



AMERICAN
PRINCIPLES PROJECT

How States Can Protect Kids from Online Pornography

A Policy Brief on Age Verification Legislation

November 1, 2023

Authors

Jon Schweppe
Policy Director
American Principles Project
jon@americanprinciplesproject.org

Craig Parshall
Senior Advisor, Civil Liberty and Legal Policy
American Principles Project

Table of Contents

● Background	3
● A Brief Note on Obscenity	4
● Age Verification vs. Other Methods	4
● The Current Age Verification Laws Aren't Effective Enough	6
● Possible Improvements to Age Verification Laws	7
○ Stronger Enforcement Mechanisms	7
○ Limiting the "Substantial Portion" Carve-out	9
○ Limiting the "News-gathering" Organization Carve-out	10
○ Eliminating the Search Engine Carve-out	11
○ Comporting Language with Section 230	12
● Utah's Age Verification Law (Full Text)	14
● APP's Model Age Verification Law	17
● Addendum 1 - Age Brackets to Determine Harm to Minors	23
● Addendum 2 - Specified Age Verification Methods	24

Background

In 1996, the Supreme Court struck down the Communications Decency Act (CDA), a federal anti-pornography bill passed by Congress that sought to limit the online distribution of obscene and indecent material to minors. It is often suggested that this case “found” a First Amendment right to pornography, thus limiting the ability for the people and their legislatures to restrict its distribution, but that is not entirely accurate.

In *Reno v. ACLU*, and again later in 2004 in *Ashcroft v. ACLU*, which struck down the Child’s Online Protection Act (COPA), the Supreme Court made two distinct arguments: first, that there is indeed a compelling governmental interest in protecting children from pornography, and second, that any law restricting pornography distribution to minors must be narrowly tailored and use the least restrictive means possible to prevent a broad suppression of adult “speech.” From *Reno*:

“We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve... It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials... But that interest does not justify an unnecessarily broad suppression of speech addressed to adults.”

This is important. While the CDA (and ultimately COPA) were deemed too restrictive on adult “speech,” the Court did not rule out the ability to enact restrictions on the distribution of pornography to minors, so long as these restrictions did not amount to an undue burden on the ability of adults to access pornography.

We can quibble with the merits of the *Reno* and *Ashcroft* decisions. At American Principles Project, we believe that these cases were wrongly decided and that pornography, especially when it is readily available to minors, amounts to illegal obscenity (and thus not protected speech.) But even under the flawed precedent set by *Reno*, we are confident that the current Supreme Court could well uphold the age verification legislation laws that have now passed in eight states (as of November 2023.) Even so, we believe there is more we can do to

strengthen these laws without running afoul of this particular interpretation of the First Amendment.

A Brief Note on Obscenity

Before we get into age verification, it's important to note that going after obscenity specifically may ultimately prove to be the best legal route to protect kids from online pornography. Earlier this year, we worked with a Texas legislator on [legislation](#) (HB 3357) that imposed civil liability whenever an individual or corporation violates a Texas obscenity statute about distributing harmful material to minors. These obscenity statutes have largely gone unenforced in recent years, so this law sought to create a new enforcement mechanism via a private cause of action. Obscenity is not protected speech – and so when legislating against obscenity specifically, we are able to avoid many of the pitfalls outlined in *Reno* and *Ashcroft*. We don't have to worry about “least restrictive means” or posing any sort of undue burden on adults because there is no constitutional right to distribute or obtain obscene material.

As it stands, there is a growing consensus around the idea of age verification. These laws do not typically invoke obscenity statutes, but we still think this is a good strategy and a worthwhile first step given how long it has been since there has been a serious political movement to limit the distribution of pornography. We encourage states to follow the blueprint that has worked and enact these kinds of bills into law, but it may make sense to pursue obscenity enforcement as a simultaneous strategy – and certainly in the future if the Courts prevent the age verification laws from taking effect.

Age Verification vs. Other Methods

Over the past several years, we have seen a surge of interest in protecting kids from online pornography, culminating with significant legislative successes in the states:

- In 2021, Utah passed a “device filters” bill that would require any tablet or smartphone sold or activated within the state to include a content filter (with a default of the filter being “on”) that would block pornography on that particular device. A provision in the bill mandates that five other states must pass similar legislation before the device filters requirement can take effect.

- In 2022 and 2023, a total of eight states, Louisiana, Utah, Virginia, Mississippi, Arkansas, Montana, Texas, and North Carolina, have passed age verification bills that would require pornography websites to verify the adult age of their users prior to distributing them sexually explicit content.

American Principles Project has taken the position of endorsing any and all legislation that advances the cause of protecting kids from online pornography. That includes the device filters legislation that has passed in Utah and has been introduced in a number of other states.

