Federal Law - Obsenity.pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

Obscenity

> The Supreme Court has ruled that, *"transmitting obscenity and child pornography, whether via the Internet or other means, is... illegal under federal law for both adults and juveniles."*
>
> -*Reno v. ACLU*, 521 U.S. 844 (1998).

Obscenity

Obscenity is not protected under First Amendment rights to free speech, and violations of federal obscenity laws are criminal offenses. The U.S. courts use a three-pronged test, commonly referred to as the *Miller* test, to determine if given material is obscene. Obscenity is defined as anything that fits the criteria of the *Miller* test, which may include, for example, visual depictions, spoken words, or written text.

Federal law makes it illegal to distribute, transport, sell, ship, mail, produce with intent to distribute or sell, or engage in a business of selling or transferring obscene matter. Convicted offenders face fines and imprisonment. Although the law generally does not criminalize the private possession of obscene matter, the act of receiving such matter could violate federal laws prohibiting the use of the mails, common carriers, or interactive computer services for the purpose of transportation. (For more information, see Citizen's Guide to Federal Law on Obscenity).

Obscenity Law and Minors

Federal law strictly prohibits the distribution of obscene matter to minors. Any transfer or attempt to transfer such material to a minor under the age of 16, including over the Internet, is punishable under federal law. It is also illegal to use misleading website domain names with intent to deceive a minor into viewing harmful or obscene material. For example, using a cartoon character or children´s television program in the domain of a website that contains harmful or obscene material may be punishable under federal law.

In addition, visual representations, such as drawings, cartoons, or paintings that appear to depict minors engaged in sexual activity and are obscene are also illegal under federal law.

It is important to note that the standard for what is harmful to minors may be different

than the standard for adults, and offenders convicted of obscenity crimes involving minors face harsher penalties than if the crimes involved only adults (For more information, see Citizen's Guide to Federal Law on Obscenity).

CEOS's Role

The Child Exploitation and Obscenity Section (CEOS) remains dedicated to the enforcement of federal obscenity laws. CEOS attorneys work with the High Technology Investigative Unit (HTIU), the Federal Bureau of Investigation (FBI), and United States Attorney's Offices throughout the country to investigate and prosecute violations of federal obscenity law.

The use of the Internet to distribute obscenity has blurred traditional notions of jurisdiction. CEOS maintains a coordinated, national-level law enforcement focus to help coordinate nationwide investigations and initiatives. Given the importance of community standards under the *Miller* test, however, CEOS recognizes that the full commitment and support of local United States Attorney's Offices, who best know local community standards, are absolutely essential to the federal obscenity enforcement efforts.

Updated August 11, 2023

U.S. Department of Justice

Criminal Division

950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Criminal.Division@usdoj.gov

Criminal Division Citizen Phone Line
202-353-4641

Citizen's Guide To U.S. Federal Law On Obscenity

18 U.S.C. § 1460- Possession with intent to sell, and sale, of obscene matter on Federal property
18 U.S.C. § 1461- Mailing obscene or crime-inciting matter
18 U.S.C. § 1462- Importation or transportation of obscene matters
18 U.S.C. § 1463- Mailing indecent matter on wrappers or envelopes
18 U.S.C. § 1464- Broadcasting obscene language
18 U.S.C. § 1465- Transportation of obscene matters for sale or distribution
18 U.S.C. § 1466- Engaging in the business of selling or transferring obscene matter
18 U.S.C. § 1466A- Obscene visual representations of the sexual abuse of children
18 U.S.C. § 1467- Criminal forfeiture
18 U.S.C. § 1468- Distributing obscene material by cable or subscription television
18 U.S.C. § 1469- Presumptions
18 U.S.C. § 1470- Transfer of obscene material to minors
18 U.S.C. § 2252B Misleading domain names on the Internet
18 U.S.C. § 2252C Misleading words or digital images on the Internet

The U.S. Supreme Court established the test that judges and juries use to determine whether matter is obscene in three major cases: *Miller v. California*, 413 U.S. 15, 24-25 (1973); *Smith v. United States*, 431 U.S. 291, 300-02, 309 (1977); and *Pope v. Illinois*, 481 U.S. 497, 500-01 (1987). The three-pronged *Miller* test is as follows:

1. Whether the average person, applying contemporary adult community standards, finds that the matter, taken as a whole, appeals to prurient interests (*i.e.*, an erotic, lascivious, abnormal, unhealthy, degrading, shameful, or morbid interest in nudity, sex, or excretion);
2. Whether the average person, applying contemporary adult community standards, finds that the matter depicts or describes sexual conduct in a patently offensive way (*i.e.*, ultimate sexual acts, normal or perverted, actual or simulated, masturbation, excretory functions, lewd exhibition of the genitals, or sado-masochistic sexual abuse); and

3. Whether a reasonable person finds that the matter, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Any material that satisfies this three-pronged test may be found obscene.

Federal law prohibits the possession with intent to sell or distribute obscenity, to send, ship, or receive obscenity, to import obscenity, and to transport obscenity across state borders for purposes of distribution. Although the law does not criminalize the private possession of obscene matter, the act of receiving such matter could violate the statutes prohibiting the use of the U.S. Mails, common carriers, or interactive computer services for the purpose of transportation (See 18 U.S.C. § 1460; 18 U.S.C. § 1461; 18 U.S.C. § 1462; 18 U.S.C. § 1463). Convicted offenders face fines and imprisonment. It is also illegal to aid or abet in the commission of these crimes, and individuals who commit such acts are also punishable under federal obscenity laws.

