individual who prevails in an action described in this section is entitled to:

(1) either:

(A) actual damages; or

(B) damages of up to five thousand dollars ($5,000);

(2) injunctive relief; and

(3) court costs, reasonable attorney's fees, and other reasonable expenses of litigation, including expert witness fees.

Sec. 14. Adult oriented website operators must use commercially reasonable methods to secure all information collected and transmitted under this chapter.

Sec. 15. The attorney general may bring an action under this chapter to obtain any or all of the following against an adult oriented website, accessible by an Indiana resident, that does not implement or properly use a reasonable age verification method:

(1) An injunction to enjoin future violations of this chapter.

(2) A civil penalty of not more than two hundred fifty thousand dollars ($250,000).

(3) The attorney general's reasonable costs in:

(A) the investigation of the violations under this chapter; and

(B) maintaining the action.

Sec. 16. When the attorney general has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in a violation of this chapter, the attorney general is empowered to issue civil investigative demands under IC 4-6-3-3 to investigate the suspected violation.

Sec. 17. In an action filed under sections 11, 12, 13, and 15 of this chapter, the verification information of a minor who accessed the adult oriented website shall remain confidential. The clerk of the court shall place all records of the minor who accessed the adult oriented website in an envelope marked "confidential" inside the court's file pertaining to the minor. Records placed in the confidential envelope may only be released to:

(1) the judge or any authorized staff member;

(2) a party and the party's attorney;

(3) the parents of a minor who accessed the adult oriented website; or

(4) any person having a legitimate interest in the work of the court or in a particular case as determined by the presiding judge or their successor who shall consider the best interests, safety, and welfare of the minor.

27. The Act amends the Indiana Trade Regulation to include in the Code's definition of "personal information": "information collected by an adult oriented website operator, or their designee, under IC 24-4-23." I.C. 24-4.9-2-10(3).

28. The Act further amends the Indiana Trade Regulation to include in the Code's "Enumeration of Deceptive Acts": "A violation of IC 24-4-23 (concerning the security of information collected and transmitted by an adult oriented website operator), as set forth in IC 24-4-23-14." I.C. 24-5-0.5-3(b)(42).

II. Communication Over the Internet

29. The internet is a decentralized, global medium of communication that links people, institutions, corporations, and governments around the world. It is a giant computer network that interconnects innumerable smaller groups of linked computer networks and individuals' computers. The internet connects an estimated 5.4 billion people—or 67% of the world's population[1]—and in Indiana, it is estimated that 77.5% of residents are internet users.[2]

30. Because the internet merely links together numerous individual computers and computer networks, no single entity or group of entities controls the material made available on the internet or limits the ability of others to access such materials. Rather, the range of digital information available to internet users is individually created, maintained, controlled, and located on millions of separate individual computers around the world.

31. The internet presents extremely low entry barriers to anyone who wishes to provide or distribute information or gain access to it. Unlike television, cable, radio, newspapers, magazines or books, the internet provides the average citizen and business, whether large or small, with an affordable means for communicating with, accessing, and posting content to a worldwide audience. Although the majority of the information on the internet does not depict or describe nudity or sexual activity, such material is indeed widely available on the internet.

32. An Internet Protocol ("IP") address is a unique address that identifies a connection to a device on the internet or a local network, much like a telephone number is used to connect a

---

[1] *Facts and Figures 2023*, INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/ (last visited June 8, 2024).

[2] *Internet Usage Penetration in the United States in November 2021, by State*, STATISTA (Dec. 12, 2023), https://www.statista.com/statistics/184691/internet-usage-in-the-us-by-state.

telephone to other telephones. In essence, an IP address is the identifier that allows information to be sent between devices on a network. Internet Service Providers ("ISPs") and telecommunications companies control "blocks" of IP addresses, and the location of an internet connection can be roughly determined according to the geo-location those companies assign to the IP address associated with a connection. In many contexts it is very common for ISPs to pre-block access to websites based on users' IP addresses, which is at least as effective as age verification by websites and harder to bypass, while still allowing adults (at non-blocked IP addresses) to freely access adult content at their discretion.