But there are some important advantages to the age verification approach. First and foremost, these bills are an easier political lift. The online pornography industry has few advocates willing to defend its interests. Meanwhile, Big Tech companies, streaming services, internet service providers, and device manufacturers have particularly powerful lobbies, and they have already demonstrated the ability in some states to stop device filters legislation from passing into law.

Second, age verification laws place a burden directly on those who actively distribute online pornography, rather than on those who facilitate distribution merely by providing access to the Internet. While our organization agrees that anyone involved in facilitating the distribution of pornography to minors should have a duty of care to prevent that from happening, it certainly makes sense from a political order of operations standpoint to go after the source of that pornography first.

Third, the laws have done well so far under the inevitable legal scrutiny they will face. Earlier this year, a U.S. District Court judge threw out a legal challenge to Utah's age verification law. Another U.S. District Court judge did the same thing for Louisiana's law. And while a federal judge in Texas did issue an injunction to stop implementation of Texas' age verification law, the 5th Circuit Court of Appeals stayed the injunction while expediting the appeals process, allowing the bill to temporarily go into effect.

And finally, we know that these age verification laws are starting to change the behavior of pornography websites – at least in part. Pornhub, one of the most trafficked pornography websites in the United States, has implemented Louisiana's state ID requirement, but has pulled out of Virginia, Arkansas, Mississippi, and Utah altogether rather than comply with the law in those states.

Other porn websites have reportedly implemented some forms of age verification in Virginia. But that's not to say the laws are perfect in their current form.

The Current Age Verification Laws Aren't Effective Enough

While a few US-based pornography websites have complied with state age verification laws by either requiring a form of age verification or blocking traffic entirely from the state, the reality is that online pornography is still widely available to children in each of the eight states that have passed these laws. According to the [Virginia Mercury](#):

“To get an understanding of how many websites are complying with the law, the Mercury attempted to access the 65 “top porn tube sites” listed on [toppornsites.com](#). As of Aug 15, only one website, xHamster, is using age verification methods mandated by the law. Ten websites are blocked altogether, and 54 remain entirely unrestricted.”

As of November 2023, children in these eight states are still able to access online pornography in the following ways:

- By visiting any non-US-based pornography website outside the jurisdiction of individual states
- By visiting a US-based pornography website that is not complying with the law
- By searching on a search engine like Google
- By searching on a social media website like X (Twitter) or TikTok
- By [disconnecting WiFi](#) and using a mobile phone's 4G or 5G Internet
- By using VPN software to mask a WiFi-connected device's location

Some of these problems can't be solved by legislation at the state level. Jurisdiction matters, and it will be difficult for a state attorney general to rein in a pornography website based out of Romania. Ultimately, this makes the case for federal legislation. If granted authority by Congress, or potentially even under existing obscenity law, the Department of Justice could seize domain names, block traffic, and/or explore other ways to prevent foreign pornography websites from distributing to American kids. But while we wait on federal action, which is unlikely to happen in the next year, there is still much work that can be done at the state level.

At American Principles Project, we are big believers that the perfect should not be the enemy of the good. Incrementalism works. While we believe the recommendations listed below will improve the policy, strengthen enforcement, and protect more kids from harm, we also recognize that the fight to protect kids from online pornography is a growing movement and passing an incremental first step is more important than introducing a bill entirely to our liking that fails to pass out of committee. Bills that become law can always be amended, or added on to, in future legislative sessions. Therefore, we urge legislators to consider all of these recommendations on a case by case basis.

Possible Improvements to Age Verification Laws

Most age verification bills look very similar. For the purpose of this document, we are working off of [S.B. 287](#), the Utah legislation that passed earlier this year. We've included a copy of Utah's bill toward the end of this policy brief.

Stronger Enforcement Mechanisms

Pornography websites have already been operating in a legal gray area due to the dozens of obscenity statutes on the books at both the federal level and the state level. That has not stopped them from operating. Enforcement is key. In order to effectively protect kids from online pornography, it will be critical for states to include strong enforcement mechanisms in their bills with severe penalties for failing to comply.

Louisiana was the first state to pass age verification, and its legislature quickly realized the first law was not adequate in terms of enforcement. To fix the problem, the legislature passed a second [law](#) that empowered the state attorney general and included specific civil penalties for pornography websites that fail to comply. We encourage other states to adopt similar language in their bills:

A.(1) Any commercial entity that knowingly and intentionally publishes or distributes material harmful to minors on the internet from a website that contains a substantial portion of such material shall be subject to civil penalties as provided in this Section if the entity fails to perform reasonable age verification methods to verify the age of individuals attempting to access the material.