In addition, federal law prohibits both the production of obscene matter with intent to sell or distribute, and engaging in a business of selling or transferring obscene matter using or affecting means or facility of interstate or foreign commerce, including the use of interactive computer services. (See 18 U.S.C. § 1465; 18 U.S.C. § 1466). For example, it is illegal to sell and distribute obscene material on the Internet. Convicted offenders face fines and up to 5 years in prison.

Moreover, Sections 1464 and 1468 of Title 18, United States Code, specifically prohibit the broadcast or distribution of obscene matter by radio communication or by cable or subscription television respectively. Convicted offenders under these statutes face fines and up to 2 years in prison.

Obscenity Involving Minors

Federal statutes specifically prohibit obscenity involving minors, and convicted offenders generally face harsher statutory penalties than if the offense involved only adults.

Section 1470 of Title 18, United States Code, prohibits any individual from knowingly transferring or attempting to transfer obscene matter using the U.S. mail or any means or facility of interstate or foreign commerce to a minor under 16 years of age. Convicted offenders face fines and imprisonment for up to 10 years.

In addition, Section 1466A of Title 18, United State Code, makes it illegal for any person to knowingly produce, distribute, receive, or possess with intent to transfer or distribute visual representations, such as drawings, cartoons, or paintings that appear to depict minors engaged in sexually explicit conduct and are deemed obscene. This statute offers an alternative 2-pronged test for obscenity with a lower threshold than the *Miller* test. The matter involving minors can be deemed obscene if it (i) depicts an image that is, or appears to be a minor

engaged in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse and (ii) if the image lacks serious literary, artistic, political, or scientific value. A first time offender convicted under this statute faces fines and at least 5 years to a maximum of 20 years in prison.

There are also laws to protect children from obscene or harmful material on the Internet. For one, federal law prohibits the use of misleading domain names, words, or digital images on the Internet with intent to deceive a minor into viewing harmful or obscene material (See 18 U.S.C. §§ 2252B, 2252C). It is illegal for an individual to knowingly use interactive computer services to display obscenity in a manner that makes it available to a minor less than 18 years of age (See 47 U.S.C. § 223(d) –Communications Decency Act of 1996, as amended by the PROTECT Act of 2003). It is also illegal to knowingly make a commercial communication via the Internet that includes obscenity and is available to any minor less than 17 years of age (See 47 U.S.C. § 231 –Child Online Protection Act of 1998).

The standard of what is harmful to minors may differ from the standard applied to adults. Harmful materials for minors include any communication consisting of nudity, sex or excretion that (i) appeals to the prurient interest of minors, (ii) is patently offensive to prevailing standards in the adult community with respect to what is suitable material for minors, (iii) and lacks serious literary, artistic, political, or scientific value for minors.

In addition to facing imprisonment and fines, convicted offenders of federal obscenity laws involving minors may also be required to register as sex offenders. Furthermore, in some circumstances, obscenity violations involving minors may also be subject to prosecution under federal child pornography laws, which yield severe statutory penalties (For more information, see Citizen´s Guide to U.S. Federal Child Pornography Laws).

Updated August 11, 2023

U.S. Department of Justice

Criminal Division

950 Pennsylvania Avenue, NW

Washington, DC 20530-0001

Criminal.Division@usdoj.gov

Criminal Division Citizen Phone Line

202-353-4641

Filter Law - Schools and Libraries .pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

NATIONAL CONFERENCE OF STATE LEGISLATURES

7700 EAST FIRST PLACE | DENVER, COLORADO | 80230
OFFICE: 303-364-7700 | FAX: 303-364-7800

Children and the Internet
Laws Relating to Filtering, Blocking and Acceptable Internet Usage Policies in Publicly Funded Schools and Libraries

Jan. 31, 2023

Overview of State Laws

Twenty-eight states and Puerto Rico have internet filtering laws that apply to publicly funded schools or libraries. The majority of these states simply require school boards or public libraries to adopt internet use policies to prevent minors from gaining access to sexually explicit, obscene or harmful materials. However, some states also require publicly funded institutions to install filtering software on library terminals or school computers.

Federal Children's Internet Protection Act (CIPA)

Congress in 2000 enacted the Children's Internet Protection Act (CIPA) as part of the Consolidated Appropriations Act. The act provides for three different types of funding: 1) aid to elementary and secondary schools; 2) Library Services and Technology Act (LSTA) grants to states for support of public libraries; and 3) the E-Rate program that provides technology discounts to schools and public libraries.

CIPA requires public libraries that participate in the LSTA and E-Rate programs to certify that they are using computer filtering software to prevent the on-screen depiction of obscenity, child pornography or other material harmful to minors. The act allows adult library patrons to request that a librarian disable the filtering software. To receive E-Rate discounts, libraries are not allowed to disable filtering programs for minor users. The Federal Communications Commission website provides background information about the Children's Internet Protection Act.