33. Websites can request that their host server block traffic from particular IP address regions ("geoblocking") or pay for expensive services that rely on GPS and data modeling to increase the accuracy of geoblocking. However, satellites and cellular towers do not respect state boundaries, and many IP-address databases are highly inaccurate. The accuracy of geolocation technology is necessarily imperfect, and residents of one state, particularly near state borders, may be mistakenly categorized as residents of another. Indeed, some blocks of IP addresses cover multiple States at once, and the accuracy of geolocating an internet user based on a user's IP address can dip as low as 55%.

34. Virtual Private Networks ("VPNs") and proxy servers, among countless other inexpensive and easily accessible technologies, bypass geoblocking by websites. Both function as an intermediary between an individual internet-connected device and the targeted server. They hide the device's actual public IP address and instead "tunnel" traffic between the device and a remote server—the only difference being that communications sent through VPNs are encrypted. Setting up a proxy server is generally free and simple, and the same is true of VPNs. Doing so permits users to obscure their location while browsing the web, whether on wireless or cellular

networks. VPNs are extremely common—used both by consumers and businesses to establish secure, remote connections to their home networks. In fact they are included by default in most consumer antivirus software.

35. The freely available "Tor" browser, which is designed to be easily downloaded and used, also hides a user's IP address when browsing the internet.

36. Even remote and virtual desktop services, which are popular among university students, allow users to appear to internet websites as though they were located wherever the cloud server (in the case of virtual desktops) or the actual computer (in the case of remote desktops) appears to be located. In all cases, the user can appear to be located in a different state or country whose laws do not require age verification by websites.

III. The Minimal Benefits of Age Verification Under the Act

37. Minors are more at risk of exposure to adult content from social media sites and search engines than traditional adult websites like Plaintiffs.[3] Search engines, by design, enable anyone to access troves of adult images and videos in seconds—content that is no less explicit than that found directly on Plaintiffs' websites. Even where adult websites implement age verification, a simple image or video search for sexually explicit terms on a search engine will yield millions of thumbnail photos and videos of content drawn from these sites.

38. Social media sites are no different. Facebook alone flagged a staggering **73.3 million** pieces of content under "child nudity and sexual exploitation" from Q1 to Q3 of 2022

[3] Neil Thurman and Fabian Obster, *The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches*, 13 POLICY & INTERNET 415, 417 (2001).

alone, not including sexually explicit content involving adults.[4] Recent research[5] found a majority of children under 13 had their own profile on at least one social media application or site and one-third of children between the ages of 8 and 17 with a social media profile signed up with a false birthdate.

39. Because most social media sites contain so much content that they will not meet the Act's "more than one-third" threshold for "sexual material harmful to minors," the Act effectively exempts most social media sites, in addition to its explicit exemption for search engines.

40. The Act also exempts erotica and other written sexually explicit material by limiting its "one-third" content threshold to adult "images and videos."

41. There are also far riskier ways to obtain adult content, such as through the Dark Web (via the freely downloadable "Tor" browser), which is replete with more extreme adult content and also a range of black markets for ransomware, sex trafficking, drugs, and even hitmen. Those determined to access adult content are likely to be pushed by the Act towards unregulated platforms, which is a more dangerous environment for users, including underage users, who would then be exposed to far more problematic online environments.

42. In addition to these alternative pathways to adult content, state-specific restrictions on traditional adult websites can be easily bypassed by VPNs and proxy servers.

---

[4] *See* Paul Bischoff, *The Rising Tide of Child Abuse Content on Social Media*, COMPARITECH, (Jan. 25, 2023), https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/.

[5] *See Children and Parents: Media Use and Attitudes Report 2022*, OFCOM, (Mar. 30, 2022), https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf.

43. All of this is magnified by the fact that minors are more tech-savvy than adults, especially older adults. Evaders of the law at the end-user level will thus largely be comprised of minors.

IV. The Burdens and Risks of Age Verification

A. The Risks to Adults

44. While rapid technological progress might suggest it's easy to verify age, in fact there is no method that does not carry inherent, unacceptable disadvantages and harms.[6] Nor does technological progress excuse First Amendment violations, or make the Act any more effective at protecting kids, or any less invasive of people's privacy, or any less dangerous in light of the broadly recognized misuse of such data[7] and vulnerability to hackers and cybersecurity attacks.