(2) The attorney general may conduct an investigation of the alleged violation and initiate a civil action in the Nineteenth Judicial District Court

for the parish of East Baton Rouge on behalf of the state to assess civil penalties. Prior to asserting a cause of action, the attorney general shall provide the commercial entity with a period of time of not less than thirty days to comply with this Section.

B.(1) Any commercial entity that violates this Section may be liable for a civil penalty, to be assessed by the court, of not more than five thousand dollars for each day of violation to be paid to the Department of Justice, in order to fund the investigation of cyber crimes involving the exploitation of children. In addition to the remedies provided in this Section, the attorney general may request and the court may impose an additional civil penalty not to exceed ten thousand dollars for each violation of this Section against any commercial entity found by the court to have knowingly failed to perform reasonable age verification methods to verify the age of individuals attempting to access the material. The civil penalty shall be paid to the Department of Justice in order to fund the investigation of cyber crimes involving the exploitation of children.

(2) Each violation may be treated as a separate violation or may be combined into one violation at the option of the attorney general.

(3) Any commercial entity that violates this Section may be liable to the attorney general for all costs, expenses, and fees related to investigations and proceedings associated with the violation, including attorney fees.

(4) If the court assesses a civil penalty pursuant to this Section, the Department of Justice shall be entitled to legal interest as provided in R.S. 9:3500 from the date of imposition of the penalty until paid in full.

While all of the age verification laws include civil liability, and some include a cause of action for the state attorney general, North Carolina's [law](#) adds a private cause of action with the following language:

(d) Cause of Action. – A civil action may be brought against any commercial entity, or third party that performs the required age verification on behalf of the commercial entity, that violates this section by any of the following: (1) A parent or guardian whose minor was allowed access to the material. (2) Any person whose identifying information is retained in violation of this section. (e) Relief and damages – Any person authorized to institute a civil action by subsection (d) of this section may seek and a court may award any or all of the following types

of relief: (1) An injunction to enjoin continued violation of this section. (2) Compensatory and punitive damages. (3) All costs, expenses, and fees related to the civil suit investigation and proceedings associated with the violation, including attorney's fees. Any judgment awarded under this section shall be subject to legal interest as provided in G.S. 24-5.

We believe including both the attorney general enforcement mechanism, extensive civil liability with specific civil penalties, and a private cause of action will all be necessary to force US-based online pornography websites to fully cooperate with the laws. We include the above provisions (and other line edits) in our model legislation at the end of the policy brief.

Limiting the “Substantial Portion” Carve-out

So far, each of the laws passed have included a “substantial portion” carveout that limits the laws’ effectiveness. The provision in question requires that websites only face liability if they include more than 33-1/3% of total “material harmful to minors.” Below is Utah’s carveout:

(10) "Substantial portion" means more than 33-1/3% of total material on a website, which meets the definition of "material harmful to minors" as defined in this section.

...

*1) A commercial entity that knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a **substantial portion** of such material shall be held liable if the entity fails to perform reasonable age verification methods to verify the age of an individual attempting to access the material.*

This provision was politically helpful to avoid pushback from certain special interest groups and companies. But unfortunately, it is likely to leave numerous websites that are actively distributing pornography to children unaffected – and therefore unlikely to change their behavior. It also invites the possibility of a pornography website flaunting the law by claiming more than 66-2/3% of material on its website fails to meet the definition of “material harmful to minors.” The vagueness of this carveout could turn into a defense attorney’s dream. How is this amount to be measured? Total pornographic videos? Words

on a webpage? Lines of code?

We would prefer to eliminate this carve-out altogether. We believe it makes the law underinclusive and therefore troublesome constitutionally (see the [Texas ruling](#).) Additionally, this carve-out seems to give some websites a lifeline when they clearly do not deserve one. Should PornHub be allowed to distribute pornography to minors? Everyone seems to agree that the answer is no. But should X (Twitter), Instagram, and TikTok be allowed to do the same thing with impunity?

That being said, we understand the carveout is likely to remain in the legislation, so we propose a simple fix in our model legislation that also includes language as part of a strengthened enforcement mechanism:

(1) A commercial entity that knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website or individual webpage that, in whole or in part, contains a substantial portion of such material shall be held liable in a civil action for damages to any person harmed by that conduct if the entity fails to perform reasonable age verification methods to verify the age of an individual attempting to access the material.

We would also propose changing the definition of “substantial portion” to reflect this amendment:

(10) "Substantial portion" means more than 33-1/3% of total material on a website or individual webpage, which meets the definition of "material harmful to minors" as defined in this section.