Supreme Court Ruling on CIPA

In June 2003, the U.S. Supreme Court upheld CIPA, overturning an earlier court ruling that had prevented the law from taking effect in libraries. In *United States v. American Library Association*, the court ruled that CIPA does not violate the First Amendment, even though it may block some legitimate sites, because libraries may disable the filters for adult patrons upon request.

A summary of state laws follows.

State Laws Relating to Filtering, Blocking and Acceptable Internet Usage Policies in Publicly Funded Schools and Libraries

STATE	CITATION	APPLIES TO SCHOOLS	APPLIES TO LIBRARIES	SUMMARY
ARIZONA	Ariz. Rev. Stat. Ann. §34-501 et seq.	X	X	Requires public libraries to install software *or* develop policies to prevent minors from gaining access on the internet to materials harmful to minors. Requires public schools to install computer software that would prevent minors from gaining access to materials harmful to minors.
ARKANSAS	Ark. Stat. Ann. §6-21-107 Ark. Stat. Ann. §13-2-103	X	X	Requires school districts to develop a policy and to adopt a system to prevent computer users from accessing materials harmful to minors. Requires public libraries to adopt a policy to prevent minors from gaining access to materials harmful to them.
CALIFORNIA	Cal. Education Code §18030.5		X	Requires public libraries that receive state funds to adopt a policy regarding internet access by minors.
COLORADO	Colo. Rev. Stat. §22-87-101 et seq. Colo. Rev. Stat. §24-90-401 et seq. Colo. Rev. Stat. §24-90-603	X	X	Requires public schools to adopt and enforce reasonable policies of internet safety that will protect children from obtaining harmful material. Provides grants to publicly supported libraries, including school libraries, that equip public access computers with filtering software and that have policies to restrict minors from accessing obscene or illegal information. Requires public libraries to adopt a policy of internet safety for minors that includes the operation of a technology protection measure for computers with internet access.
DELAWARE	Del. Code tit. 29, §6601C et seq.		X	Requires public libraries to have acceptable use policies and prohibits the use of library computers or mobile devices to access illegal or obscene materials. The minor's parent or guardian must specify the level of access to the internet the minor may have.

GEORGIA	Ga. Code §20-2-324 Ga. Code §20-5-5	X	X	Requires public schools and public libraries to adopt and enforce reasonable policies of internet safety that will protect children from access to harmful material. Prohibits a public school or library from receiving state funds unless it implements and enforces the acceptable-use policy.
IDAHO	Idaho Code §33-132 Idaho Code §33-1025 Idaho Code §33-2741	X	X	Requires each local school district in the state to adopt and file an internet use policy with the state superintendent of public instruction. The policy, approved by the local board of trustees, shall require filtering technology that blocks internet materials that are harmful to minors, establish disciplinary measures for violators, and provide a component of internet safety to be integrated into school instructional programs. Public libraries receiving public moneys and governed by the provisions of chapters 26 and 27, title 33, Idaho Code, that offer use of the internet or an online service to the public shall have in place a policy of internet safety for minors including the operation of a technology protection measure with respect to any publicly accessible wireless internet access or publicly accessible computers with internet access and that protects against access through such computers or wireless internet access to visual depictions that are obscene or child pornography or harmful to minors; and shall enforce the operation of such technology protection measure during any use of a computer or wireless internet access by a minor.

INDIANA	Ind. Code §20-26-5-40.5 Ind. Code §36-12-1-12	X	X	Each school corporation and charter school shall adopt and implement an internet use policy that: (1) prohibits the sending, receiving, viewing, or downloading of materials that are harmful to minors (as described in IC 35-49-2-2) on computers and other technology related devices owned by the school corporation or charter school; (2) provides for the use of hardware or installation of software on computers and other technology related devices described in subdivision (1) to filter or block internet access to materials that are harmful to minors; and (3) establishes appropriate disciplinary measures to be taken against persons violating the policy established under this section and shall use hardware or install software on computers and other technology related devices to filter or block internet access to materials that are harmful to minors. Each school corporation and charter school shall post on the school corporation's or charter school's internet web site the internet use policy The board of a public library shall adopt a policy concerning the appropriate use of the internet or other computer network by library patrons in all areas of the library.
IOWA	Iowa Code §256.57		X	Requires public libraries that apply for and receive state "Enrich Iowa Program" money to have an internet use policy in place, which may or may not include internet filtering.
KANSAS	Kan. Stat. Ann. §75-2589	X	X	Any school district that provides public access to a computer shall implement and enforce technology protection measures to ensure that no minor has access to visual depictions that are child pornography, harmful to minors or obscene. Any public library that provides public access to a computer shall implement and enforce technology protection measures to: (A) Ensure that no minor has access to visual depictions that are child pornography, harmful to minors or obscene; and (B) ensure that no person has access to visual depictions that are child pornography or obscene.