---

[6] *See, e.g.*, Jason Kelley and Adam Schwartz, *Age Verification Mandates Would Undermine Anonymity Online*, ELECTRONIC FRONTIER FOUNDATION, (Mar. 10, 2023), https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online (explaining the flaws of age verification systems and why they are the wrong approach to protecting young people online, as they would force websites to require visitors to prove their age by submitting information such as government-issued identification. "This scheme would lead us further towards an internet where our private data is collected and sold by default. The tens of millions of Americans who do not have government-issued identification may lose access to much of the internet. And anonymous access to the web could cease to exist.").

[7] *See, e.g.*, 8 F.R. 51273 (available at https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security) (requesting public comment on the prevalence of commercial surveillance and data security practices that harm consumers, and inviting comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive, recognized, among others, that data is regularly collected for one purpose and used for another).

45. Hackers are targeting information shared on the Internet at exponentially high rates, including data kept in the safest locations—including federal and state agencies, which have themselves been subjected to multiple breaches.[8]

46. Any claimed benefit of age verification imposed by the Act does justify the burdens imposed on adults—the vast majority of whom value their online privacy and do not wish to expose exploitable personal data simply to view constitutionally-protected material they have every right to view. The high risk of data breaches and leaks resulting from compliance with the Act serves as an unavoidable barrier preventing adults from divulging their information over the internet. If that is set as a condition to view legal adult content, users will simply go elsewhere for that content instead (especially since that content is available elsewhere on the Internet, not just on adult entertainment websites targeted by the Act).

47. Online age-verification is fundamentally different from an employee at a brick-and-mortar store checking a driver's license. Online and offline age verification do not share the same risks. Offline age verification does not carry the threat of producing an accessible ledger of adults that view adult content (or adults whose identity has been stolen and used to view adult content) or of creating a digital trail that could expose an individual to financial or reputational harm. Someone can enter a brick-and-mortar adult bookstore or sex shop merely by briefly displaying their license, for a human worker's real-time review. No record is made or kept, and that is the end of the matter. Online age verification, in contrast, carries the real risk that the viewer's digital

[8] *See e.g.*, Kevin Collier, *U.S. Government Says Several Agencies Hacked As Part Of Broader Cyberattack*, NBC NEWS, (June 15, 2023), https://www.nbcnews.com/tech/security/us-govenment-agencies-hacked-cyberattack-moveit-rcna89525 (discussing a hack of several U.S. agencies, as part of a broader cyberattack that hit dozens of companies and organizations through a previously unknown vulnerability in a popular file sharing software).

"fingerprint" will take on a life of its own, enabling a third party to determine the viewer's identity, expose the viewer as a viewer of adult content, and steal the viewer's identity to commit financial fraud, extortion, and other crimes.[9]

48. This risk is not hypothetical. Louisiana recently passed an age verification law that provides for age verification utilizing a state-maintained database of digital driver's licenses. After going live, that database was breached almost immediately[10], exposing the information of everyone who enrolled in Louisiana's optional digital identification program for the purposes of accessing adult content. It is no coincidence that the number of identity thefts in Louisiana have increased since the age verification law became effective.

49. Data minimization is the principle that reducing the amount of data collected in the first place reduces subsequent risk.[11] This is true, for instance, in the case of a disreputable adult site that might take advantage of the age verification law's requirements to force visitors to provide

---

[9] *See, e.g.*, Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED, (Aug. 18, 2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data (discussing Ashley Madison data breach and hackers' threat to "release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses."). The Ashley Madison breach is associated with at least two suicides. *See* Morgan Sharp, *Two People May Have Committed Suicide After Ashley Madison Hack: Police*, REUTERS, (Aug. 24, 2015), https://www.reuters.com/article/us-ashleymadisoncybersecurity-idUSKCN0QT1O720150824//.

[10] *See* Connor Van Lighten, *Major Cyber Attack Exposes Louisiana Residents' Data – Here's What You Should Do Now*, 4WWL, (June 16, 2023), https://www.wwltv.com/article/news/crime/louisiana-cyber-attack-omv-data-breach-driver-license-id-exposed-information/289-3d263eff-2ace-41b8-98c2-a6ba174935cc.