In the model legislation included at the end of this document, we chose to nuance the 33-1/3% benchmark. We have expressly detailed how that metric should apply, depending on whether the distributor of the content is a social media site, a search engine, or a website. See section 10 (a) - (c) of the proposed statute.

Limiting the “News-gathering Organization” Carve-out

A pornography website could seek immunity by identifying itself publicly as a “news-gathering organization.” Each of the laws contain similar news

carve-outs that read as follows:

(5) This section shall not apply to any bona fide news or public interest broadcast, website video, report, or event and shall not be construed to affect the rights of a news-gathering organization.

If PornHub simply adds a news component to its website, it would appear to be immune from any liability. To prevent this, we propose adding an additional section:

(5a) An Interactive Computer Service is not deemed to be a news-gathering organization unless its primary business is as an Information Content Provider, news publisher, or broadcaster, of current news and public interest.

Eliminating the Search Engine Carve-out

As these bills are currently written, search engines enjoy immunity from any liability under the law. That means that a child could simply access Google, turn “safe search” off with the click of a button, and access pornographic images without leaving Google’s website. In addition to limiting the ability to achieve the law’s aims, this carve-out makes the law underinclusive and therefore possibly unconstitutional.

As Judge David Alan Ezra stated in his order granting a preliminary injunction against Texas’ age verification law:

“H.B. 1181 will regulate adult video companies that post sexual material to their website. But it will do little else to prevent children from accessing pornography. Search engines, for example, do not need to implement age verification, even when they are aware that someone is using their services to view pornography... Defendant argues that the Act still protects children because they will be directed to links that require age verification... This argument ignores visual search, much of which is sexually explicit or pornographic, and can be extracted from Plaintiffs’ websites regardless of age verification... Defendant’s own expert suggests that exposure to online pornography often begins with “misspelled searches[.]”

Search engines have already demonstrated the technological capability to block pornographic images from the vast majority of user queries. Google has implemented a “safe search” system with a default of “on” when it has not verified a user to be 18 years or older. DuckDuckGo, a Google competitor, has implemented similar technology. But users of all ages ultimately have the option to turn this setting off – and if they do, both search engines readily display pornographic material on their own websites.

Eliminating the search engine carve-out would require these search engines to add an age verification system that is needed only in the instances the search engines are displaying pornographic images on their own websites. In other words, Google and DuckDuckGo would not need to verify a user’s age to allow them to conduct a search, but they would be required to verify a user’s age in order to distribute pornographic images to them.

Comporting Language with Section 230

American Principles Project has long advocated for Congress to make structural changes to Section 230, a law passed back in 1996 as part of the Communications Decency Act. We detailed some of our proposed reforms in a [blueprint](#) we published back in 2020. There are also a number of legal cases making their way through the courts that may eventually challenge the constitutionality of the statute.

But our approach to state legislation has been to play under the current rules – assuming that existing Section 230 precedent will hold – and that certainly dictates what we can and can’t do at the state level.

We have addressed Section 230 in our proposal in two different ways. First, in a direct way, we have sought to embed those legally defensible ways in which the statute’s immunity from civil liability for interactive computer services can be avoided while still being consistent with Section 230’s own language.

Obviously, a long line of legal cases have unnecessarily broadened the breadth of the civil immunity that is granted to online platforms under Section 230. But that doesn’t mean that there are no exceptions to that immunity. Our legislative proposal seeks to fit the liability of tech platforms for harmful content into categories that courts have already recognized. For instance, tech platforms can be liable for the content they disseminate over the internet if they are, at least as to the content in question, not just a distribution service, but a content

creator.

In the ordinary course, social media platforms profess to make content moderation decisions supposedly guided by their terms of service. They also deny joining their users in co-creating content with them. As a result, Section 230, under the current judicial approach, permits the platforms generous *carte blanche* to decide which content will be allowed, and which will be blocked, demonetized, restricted, or otherwise treated adversely as compared to other user content, all without incurring legal liability.

This changes, though, when a platform has become a *content creator* of certain online user information at issue, and not just a distributor or a gatekeeper for third-party user material. Section 230 defines an information content creator as an entity, platform or service “that is responsible, in whole or in part, for the creation or development of information provided through the internet.” Case law has developed in several federal circuits, defining what it means for a platform to be “responsible” for the “creation or development” of online information on the internet, thus rendering the platform civilly liable for that activity regarding specific problematic content.

Our proposal has adopted some of the language from decisions of those U.S. Courts of Appeal that have found a particular website to have been civilly liable as an “information content provider.”