KENTUCKY	Ky. Rev. Stat. §156.675	X		Requires the Department of Education to develop regulations to prevent sexually explicit material from being transmitted via education technology systems.
LOUISIANA	La. Rev. Stat. Ann. §17:100.7	X		Each governing authority of a public elementary or secondary school shall adopt policies, in accordance with policies adopted by the State Board of Elementary and Secondary Education, regarding access by students and employees to internet and online sites that contain or make reference to harmful material the character of which is such that it is reasonably believed to be obscene, child pornography, conducive to the creation of a hostile or dangerous school environment, pervasively vulgar, excessively violent, or sexually harassing in the school environment all as defined by any applicable state or federal laws and the policies adopted pursuant to this Subsection. Such policies shall include but not be limited to prohibitions against accessing sites containing information on the manufacturing or production of bombs or other incendiary devices. Any policies adopted by a governing authority of a public elementary or secondary school pursuant to the provisions of this Subsection shall include the use of computer-related technology or the use of internet service provider technology designed to block access or exposure to any harmful material as specified in Paragraph (1) of this Subsection, or both.
MARYLAND	Md. Education Code Ann. §23-506.1		X	Requires county-state libraries to adopt policies to prevent minors from obtaining access to obscene materials via the internet.
MASSACHUSETTS	Mass. Gen. Laws ch. 71, §93	X		Requires public schools providing computer access to students to have a policy regarding internet safety measures to protect students from inappropriate subject matter and materials that can be accessed via the internet.
MICHIGAN	Mich. Comp. Laws §397.606		X	Requires libraries to use a system to prevent minors from viewing obscene or sexually explicit matter, or to reserve separate terminals exclusively for adults or children so as to prevent minors' access to obscene or sexually explicit matter.

MINNESOTA	Minn. Stat. §125B.15 Minn. Stat. §134.45 Minn. Stat. §134.50	X	X	Requires all computers at a school site with access to the internet available for student use must be equipped to restrict, including by use of available software filtering technology or other effective methods, all student access to material that is reasonably believed to be obscene or child pornography or material harmful to minors under federal or state law. A school site is not required to purchase filtering technology if the school site would incur more than incidental expense in making the purchase. A school district receiving technology revenue under section 125B.26 must prohibit, including through use of available software filtering technology or other effective methods, adult access to material that under federal or state law is reasonably believed to be obscene or child pornography. Requires public library computers with access to the internet available for use by children under 17 to be equipped to restrict, including by use of available software filtering technology or other effective methods, access to material that is reasonably believed to be obscene or child pornography or material harmful to minors. Also requires public libraries that receive state money to prohibit, including through the use of available software filtering technology or other effective methods, adult access to material that under federal or state law is reasonably believed to be obscene or child pornography.
MISSOURI	Mo. Rev. Stat. §182.825 et seq.	X	X	Requires public school and public libraries with public access computers to either (a) equip the computer with software or a service to restrict minors' access to material that is pornographic for minors, or (b) develop a policy that establishes measures to restrict minors from gaining access to such material.
NEW HAMPSHIRE	N.H. Rev. Stat. Ann. §194:3-d	X		Requires school boards to adopt a policy regarding internet access for school computers and establishes liability for violation of the policy.
NEW YORK	N.Y. Education Law §260(12)		X	Requires public libraries to establish policies concerning patron use of computers.

OHIO	Ohio Rev. Code Ann. §3302.42 Ohio Rev. Code Ann. §3314.21	X		For any internet- or computer-based community school, the contract between the sponsor and the governing authority of the school described in section 3314.03 of the Revised Code shall specify a requirement that the school use a filtering device or install filtering software that protects against internet access to materials that are obscene or harmful to juveniles on each computer provided to students for instructional use. The school shall provide such device or software at no cost to any student who works primarily from the student's residence on a computer obtained from a source other than the school.
OKLAHOMA	Okla. Stat. tit. 70, §11-201 et seq.	X	X	Digital or online library database resources offered by school districts, charter schools, virtual charter schools, state agencies, public libraries, or universities to students in kindergarten through 12th grade shall have safety policies and technology protection measures that: 1. Prohibit and prevent a user of the resource from sending, receiving, viewing, or downloading materials that are child pornography or obscene materials, as defined in Section 1024.1 of Title 21 of the Oklahoma Statutes, or materials that depict child sexual exploitation, as defined in Section 843.5 of Title 21 of the Oklahoma Statutes; and 2. Filter or block access to child pornography or obscene materials, as defined in Section 1024.1 of Title 21 of the Oklahoma Statutes, or materials that depict child sexual exploitation, as defined in Section 843.5 of Title 21 of the Oklahoma Statutes.
PENNSYLVANIA	Pa. Stat. tit. 24, §4601 et seq.	X	X	Requires school boards and publicly funded libraries to adopt and enforce acceptable use policies for internet access that include the (1) use of software programs reasonably designed to block access to visual depictions of obscenity, child pornography or material that is harmful to minors; or (2) selection of online servers that block access to visual depictions of obscenity, child pornography or material that is harmful to minors.