[11] *See, e.g.*, Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, RSTREET, May 24, 2023, https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/ (discussing how data minimization lessens the potential of data breach); *see also Data Minimization Principle*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/resources/article/data-minimization-principle/.

personal information that can be used for marketing, sold to data brokers, or stolen by attackers. This problem is exacerbated for certain vulnerable adult populations, such as the elderly, who are more susceptible to online hacks and scams.[12] Online age verification does not comport with the principle of data minimization.

50. The Act's nominal data-deletion requirement brings the problem into stark relief. Such requirement is not technologically possible. Furthermore, that requirement binds the regulated website and any third-party verification service, such entities remain free to *transmit* adults' sensitive information to unregulated third parties.

51. That the Act provides a cause of action to victims of hacks or leaks is but a consolation prize to victims, given the time and expense of burdensome litigation. I.C. 24-4-23-8.

B. Risks to Minors

52. The Act's "solution" is far worse than the purported problem it aims to solve. Today's children are "digital natives." They are only more likely than adults to try to circumvent the Act, and thus be pushed to Tor and the Dark Web—and thus be exposed to illegal activities and more extreme material, including violent pornography and criminal gang activities.[13]

---

[12] *See, e.g.*, Emma Fletcher, *Older Adults Hardest Hit By Tech Support Scams*, FEDERAL TRADE COMMISSION CONSUMER PROTECTION, (Mar. 7, 2019), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2019/03/older-adults-hardest-hit-tech-support-scams (finding that "[o]lder adults face unique barriers to adoption, ranging from physical challenges to a lack of comfort and familiarity with technology.").

[13] *See* Kate McCann, *Warning that Age-Checks on Porn Sites Risks Pushing Children to Dark Web*, TELEGRAPH, (Jan. 5, 2018), https://www.telegraph.co.uk/news/2018/01/05/warning-age-checks-porn-sites-risks-pushing-children-dark-web/.

C. The Burden on Websites

53. Commercially available age verification services that are reputable are also exorbitantly expensive. For instance, Trustmatic, the cheapest option in the table below, still costs $40,000 per 100,000 verifications and intrusively requires users to upload pictures of their face.

Vendor	Website (pricing)	$ per verification	100M verifications	5M verifications	100k verifications
Yoti	https://www.yoti.com/business/identity-verification/	£1.20	£120,000,000	£6,000,000	£120,000
Ondato	https://ondato.com/plans-pricing/	€0.95	€95,005,180	€4,750,259	€95,005
Stripe	https://stripe.com/identity#pricing	$1.50	$150,000,000	$7,500,000	$150,000
veriff	https://www.veriff.com/plans	$0.80	$80,000,000	$4,000,000	$80,000
Trustmatic*	https://trustmatic.com/pricing	€0.40	$40,000,000	$2,000,000	$40,000
Faceki	https://apps.faceki.com/pricing	$0.93	$93,000,000	$4,650,000	$93,000

* as of August 2023; it appears that Trustmatic now hides its pricing model.

V. A Less Restrictive Alternative: Blocking and Filtering

54. Improvements in technology have not made online age verification superior to other alternatives, which have also improved and do not share the same vulnerabilities and ease-of-evasion.

55. Content filtering at the browser and/or the device level allows anyone wishing to implement that technology on minors' devices to block access to any unwanted site, including adult sites. These methods are more effective and less restrictive in terms of protecting minors from adult content. While adults have every reason to be concerned about providing their personal information online, parents, who should be the first line of protective defense of their children, have many tools available to them to protect their children from inappropriate adult content.

56. Virtually every available electronic device capable of accessing content online already has built-in parental controls. Internet service providers are also capable of filtering unwanted content and do so every day. And there are additional software and apps freely available on the market allowing for more advanced parental control features, including, for example, from https://www.qustodio.com, https://www.bark.u, https://us.norton.com/products/norton-family,

https://usa.kaspersky.com/safe-kids, https://kidlogger.net/, https://www.mobicip.com/, https://www.eset.com, https://www.webwatcher.com/, and https://www.spyrix.com/.