The second way we have addressed Section 230, this time somewhat indirectly, is by expressly excluding almost all tech platforms from escaping liability under the Utah exception for a “news-gathering organization.” Only an online service whose *primary business* is in the news gathering business will qualify for the exception. Otherwise, the typical online platform will be responsible for civil liability caused by their conduct regarding content that is harmful to minors, assuming of course, that it has also been a “content creator” in partnering in the “creation or development” of the offensive material that caused the harm.

Utah's Age Verification Law (Full Text)

[SB0287](#)

Signed Into Law on March 14, 2023

Be it enacted by the Legislature of the state of Utah:

Section 1. Section 78B-3-1001 is enacted to read:

Part 10. Liability for Publishers and Distributors of Material Harmful to Minors

78B-3-1001. Definitions.

As used in this chapter:

(1) "Commercial entity" includes corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities.

(2) "Digitized identification card" means a data file available on any mobile device which has connectivity to the Internet through a state-approved application that allows the mobile device to download the data file from a state agency or an authorized agent of a state agency that contains all of the data elements visible on the face and back of a license or identification card and displays the current status of the license or identification card.

(3) "Distribute" means to issue, sell, give, provide, deliver, transfer, transmute, circulate, or disseminate by any means.

(4) "Internet" means the international computer network of both federal and non-federal interoperable packet switched data networks.

(5) "Material harmful to minors" is defined as all of the following:

(a) any material that 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 is designed to pander to, the prurient interest;

(b) material that exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated display or depiction of any of the following, in a manner patently offensive with respect to minors:

(i) pubic hair, anus, vulva, genitals, or 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) the material taken as a whole lacks serious literary, artistic, political, or scientific value for minors.

(6) "Minor" means any person under 18 years old.

(7) "News-gathering organization" means any of the following:

(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, while operating as an employee as provided in this subsection, who can provide documentation of such employment with the newspaper, news publication, or news source; or

(b) an employee of a radio broadcast station, television broadcast station, cable television operator, or wire service while operating as an employee as provided in this subsection, who can provide documentation of such employment.

(8) "Publish" means to communicate or make information available to another person or entity on a publicly available Internet website.

(9) "Reasonable age verification methods" means verifying that the person seeking to access the material is 18 years old or older by using any of the following methods:

(a) use of a digitized information card as defined in this section;

(b) verification through an independent, third-party age verification service that compares the personal information entered by the individual who is seeking access to the material that is available from a commercially available database, or aggregate of databases, that is regularly used by government agencies and businesses for the purpose of age and identity verification; or

(c) any commercially reasonable method that relies on public or private transactional data to verify the age of the person attempting to access the material.

(10) "Substantial portion" means more than 33-1/3% of total material on a website, which meets the definition of "material harmful to minors" as defined in this section.

(11) (a) "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.

(b) "Transactional data" includes records from mortgage, education, and employment entities.

Section 2. Section 78B-3-1002 is enacted to read:

78B-3-1002. Liability for publishers and distributors – Age verification – Retention of data – Exceptions.

(1) A commercial entity that knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a substantial portion of such material shall be held liable if the entity fails to perform reasonable age verification methods to verify the age of an individual attempting to access the material.

(2) A commercial entity or third party that performs the required age verification shall not retain any identifying information of the individual after access has been granted to the material.

(3) A commercial entity that is found to have violated this section shall be liable to

an individual for damages resulting from a minor's accessing the material, including court costs and reasonable attorney fees as ordered by the court.

(4) A commercial entity that is found to have knowingly retained identifying information of the individual after access has been granted to the individual shall be liable to the individual for damages resulting from retaining the identifying information, including court costs and reasonable attorney fees as ordered by the court.

(5) This section shall not apply to any bona fide news or public interest broadcast, website video, report, or event and shall not be construed to affect the rights of a news-gathering organization.

(6) No Internet service provider, affiliate or subsidiary of an Internet service provider, search engine, or cloud service provider shall be held to have violated the provisions of this section solely for providing access or connection to or from a website or other information or content on the Internet, or a facility, system, or network not under that provider's control, including transmission, downloading, storing, or providing access, to the extent that such provider is not responsible for the creation of the content of the communication that constitutes material harmful to minors.