PUERTO RICO	P.R. Code Ann. tit. 18, §1118a	X	X	All public and private schools, libraries and any other public or private institution that offers services through computers with access to the internet, the obligation to implement technological devises or filters as necessary in computers available to children and youths under the age of 18, in order to restrict and identify the access and use of pornographic material that is harmful and detrimental to the physical and emotional safety and to the integrated development of boys, girls and underage youths.
SOUTH CAROLINA	S.C. Code Ann. §10-1-205 et seq.	X	X	Requires publicly funded libraries and public school libraries to adopt policies intended to reduce the ability of the user to access websites displaying obscene material. Also establishes a pilot program to evaluate the use of filtering software in libraries.
SOUTH DAKOTA	S.D. Codified Laws Ann. §22-24-55 et seq.	X		Requires schools to equip computers with filtering software or to adopt policies to restrict minors from access to obscene materials.
TENNESSEE	Tenn. Code §49-1-221	X		Requires the development of acceptable internet use policies for public and private schools to protect children from certain online material.
UTAH	Utah Code Ann. §9-7-215 et seq. Utah Code Ann. §53G-7-1001 et seq.	X	X	Prohibits a public library from receiving state funds unless the library enforces measures to filter internet access to certain types of images; allows a public library to block materials that are not specified in this bill; and allows a public library to disable a filter under certain circumstances. Prohibits school boards from receiving state funds unless local school boards adopt and enforce a policy to restrict access to internet or online sites that contain obscene material.

VIRGINIA	Va. Code §22.1-70.2 Va. Code §42.1-36.1	X	X	Requires public libraries to adopt internet use policies. Requires public schools to adopt internet use policies that 1) prohibit transmitting or viewing illegal material on the internet, 2) prevent access by students to materials the school determines harmful, and 3) select technology to filter or block child pornography and obscenity. Requires each school division and public library to post its internet use policies on its website.
WISCONSIN	Wis Stat. §16.997	X		Except as provided in section 196.218(4t), the department of administration shall promulgate rules establishing an educational telecommunications access program to provide educational agencies with access to data lines. The rules shall establish eligibility requirements for an educational agency to participate in the program established under sub. (1) and to receive additional telecommunications access under section 16.998, including a requirement that a charter school sponsor use data lines to benefit pupils attending the charter school and a requirement that internet access to material that is harmful to children, as defined in section 948.11(1)(b), is blocked on the computers of juvenile correctional facilities that are served by data lines subsidized under this section.

OTHER RELATED STATE LAWS

STATE	CITATION	SUMMARY
CONNECTICUT	Conn. Gen. Stat. §10-262n	The Department of Education shall administer, within available appropriations, a program to assist local and regional school districts to improve the use of information technology in their schools. Under the program, the department shall provide grants to local and regional boards of education and may provide other forms of assistance such as the provision of purchasing under state-wide contracts with the Department of Information Technology. Grant funds may be used for: (1) Wiring and wireless connectivity, (2) the purchase or leasing of computers, and (3) interactive software and the purchase and installation of software filters.
FLORIDA	Fla. Stat. §257.12(3)	Encourages public libraries to adopt an internet safety education program, including the implementation of a

		computer-based educational program.
LOUISIANA	La. Rev. Stat. §51:1426	Requires internet service providers to make available to subscribers who are Louisiana residents a product or service that enables the subscriber to control a child's use of the internet.
MARYLAND	Md. Commercial Law Code §14-3701 et seq.	Requires internet service providers to make parental controls that enable blocking or filtering of websites available to subscribers in the state.
NEVADA	Nev. Rev. Stat. §603.100 et seq.	Requires internet service providers to offer, under certain circumstances, products or services that enable subscribers to regulate and monitor a child's use of the internet.
TEXAS	Tex. Business & Commerce Code §§323.001 et seq.	A person who charges a fee to provide an interactive computer service shall provide free of charge to each subscriber of the service in this state a link leading to fully functional shareware, freeware, or a demonstration version of software or to a service that, for at least one operating system, enables the subscriber to automatically block or screen material on the internet. Establishes a civil penalty of $2,000 for each day the provider fails to comply.
UTAH	Utah Code §76-10-1231	Requires internet service providers, upon request by a consumer, to provide in-network filtering or filtering software to prevent transmission of material harmful to minors.
UTAH	Utah Code §78B-6-2201 et seq. Contingent upon five additional states enacting similar legislation	Beginning on Jan. 1 of the year following the year this bill takes effect, a manufacturer shall manufacture a device that, when activated in the state, automatically enables a filter that: (1) when enabled, prevents the user from accessing or downloading material that is harmful to minors on: (a) mobile data networks; (b) applications owned and controlled by the manufacturer; (c) wired internet networks; and (d) wireless internet networks; (2) notifies the user of the device when the filter blocks the device from downloading an application or accessing a website; (3) gives a user with a passcode the opportunity to unblock a filtered application or website; and (4) reasonably precludes a user other than a user with a passcode the opportunity to deactivate, modify, or uninstall the filter.

NCSL Contact: Heather Morton, 303-856-1475, heather.morton@ncsl.org

Filter Laws 2023-2024 .pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

NATIONAL CONFERENCE OF STATE LEGISLATURES

7700 EAST FIRST PLACE | DENVER, COLORADO | 80230

OFFICE: 303-364-7700 | FAX: 303-364-7800

Internet Filtering 2024 Legislation

March 1, 2024

Jurisdiction	Bill Number	Bill Title	Bill Status	Bill Summary
Alabama	H 167	Filter Requirements on Internet Enabled Devices	Pending	Relates to consumer protection; provides certain requirements for the use of a filter on certain Internet-enabled devices in this state; provides certain requirements for the filter and authorizes a civil action for a violation.
Alaska	S 245	Obscene Material Filters	Pending	Relates to obscene material filters for electronic devices used by minors; provides for an effective date.
Arizona	H 2661	Electronic Devices and Filters and Obscene Material	Pending	Relates to electronic devices; relates to filters; relates to obscene material.
Arkansas	None			
California	None			
Colorado	None			
Connecticut	None			
Delaware	None			
District of Columbia	None			
Florida	H 1129	Harm To Minors	Pending	Requires manufacturers of tablets or smartphones to manufacture such devices so that a filter is enabled upon activation; provides for enforcement; provides civil liability for