57. There are websites devoted to evaluating different parent control applications, such as parentalcontrolnow.org.[14] Similarly, buyersguide.org even offers a chart to compare filtering services:

	1. AURA	2. bark	3. gabb	4. kaspersky	5. Qustodio	6. norton
Monitors	Online activity, online gaming, app usage, online chatting (voice and text)	Texts, emails, social media, and app usage	Phone calls, texting, location, and contacts	Digital activity (app, web, and YouTube), screen time, and location	Browsing history, YouTube views, social media use, location	View child's search terms, videos watched, age-appropriate content, location
Devices	iOS and Android devices. Safe Gaming available on Windows PC	Android, iPhone, iPad, Chromebook, Kindle Fire	Gabb Phone, Gabb Phone Plus, Gabb Watch 2	Windows, Mac, iOS, Android	Windows, Mac, iOS, Android, Chromebook, Kindle	Windows PC, Android, or iOS
Time Limits	Yes. Pause the Internet and set time limits for app and website usage	Yes. Set up customizable screen time rules and schedules	Lock mode available on watches during school and focus time	Yes, including daily time limits for specific apps and overall device use time limits	Yes. Set time limits for screen usage and pause internet access	Yes. Set time limits, schedule days and times for usage
Content Limits	Yes. Block inappropriate content from all devices where Aura parental controls are enabled	Yes. Block specific websites and apps on phone, gaming consoles, TV, and more	Yes. Gabb devices have simplified parental controls as they come without internet, social media, gaming, time consuming or dangerous apps	Yes, block harmful content with Safe Search and block specific apps	Yes. Filter websites, apps and games	Yes. Block certain content during schooltime, app supervision, block inappropriate sites
Alerts	Cyberbullying alerts, online usage insights and alerts, online predator alerts, personal information request alerts, and alert parents if a child deleted the app	Cyberbullying, online predators, suicidal ideation, sexting, and more	Safe zone location alerts, SOS emergency call option on watch devices, usage summaries and call/text logs available in the parent account	Low battery alerts for your child's device; web and app use reports	Receive weekly and monthly reports and set alerts for activity you want to know about in real time	Internet usage, search terms, app downloads and installs
Includes	Safe browsing, dark web monitoring and data breach alerts, password manager, antivirus, anti-malware, anti-spyware protection	Website filters, screentime schedules, location alerts, saved photo and video monitoring, child-psychologist advice and tips	Not applicable		Call tracking and SMS for Android and iOS, location alerts, block inappropriate apps, games and websites	Antivirus, VPN, identity protection, password manager, reputation defender

58. The two major personal computer operating systems, Microsoft and Apple, include parental control features by default, straight out of the box, at no additional cost. All major browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple's Safari, also have parental control options. If parents want to add additional parental control features, they may easily purchase supplementary software like Bark or NetNanny or even download additional software for free, including Questodio, Kaspersky Safe Kids, FamilyKeeper, and others. These features enable parents to block access to sexually explicit materials on the Web, prevent minors from giving personal information to strangers by e-mail or in chat rooms, limit a child's screentime, and maintain a log of all online activity on a home computer. Parents can also use

[14] *See, e.g.*, *Best Parental Control Apps for 2023*, PARENTAL CONTROL NOW, https://parentalcontrolnow.org/best-parental-control-appsus/?gclid=EAIaIQobChMIqf6xyuKggAMVxgCtBh3m6g3YEAMYASAAEgJXt_D_BwE.

screening software that blocks messages containing certain words, as well as tracking and monitoring software. A parent also may restrict and observe a child's use of the internet merely by placing a computer in a public space within the home. All of these methods constitute "less restrictive means" for accomplishing the same ends.

59. Filtering technology carries an additional benefit, in that a seventeen-year-old is very different than a twelve-year-old. Parents of an older minor can tailor exceptions for websites that offer, for instance, sexual education materials of clear benefit to an older minor but potentially inappropriate for a younger minor.

60. Filtering technology is available for smartphones and cellular networks as well, such as on the Android operating system.