APP Draft Model Age Verification Law

Based on Utah SB0287 Template

(Changes in Yellow)

Last Updated: November 1, 2023

LIABILITY FOR PUBLISHERS AND DISTRIBUTORS OF MATERIAL HARMFUL TO MINORS

Definitions

As used in this chapter:

- (1) "Commercial entity" includes corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities.
- (2) "Digitized identification card" means a data file available on any mobile device which has connectivity to the Internet through a state-approved application that allows the mobile device to download the data file from a state agency or an authorized agent of a state agency that contains all of the data elements visible on the face and back of a license or identification card and displays the current status of the license or identification card.
- (3) "Distribute" means to issue, sell, give, provide, deliver, transfer, transmute, circulate, or disseminate by any means.
- (4) "Internet" means the international computer network of both federal and non-federal interoperable packet switched data networks.
- (4a) Interactive Computer Service means any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions.¹
- (4b) Information Content Provider means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the

¹ This is identical to 47 U.S.C. sec. 230 (f) (2) (i.e. section 230 of the Communications Decency Act).

internet or any interactive computer service.² This includes³ any material contribution⁴ or participation in⁵ any illegal aspect of content provided by an Information Content Provider, such as requesting or recommending certain illegal content or suggesting that the Provider change or edit illegal content in any manner other than total deletion or removal, or any similar action that otherwise knowingly facilitates⁶ or furthers the Provider's publishing or distribution of content prohibited under this Act.

(5) "Material harmful to minors" is defined as all of the following: (a) any material that 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 is

² This is identical to 47 U.S.C. sec. 230 (f) (3).

³ This language is an accumulated test from three Circuit Courts of Appeal; e.g. see the 10th Circuit in *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1199–1200 (10th Cir. 2009). That court stated that to be responsible for offensive content, "one must be *more than a neutral conduit* ... We therefore conclude that a service provider is "responsible" for the development of offensive content only if it in some way *specifically encourages development of what is offensive about the content*" ... "the Ninth Circuit, sitting en banc, has held that the provider of an online roommate-matching service was responsible for the development of discriminatory preferences contained in its users' personal-profile pages. *Roommates.com*, 521 F.3d at 1167-68. Subscribers of the website were required to specify from a set of preselected answer choices their "sex, sexual orientation and whether [they] would bring children to a household." *Id.* at 1161 and 1165 & n. 17. Subscribers also had to select their "preferences in roommates with respect to the same three criteria." *Id.* at 1161" (emphasis added).

In *Accusearch Inc.*, 570 F.3d at 1199–1200 the precise facts before the 10th Circuit involved a website that had "developed" the offending information by "*solicit[ing] requests*" for the wrongful information and by "*pa[ying] researchers to obtain it*" (emphasis added). Under both *Accusearch* and *Roommates*, to "develop" online content includes conduct that will "enhance" what is offensive [or in our statute, to enhance the reach or the harmful aspects of the content that is harmful to minors].

See also: *Huon v. Denton*, 841 F.3d 733, 741 (7th Cir. 2016): "A company can, however, be liable for creating and posting, *inducing another* to post, or *otherwise actively participating in the posting of* a defamatory statement in a forum that that company maintains. See *Chi. Lawyers' Comm.*, 519 F.3d at 671 ; see also *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1166–67 (9th Cir. 2008) (en banc) (concluding that a website was *not a "passive transmitter of information provided by others" but instead helped develop the information by "requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers"*) (emphasis added).

⁴ See: *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269, n. 4 (9th Cir. 2016) (noting that most circuits have adopted the *Roommates.com* test that makes civilly actionable, any "material contribution" to the aspect of the content that makes it illegal; i.e. the website or other platform. has become, as to that illegal content, something beyond the traditional conduct of a publisher who simply editorially screens welcome versus unwelcome content).

⁵ *G.G. v. Salesforce* (7th Cir. 2023) (230 immunity at motion to dismiss stage denied in a civil suit for online sex trafficking a minor under 18 U.S.C. 1595. Liability of Salesforce was based on "participation in a venture" in which it benefited from sex trafficking through its soft wear provided to Backpage that helped make it successful. The court applying a "knew or should have known" scienter test to Salesforce).

⁶ The *Salesforce* court in rejecting the defendant's 230 argument, applied section 1595's prohibition of "knowingly ... *facilitating*" a venture engaged in sex trafficking. We have adapted that phrase to harmful-to-minors content.

designed to pander to, the prurient interest; (b) material that exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated display or depiction of any of the following, in a manner patently offensive with respect to minors: (i) pubic hair, anus, vulva, genitals, or 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) the material taken as a whole lacks serious literary, artistic, political, or scientific value for minors.

(6) "Minor" means any person under 18 years old.⁷

(7) "News-gathering organization" means any of the following: (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, while operating as an employee as provided in this subsection, who can provide documentation of such employment with the newspaper, news publication, or news source; or (b) an employee of a radio broadcast station, television broadcast station, cable television operator, or wire service while operating as an employee as provided in this subsection, who can provide documentation of such employment.

(7a) A website or an interactive computer service is not deemed to be a news-gathering organization unless its primary business is as an information content provider, news publisher, or broadcaster, of current news and public interest.