				individuals who enable passwords to remove a filter on a device in possession of minor; increases criminal penalties for certain offenses; prohibits persons who are of at least a specified age from knowingly engaging in communication that is part of pattern of communication or behavior that meets specified criteria.
Florida	S 1196	Protect Our Children Act	Pending	Cites this act as the Protect Our Children Act; requires manufacturers of tablets or smartphones to manufacture such devices so that a filter meeting certain requirements is enabled upon activation of the device in the State; authorizes the Attorney General to enforce the act; provides for damages; increases criminal penalties for adults who intentionally lure or entice, or who attempt to lure or entice, children under a specified age into a structure, dwelling or conveyance for other than a lawful purpose.
Georgia	H 338	Student Technology Protection Act	Pending - Carryover	Amends the Quality Basic Education Act, so as to provide for the inclusion of methods for the promotion of the safe and appropriate use of technology and responsible digital citizenship in the comprehensive character education program; revises requirements for internet safety polices in public schools; requires local boards of education and governing bodies of charter schools to annually submit acceptable-use policies and technology protection measures for review by the State Board of Education.
Guam	None			
Hawaii	None			
Idaho	H 663	Education	Pending	Amends and adds to existing law to require school districts to establish internet access policies to block certain content and to establish digital literacy instruction for students in grades 6 through 12.
Idaho	S 1222	Child Safety	Pending	Add new chapter to the Idaho code establishing provisions requiring certain internet filters on computer devices used by children.
Idaho	S 1253	Child Safety	Pending	Adds to existing law to establish provisions requiring certain internet filters on computer devices used by children.

Illinois	H 5163	Database Resources for Students Act	Pending	Creates the Database Resources for Students Act; provides that a school district, State agency, public library, or public university or community college may offer digital or online library database resources to students in grades kindergarten through 12 only if the provider of the resources verifies that all the resources have safety policies and technology protection measures that prohibit and prevent a user of the resources from sending, receiving, viewing, or downloading and filter or block access.
Indiana	S 201	Minor Use of Mobile Devices and Social Media	Pending	Relates to minor use of mobile devices and social media; requires the manufacturer of a mobile smart device that incorporates an adult content filter and that is sold in the state after specified date to configure the operating system of the mobile smart device, such that the adult content filter is enabled upon activation of the mobile smart device, and in a manner that reasonably ensures that a minor cannot disable the adult content filter.
Iowa	H 2114	Minors Using Mobile Devices	Pending	Relates to minors using mobile devices, including protections for minors, civil liability, and provides penalties.
Iowa	S 50	Requirements for Filters on Mobile Devices	Pending	Relates to requirements for filters on mobile devices activated in the state; provides for civil liability for manufacturers of mobile devices for certain violations; includes penalties.
Iowa	S 2213	Minors Using Mobile Devices	Pending	Relates to minors using mobile devices, including protections for minors and civil liability.
Kansas	None			
Kentucky	H 463	Protection of Children Using Social Media	Pending	Defines terms; specifies what entities are subject to this Act; requires digital service providers to register the age of the user; specifies the duties of digital services providers relating to agreements with minors; requires digital service providers to develop internal controls to prevent minors from being exposed to obscene matter, create parental monitoring tools, prevent advertising certain goods and services to minors, and provide information related to algorithms and content promotion.
Louisiana	None			
Maine	H 847	Student Data Collection Best Practices	Pending	Provides that the Department of Education shall submit a report to the Joint Standing Committee on Education and Cultural Affairs on school internet and student data collection policies and efforts

				to ensure that the state is using best practices, including but not limited to ensuring that schools are using appropriate internet and digital media filtering hardware and software; appropriates funds.
Maryland	H 772	Online Child Protection Act	Pending	Prohibits a person from selling an Internet-connected device that is intended for minors unless the device is sold with a certain filter, certain privacy settings, and other features; makes a violation of the prohibition an unfair, abusive, or deceptive trade practice that is subject to the enforcement and penalties under the State Consumer Protection Act; requires that preference be given to certain grant applications that include the use of broadband providers.
Maryland	H 1311	Obscene Material Device Filters	Pending	Requires, beginning a specified date, all devices activated in the state to enable a certain filter to prevent minors from accessing obscene material; prohibits a certain person from deactivating the filter; provides that a manufacturer of a device and certain persons are subject to civil and criminal liability for certain conduct related to device filters; authorizes the attorney general to take certain actions against persons who violate the Act.
Maryland	S 780	Online Child Protection Act	Pending	Prohibits a person from selling an Internet-connected device that is intended for minors unless the device is sold with a certain filter, certain privacy settings, and other features; makes a violation of the prohibition an unfair, abusive, or deceptive trade practice that is subject to the enforcement and penalties under the Maryland Consumer Protection Act; requires that preference be given to certain grant applications that include the use of broadband providers that implement the use.
Massachusetts	None			
Michigan	None			
Minnesota	H 1894	Public Safety	Pending	Relates to public safety; establishes the Human Trafficking and Child Exploitation Prevention Act; provides for rulemaking; requires a report.
Minnesota	S 846	Public Safety	Pending	Relates to public safety; establishes the Human Trafficking and Child Exploitation Prevention Act; provides for rulemaking; requires a report.