61. Filtering technology includes not only Domain Name System (DNS) filtering but also artificial intelligence (AI). DNS filtering blocks websites based on how their domain names are categorized. This filtering is dynamic in that once the user blocks a category like adult content, the DNS filtering services constantly scan the Internet and update that category with the latest websites. In fact, uncategorized websites can be blocked as well, given that newly registered websites are the most common source of malware, viruses, and other malicious content. For families, Cisco Systems, one of the largest companies for Internet technologies, provides DNS filtering free of charge via its OpenDNS FamilyShield service. AI is also being incorporated into filtering technology, enabling dynamic, real-time scanning and filtering of website content to block specific images, videos, and text within a webpage that are identified as falling under a blocked category.

VI. A Less Restrictive Alternative: Verifying Age at the Device Level

62. Allowing parents to verify their child's age at the device level is also a viable alternative. Rather than requiring a user to verify with a website, an application can be installed

on children's' devices that allows parents to input their child's age. Requests to visit a website coming from the device can imbed that information and allow the website to reject the request if the child is underage for the website.[15] The privacy advantages of this are palpable, as protecting minors using this system would not rely on collecting even more data that can be used for malicious purposes.

VII. The Act Discriminates Against Adult Content Industry Speakers

63. The Act, by singling out adult content websites for its onerous age verification requirements, while exempting other obvious sources of sexual content online, engages in speaker-based discrimination. The Act ignores search engines explicitly, as well as social media sites, which will not meet the "one-third" threshold of adult content, despite that these sites contain copious amounts of sexually explicit content. Further, search engines and social media sites are where minors most commonly encounter adult content on the Internet.

VIII. Plaintiffs' Additional Injuries

64. The age verification provisions of the Act deprive Plaintiffs and other adult entertainment providers of the goodwill of their Indianan customers, due to the burden age verification imposes and the risks it carries.

IX. The Act's Vagueness

65. Because many of the terms in the Act are vague, the Act further chills the speech of providers of content online and restricts the availability of certain material to those entitled and wishing to receive it. The Act is riddled with vague words, phrases, and requirements, including but not limited to the following:

---

[15] *See* Tonya Riley, *Nationwide Push to Require Social Media Age Verification Rasies Questions About Privacy, Industry Standards*, CYBERSCOOP, (May 8, 2023), https://cyberscoop.com/age-verfication-schatz-cotton-social-media/.

66. The phrase "considered as a whole" in the definition of "material harmful to minors" is vague because what constitutes the "whole" is unclear in the context of the internet generally, or a particular website more specifically. *See* I.C. 24-4-23-3, 35-49-2-2. Should one consider only a specific article, certain text, or an individual image on a website? Or should one consider the web page on which that text or image appears? Or the entire website? And should one include linked material? The Act does not say, and Plaintiffs are left only to guess.

67. The phrases "of minors" and "for minors" in the definition of "material harmful to minors" are also vague because the Act defines a minor as anyone under the age of eighteen. *See* I.C. 24-4-23-4. But sexual material harmful to an 8-year-old may not be harmful to a 17-year-old. The definition of "material harmful to minors" provides no way to make this distinction, rendering the definition inherently confusing and potentially self-contradictory.

68. The statutory catch-all permitting "[a]ny commercially reasonable method that relies on public or private transactional data" as a means of verifying a user's age provides no guideposts whatsoever, as "commercially reasonable" is a vague term not defined by the Act.

69. The Act does not even explain how often age verification must occur. Individuals can access a website more than once, and from different devices and browsers. Must age verification recur every hour; every time a web browser is closed and reopened; just once, if the website operator can find a way to link a particular verification to a particular device; or something else?

X. The Need for Injunctive Relief

70. The passage of the Act has placed Plaintiffs in reasonable fear that, if they continue their current course of conduct as they intend, they will be sued under the Act. Indeed, the Act squarely targets Plaintiffs, the core entities whose behavior the Act aims to change. Enforcement

against other entities would constitute enforcement merely on the fringes of the adult industry, which the Act targets.

71. The Act impinges on the constitutional right to access protected speech and expressive conduct, in violation of the First Amendment.

72. The Act authorizes a lawsuit in violation of section 230, which provides Plaintiffs with an immunity to court proceedings that will be irretrievably lost if the Attorney General is permitted to enforce the Act.

73. The Act will destroy Plaintiffs' goodwill in Indiana by forcing Plaintiffs to either withdraw from Indiana or comply with the Act and nevertheless lose a vast number of new and longstanding adult visitors to their websites. The age verification provisions of the Act deprive Plaintiffs and other adult entertainment providers of the goodwill of their Indianan customers, due to the burden age verification imposes and the risk it carries.