(8) "Publish" means to communicate or make information available to another person or entity on a publicly available Internet website.

(9) "Reasonable age verification methods" means verifying that the person seeking to access the material is 18 years old or older by using any of the following methods, as long as not violative of any other provisions of this act:

(a) use of a digitized information card as defined in this section;

(b) verification through an independent, third-party age verification service that compares the personal information entered by the individual who is seeking access to the material that is available from a commercially available database, or aggregate of databases, that is regularly used by government agencies and businesses for the purpose of age and identity verification; or

(c) any available, reasonable method that relies on public or private transactional data to verify the age of the person attempting to access the material.⁸

⁷ See Addendum 1 for a method of using age brackets for the harmfulness determination in order to avoid one of the reasons why the Texas court placed an injunction on HB1181 (the Texas age verification law.)

⁸ See Addendum 2 for additional language that helps to specify the types of age verification methods that would qualify as reasonable. This was also written to address some of the criticisms made by the Texas court.

(10) "Substantial portion" means that material on the following sites meets the definition of "material harmful to minors" as defined in this section if:

(a) On a social media platform, more than 33-1/3% of its total user accounts contain any material harmful to minors, or if more than 33-1/3% of one or more user's page on that platform contains material harmful to minors;

(b) On a search engine, more than 33-1/3% of its hypertext links to web pages in response to any user query will link the user to any material harmful to minors;

(c) On a search engine, more than 33-1/3% of its thumbnail images in response to any user query contain any material harmful to minors;

(d) On a website, including a search engine, if more than 33-1/3% of the total material contained on it or on any individual webpage is harmful to minors. If a website links by hypertext link to the material of a third-party website, the material on such third-party website shall not be considered toward the total percentage of material if that third-party website does not contain material harmful to minors and if such linking does not constitute an attempt to intentionally dilute the percentage calculation of material harmful to minors in order to evade the provisions of this section.

(11) (a) "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.

(b) "Transactional data" includes records from mortgage, education, and employment entities.

Liability for publishers and distributors – Age verification – Retention of data – Exceptions.

(1) A commercial entity that knowingly and intentionally publishes or distributes material harmful to minors on the Internet on either a website, or on an individual webpage, whichever contains less content, and that contains a substantial portion of such material,⁹ shall be held liable in a civil action for damages to any person harmed by that conduct if the entity fails to perform reasonable age verification methods to verify the age of an individual attempting to access the material.

(2) A commercial entity or third party that performs the required age verification shall not retain any identifying information of the individual after access has been granted to the material.

⁹ The Texas law used a 1/3 rule to define "substantial." In *Free Speech Coalition v. Colmenero* (USDC W.D. Tex. August 2023) the court found uncertainty in that Texas language. This Model Act cures that. The court said "H.B. 1181 limits its coverage to a "commercial entity that knowingly and intentionally publishes or distributes material on an Internet website, including a social media platform, *more than one-third of which is sexual material harmful to minors.*" H.B. 1181 § 129B.002(a). But it is unclear whether '*one-third*' modifies 'material' or 'website.'" *Id.*, slip. op. at 30 (emphasis added). Our Model Act more explicitly defines how that 1/3 metric is determined.

(3) A commercial entity that is found to have violated this section shall be liable to an individual for damages resulting from a minor's accessing the material, including court costs and reasonable attorney fees as ordered by the court. Damages in a private civil action under this section may include compensatory damages and damages for emotional pain and suffering, and shall include punitive damages if the conduct of the defendant is found to be willful, wanton, or reckless.

(4) A commercial entity that is found to have knowingly retained identifying information of the individual after access has been granted to the individual shall be liable to the individual for damages resulting from retaining the identifying information, including court costs and reasonable attorney fees as ordered by the court.

(5) This section shall not apply to any bona fide news or public interest broadcast, website video, report, or event and shall not be construed to affect the rights of a news-gathering organization.

(6) No Interactive Computer Service, including any internet service provider, affiliate or subsidiary of an internet service provider, search engine or cloud service provider in the business of providing access to or for the posting of user content on an internet platform, website, network or social media site, shall be held to have violated the provisions of this section solely for providing access or connection to or from a website or other information or content on the Internet, or a facility, system, or network not under that provider's control, including transmission, downloading, storing, or providing access; provided, however, that an Interactive Computer Service that is an information content provider for or that participates in a venture with, and knowingly benefits from¹⁰, a commercial entity in violation of (1) regarding that entity's knowing and intentional publishing or distribution of material harmful to minors, is liable for damages under (1) and (1a).