Mississippi				
Missouri	S 906	Sexual Exploitation of Vulnerable Persons	Pending	Modifies provisions relating to the sexual exploitation of vulnerable persons.
Missouri	S 1084	Obscene Websites	Pending	Relates to obscene websites.
Montana	No 2024 legislative session			
Nebraska	L 635	Access to Digital and Online Resources	Pending	Provides requirements regarding access to digital and online resources provided for students by school districts, schools, and the State Library Commission.
Nevada	No 2024 legislative session			
New Hampshire	None			
New Jersey	A 3819	Human Trafficking and Child Exploitation Prevention	Pending	Regards the Human Trafficking and Child Exploitation Prevention Act; requires Internet connected devices to have blocking capability in certain circumstances.
New Mexico	None			
New York	S 379	Parental Controls for Internet Services	Pending	Offers parental controls for internet services.
North Carolina	H 786	Youth Health Protection Act	Pending	Protects minors from administration of puberty blockers and cross-sex hormones and other related actions, procedures, and treatments; prohibits obscenity on smart phones for minors.
North Dakota	No 2024 legislative session			
N. Mariana Islands	Not available			
Ohio	None			
Oklahoma	H 1050	Human Trafficking and Child Exploitation	Pending	Relates to human trafficking and child exploitation; creates the Human Trafficking and Child Exploitation Prevention Act; defines terms; directs retailers of Internet-enabled devices to equip

				products with certain filters; requires retailers of Internet-enabled devices to ensure functionality of filters; establishes reporting requirements; directs retailers to submit reports of child pornography to certain tipline; prohibits retailers from blocking access to certain websites.
Oklahoma	H 3097	Crimes and Punishments	Pending	Relates to crimes and punishments; defines terms; makes commercial entities liable for publishing or distributing obscene material on the Internet; provides internet and cellular service subscribers the opportunity to make certain request; requires commercial entities to block access without charge; establishes liability provisions for violations; provides exemptions from liability; prohibits the retention of identifying information.
Oklahoma	H 3277	Student Digital Safety and Awareness Act	Pending	Relates to schools; creates the Student Digital Safety and Awareness Act; directs boards of education to adopt and implement digital safety policies; lists components to address in digital safety policy; requires data privacy and protection measures and transparency in data collection; mandates schools to report annually on the digital safety policy effectiveness; directs the state Department of Mental Health and Substance Abuse Services to oversee and ensure compliance with act.
Oklahoma	S 1959	Consumer Protection	Pending	Relates to consumer protection; defines terms; allows for damages to be sought under certain conditions; prohibits commercial entities from distributing certain material without verification; provides for lawful access to certain material; prevents a commercial entity from being held liable under certain conditions; prohibits a commercial entity from retaining individual's information; exempts certain providers; requires attorney general to take certain action; authorizes attorney general to develop.
Oregon	None			
Pennsylvania	H 1501	Filtered Devices	Pending	Provides for filtered devices required, for manufacturer liability, for damages and for civil action for enforcement and penalties.
Pennsylvania	S 187	Child Internet Protection Act	Pending	Amends the act known as the Child Internet Protection Act; provides for title and for definitions; makes editorial changes.

Puerto Rico	H 1020	Computer Privacy Citizen Orientation Office Duties	Pending	Amends Law 5 of 1973, the Organic Act of the Department of Consumer Affairs, in order to group and consolidate into a single Act, the functions, powers and duties of the Citizen Orientation Office on Protection of Computer Privacy, and Against Obscenity and Child Pornography on Radio, Television and the Internet; arranges for the transfer of all property, documents, unspent amounts of allowances, items and other funds held and under the custody of the Office to the Department of Consumer Affairs.
Rhode Island	None			
A. Samoa	Not available			
South Carolina	H 4540	Childrens Default to Safety Act	Pending	Relates to Safeties Act; provides protections for children against unfiltered devices; provides necessary definitions; requires manufacturers of smart phones and tablets to automatically enable and passcode-protect the filters blocking material harmful to minors on devices activated in this state; subjects manufacturers to civil and criminal liability for violations of this article; subjects individuals to criminal and civil liability for violations of this article.
South Carolina	H 4572	Requirements and Restrictions on School Districts	Pending	Provides the state Department of Education shall review and approve all internet websites, computer applications, and other computer software proposed for use on school-issued digital devices to ensure their alignment to curriculum approved for use in schools; provides related requirements and restrictions on school districts and students; provides the department shall develop a procedure for district personnel to obtain such approval.
South Carolina	H 4689	Children's Device Protection Act	Pending	Enacts the Children's Device Protection Act by adding specified article so as to require smartphones and tablets to contain certain filters and other features to prevent minors from accessing obscene materials through the internet; creates civil and criminal liability for manufacturers of these devices for certain violations of the provisions of this article, with exceptions, and to authorize the attorney general and solicitors to bring actions to enforce the provisions of the article.