74. Plaintiffs thus have no adequate remedy at law.

COUNT I

(42 U.S.C. § 1983 (All Plaintiffs))

(The First Amendment)

75. Plaintiffs repeat and re-allege each of the foregoing paragraphs as if set forth entirely herein.

76. The Act is facially overbroad in violation of the First Amendment (made applicable to the states through the Fourteenth Amendment) because its age verification requirement is substantially overbroad, is not narrowly tailored, and does not pursue a compelling state interest. It is substantially overbroad because it imposes a barrier to the rights of adults to access speech that is constitutionally protected for them. It not narrowly tailored, because there are at least two

superior, less restrictive alternatives: pre-blocking by internet service providers and the use of filtering technology by parents or others at the device level. It does not pursue a compelling state interest, because it is dramatically underinclusive, exempting internet search engines, most social media sites, news media and written sexually explicit material, and is targeted against adult entertainment websites.

77. The Act is further overbroad because it does not satisfy the First Amendment's heightened standards for clarity. It is incurably vague regarding to whom it applies and what it requires, thus chilling protected speech as website operators seek to avoid liability by steering clear of the law by a wider margin than would otherwise be required.

78. Plaintiffs are thus entitled to injunctive relief to preclude the Indiana Attorney General from depriving Plaintiffs of their rights guaranteed by the Constitution.

COUNT II

(42 U.S.C. § 1983 (All Plaintiffs))

(The Fourteenth Amendment)

79. Plaintiffs repeat and re-allege each of the foregoing paragraphs as if set forth entirely herein.

80. The Act violates the rights of Plaintiffs under the Due Process Clause of the Fourteenth Amendment (procedural component) because it is impermissibly vague and fails to provide a person of ordinary intelligence fair notice of what is prohibited.

81. The Act violates the rights of Plaintiffs under the Due Process Clause of the Fourteenth Amendment (substantive component) because it deprives Plaintiffs of a protected property right, in the form of their goodwill in Indiana, without a rational basis.

82. The Act violates the Equal Protection Clause of the Fourteenth Amendment because, with no rational basis for doing so, it exempts, for example, internet search engines and most social media sites while targeting adult entertainment platforms.

83. Plaintiffs are thus entitled to injunctive relief to preclude the Indiana Attorney General from depriving Plaintiffs of their rights guaranteed by the Constitution.

COUNT III

(42 U.S.C. § 1983 (All Plaintiffs))

(The Eighth Amendment)

84. Plaintiffs repeat and re-allege each of the foregoing paragraphs as if set forth entirely herein.

85. Plaintiffs have a right against Excessive Fines under the Eighth Amendment.

86. The Act authorizes civil penalties of $250,000 per violation.

87. These penalties are grossly disproportionate to any putative harm addressed by the Act.

88. Plaintiffs are thus entitled to injunctive relief to preclude the Indiana Attorney General from depriving Plaintiffs of their rights guaranteed by the Constitution.

COUNT IV

(42 U.S.C. § 1983 (All Plaintiffs))

(The Fifth Amendment)

89. Plaintiffs repeat and re-allege each of the foregoing paragraphs as if set forth entirely herein.

90. Plaintiffs have a right against unconstitutional takings of "private property" for "public use, without just compensation" under the Fifth Amendment.

91. Under *Penn Central Transportation Co. v. City of New York*, 438 U.S. 104, 124 (1978), a regulatory taking violates the Fifth Amendment where: (a) "[t]he economic impact of the regulation"; (b) "the extent to which the regulation has interfered with reasonable investment-backed expectations"; and (c) "the character of the governmental action." The Act inflicts a regulatory taking under each factor.

92. The Act imposes a regulatory taking at least by forcing Plaintiffs to implement age verification at exorbitant costs that some cannot afford, either by building infrastructure within their own websites or contracting with a third-party provider.

93. Plaintiffs have a substantial property interest in and associated with their websites and businesses, and, if the Act becomes effective, the Act will deprive Plaintiffs of that property protected by the Takings Clause.