Enforcement by the State Attorney General¹¹

(A)(1) The attorney general may conduct an investigation of the alleged violation under this Act and initiate a civil action on behalf of the state to assess civil penalties. Prior to asserting a cause of action, the attorney general shall provide the commercial entity with a period of time of not less than thirty days to comply with this Section.

(2) Enforcement by the attorney general in this section is in addition to, and is not a limitation of, the rights of private persons to pursue a civil action under this Act.

(B)(1) Any commercial entity that violates this Section may be liable for a civil penalty, to be assessed by the court, of not more than five thousand dollars for each day of

¹⁰ Compare with 18 U.S.C. sec. 1595 that imposes liability against any entities that "knowingly benefit[] from" human trafficking, upheld at the motion stage against a sec. 230 argument in *Salesforce*, n. 5, *supra*.

¹¹ This language is borrowed from Louisiana House Bill 77, which passed into law earlier this year. This was an addendum to the initial Louisiana age verification law to help strengthen enforcement. We have omitted textual cross-references to Louisiana statutes.

violation to be paid to the Department of Justice, in order to fund the investigation of cyber-crimes involving the exploitation of children. In addition to the remedies provided in this Section, the attorney general may request and the court may impose an additional civil penalty not to exceed ten thousand dollars for each violation of this Section against any commercial entity found by the court to have knowingly failed to perform reasonable age verification methods to verify the age of individuals attempting to access the material. The civil penalty shall be paid to the Department of Justice in order to fund the investigation of cyber-crimes involving the exploitation of children.

(2) Each violation may be treated as a separate violation or may be combined into one violation at the option of the attorney general.

(3) Any commercial entity that violates this Section may be liable to the attorney general for all costs, expenses, and fees related to investigations and proceedings associated with the violation, including attorney fees.

(4) If the court assesses a civil penalty pursuant to this Section, the Department of Justice shall be entitled to legal interest from the date of imposition of the penalty until paid in full.

Addendum 1: Age Brackets to Determine Harm to Minors

In *Free Speech Coalition v. Colmenero* (USDC W.D. Tex. August 2023) the court intimated that part of the reason it placed an injunction on Texas' age verification law was because it failed to differentiate between ages under 18. In other words, the law treated the harmfulness of pornography the same for a 17-year-old as for a 7-year-old. One way to avoid that argument is to establish harmfulness separately for certain age brackets. Here is one approach that could be used in the bill's definitions section:

(6) "Minor" means any person under 18 years old, and as to the application of this law to questions of harm to minors, harmfulness to minors shall be determined:

(a) separately as to minors under the age of 10;

(b) separately as to minors from ages of 10 to and including 14;

(c) separately as to minors from the ages of 15 to and including 17.¹²

¹² See: [Exposure to sexually explicit media in early adolescence is related to risky sexual behavior in emerging adulthood - PMC \(nih.gov\)](#): "Exposure to sexually explicit media in early adolescence had a substantive relationship with risky sexual behavior in the emerging adulthood." See also: [Age-appropriate-behaviours-book.pdf \(ncsby.org\)](#) (age bracketing the evaluation of child sexual behavior for 0-4 years, 5-9, 9-12, and 13-18). See also: [Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis - ScienceDirect](#) (bracketing ages of 3-5, 6-12, and 13-17).

Addendum 2: Specified Age Verification Methods

Similarly, in *Free Speech v. Colmenero* (USDC W.D. Tex. August 2023), the court suggested that the Texas age verification law needed to be more specific about the various methods of age verification that pornography websites could use to fulfill the requirements of the law. We recognize that there are both political and policy reasons not to include every possible form of age verification in the text of the legislation, but if we were to do so, we would add the following section after (9) in our model legislation:

(9)(a) A determination of whether an age verification method is “reasonable” shall include such factors as technological feasibility, operational effectiveness of the age verification system, and the scale and number of users and the primary consumer use of a specific Interactive Computer Service. An age verification system that violates any other part of this section is not reasonable. A method may be reasonable if it employs one or more of the following in a manner that effectively prevent minors from accessing material harmful to minors:

1. Biometric identification system that verifies age, or
2. A method that blocks or screens out Pop Up Ads that contain material that is harmful to minors or Pop Up Ads that provides access to such content, or
3. Content filtering, or,
4. Coupled with one or more effective methods, a tracking system that follows only an adult user’s digital trail with such user’s consent so that the adult user need not repeatedly re-establish their adult status online when accessing material that would be otherwise harmful to minors, provided that the system does not track the digital trail of a minor.¹³

¹³ The absence of any of these four methods was used by the court in *Free Speech Coalition v. Colmenero*, *infra* n. 9 below, to conclude that the Texas law was not the least restrictive means to achieve its otherwise legitimate goal.