94. The Act does not compensate Plaintiffs, let alone justly, for the destruction of their businesses.

95. Plaintiffs are thus entitled to appropriate monetary relief lest the Indiana Attorney General deprive Plaintiffs of their rights guaranteed by the Constitution.

COUNT V

(42 U.S.C. § 1983 & 47 U.S.C. § 230 (Plaintiffs FSC, Aylo Premium as to SpiceVids, Aylo Freesites as to Pornhub, WebGroup, NKL, and MediaME))

96. Plaintiffs repeat and re-allege each of the foregoing paragraphs as if set forth entirely herein.

97. Under the Supremacy Clause of the United States Constitution, the laws of the United States are "the supreme law of the land."

98. Federal law confers a personal right of immunity against proceedings where the theory of liability equates websites with third-party publishers. 47 U.S.C. § 230(c)(1) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(e)(3) states: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."

99. Plaintiffs WebGroup, NKL, FSC, Aylo Premium, Aylo Freesites, and MediaME, as website platforms, are providers of an "interactive computer service" under section 230.

100. As applied to these Plaintiffs, the Act is preempted through the Supremacy Clause as a violation of section 230, because it imposes liability on website operators for putative harm caused by the content of third-party publishers.

101. Plaintiffs are thus entitled to injunctive relief to preclude the Indiana Attorney General from depriving Plaintiffs of their rights guaranteed by the Constitution and federal law.

COUNT VI

(42 U.S.C. § 1983 & 28 U.S.C. §§ 2201-02 (All Plaintiffs))

(Declaratory Judgment)

102. Plaintiffs repeat and re-allege each of the foregoing paragraphs as if set forth entirely herein.

103. There is a present and justiciable dispute as to whether enforcement of the Act by Defendant violates the Plaintiffs' rights under the U.S. Constitution and federal law, as stated in Counts I-V.

104. The interests of Plaintiffs, on the one hand, and Defendant, on the other, are real and adverse.

105. Absent court intervention, which would resolve the dispute over the Act's lawfulness, Defendant will proceed to enforce the Act even though the Act is unconstitutional and void.

106. Plaintiffs are accordingly entitled to a declaration of rights in the form of a declaratory judgment that the Act is unconstitutional and unenforceable and, to the extent it is enforceable, a violation of the Takings Clause entitling Plaintiffs to just compensation.

107. Plaintiffs are entitled to all further necessary and proper decrees of relief based on the foregoing declaration of rights.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that the Court order the following relief and remedies:

1. Preliminarily and permanently enjoin Defendant, his officers, agents, servants, employees, and attorneys, and those persons in active concert or participation with those who receive actual notice of the injunction, from enforcing the Act;
2. Declare the Act unconstitutional and unenforceable, as a violation of the First Amendment, Fourteenth Amendment, Eighth Amendment, and Supremacy Clause of the U.S. Constitution;
3. Declare the Act a violation of the Takings Clause of the Fifth Amendment entitling Plaintiffs to just compensation;
4. Award Plaintiffs damages and their reasonable costs and fees pursuant to 42 U.S.C. § 1988; and
5. Grant Plaintiffs such other and further relief as the Court deems just and proper.

Dated: June 10, 2024 By /s/ *Kian Hudson*

Derek L. Shaffer (*pro hac vice forthcoming*)
derekshaffer@quinnemanuel.com
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Telephone: (202) 538-8000
Fax: (202) 538-8100

Kian Hudson (Bar No. 32829-02)
Kian.hudson@btlaw.com
BARNES & THORNBURG LLP
11 S Meridian St
Indianapolis, Indiana 46204
Telephone: (317) 236-1313
Fax: (317) 231-7433

Taylor E. Comerford (*pro hac vice forthcoming*)
taylorcomerford@quinnemanuel.com
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
111 Huntington Ave Suite 520
Boston, MA 02199
Telephone: (617) 712-7100
Fax: (617) 712-7200

Michael T. Zeller (*pro hac vice forthcoming*)
Arian Koochesfahani (*pro hac vice forthcoming*)
michaelzeller@quinnemanuel.com
ariankoochesfahani@quinnemanuel.com
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
865 South Figueroa Street, 10th Floor
Los Angeles, CA 90017-2543
Telephone: (213) 443-3000
Fax: (213) 443-3100