South Carolina	S 591	Childrens Default to Safety Act	Pending	Enacts the children's default to safety act; provides protections for children against unfiltered devices; provides necessary definitions; requires manufacturers of smart phones and tablets to automatically enable and passcode protect the filters blocking material harmful to minors on devices activated in this state; subjects manufacturers to civil and criminal liability for violations of this article; subjects individuals to criminal and civil liability for violations of this article.
South Dakota	H 1197	Minors Obscene Materials Access Restriction Publication	To governor	Requires the publication of measures taken to restrict the access of obscene materials by minors; provides that each public school in the state shall equip each public access computer with software that will limit minors ability to gain access to obscene matter or materials or purchase internet connectivity from an internet service provider that provides filter services to limit access to obscene materials; provides that each public library in the state shall take specified actions.
Tennessee	H 761	Consumer Protection	Pending	Enacts the Youth Mental Health Safety Act.
Tennessee	S 138	Consumer Protection	Pending	Enacts the Youth Mental Health Safety Act; relates to devices capable of accessing the internet.
Texas	No 2024 legislative session			
Utah	S 104	Childrens Device Protection Act	To governor	Requires a tablet or a smartphone manufactured on or after specified date to automatically enable a filter upon device activation by a minor; requires the filter to prevent a minor user of the device from accessing material that is obscene; provides that an adult individual, other than the parent or legal guardian of the minor in possession of a device, who disables the filter on a device in possession of a minor for the purpose of disseminating pornography to the minor, commits a class A misdemeanor.
Vermont	None			
Virginia	None			
U.S. Virgin Islands	None			

Washington	None			
West Virginia	H 5191	Permitting Obscenity in Schools	Pending	Relates to permitting obscenity in schools.
Wisconsin	None			
Wyoming	None			

NATIONAL CONFERENCE OF STATE LEGISLATURES

7700 EAST FIRST PLACE | DENVER, COLORADO | 80230

OFFICE: 303-364-7700 | FAX: 303-364-7800

Internet Filtering 2023 Legislation

Nov. 7, 2023

Jurisdiction	Bill Number	Bill Title	Bill Status	Bill Summary
Alabama	H 298	Consumer Protection	Failed - Adjourned	Relates to consumer protection; provides requirements for certain internet filters on electronic devices.
Alaska	None			
Arizona	None			
Arkansas	None			
California	None			
Colorado	None			
Connecticut	None			
Delaware	None			
District of Columbia	None			
Florida	H 379	Student Use of Social Media Platforms	**Enacted**	Relates to technology in k-12 public schools; requires each district school board to adopt an internet safety policy for student access to the internet provided by the school district; provides requirements; requires each school district to prohibit and prevent student access to social media through internet access provided by the school district; provides an exception; prohibits the use of certain platforms on district-owned devices and through internet access provided by the school district.

Florida	S 1426	Device Filtering	Failed - Adjourned	Relates to device filtering; requires manufacturers of tablets or smartphones to manufacture such devices so that a filter meeting certain requirements is enabled upon activation of the device in this state; subjects such manufacturer to civil and criminal liability for certain acts of noncompliance; provides an exception; provides civil liability for individuals who enable a password to remove the required filter on a device in the possession of a minor under certain circumstances.
Georgia	H 338	Student Technology Protection Act	Pending - Carryover	Amends the Quality Basic Education Act, so as to provide for the inclusion of methods for the promotion of the safe and appropriate use of technology and responsible digital citizenship in the comprehensive character education program; revises requirements for internet safety polices in public schools; requires local boards of education and governing bodies of charter schools to annually submit acceptable-use policies and technology protection measures for review by the State Board of Education.
Guam	None			
Hawaii	None			
Idaho	S 1057	Protection of Minors	Failed - Adjourned	Adds to existing law to establish the Parental Rights Protection of Minors Act to protect minors from exposure to harmful materials on certain devices.
Idaho	S 1163	Protection of Minors	Failed	Adds to existing law to establish the Parental Rights Protection of Minors Act to protect minors from exposure to harmful materials on certain devices; requires the installation of filters on certain devices; defines device to mean a tablet or a smartphone manufactured on or after Jan. 1 of the year following the year this chapter takes effect.
Illinois	None			
Indiana	None			
Iowa	S 50	Requirements for Filters on Mobile Devices	Pending - Carryover	Relates to requirements for filters on mobile devices activated in the state; provides for civil liability for manufacturers of mobile devices for certain violations; includes penalties.
Kansas	None			
Kentucky	None			
Louisiana	None			

Maine	H 847	Student Data Collection Best Practices	Pending - Carryover	Provides that the Department of Education shall submit a report to the Joint Standing Committee on Education and Cultural Affairs on school internet and student data collection policies and efforts to ensure that the state is using best practices, including but not limited to ensuring that schools are using appropriate internet and digital media filtering hardware and software; appropriates funds.
Maryland	H 1082	Handheld Smart Device Child Blocker	Failed - Adjourned	Requires a manufacturer of a tablet or smart phone manufactured on or after a specified date and sold or offered for sale in the state to manufacture the tablet or smart phone to automatically enable a certain filter, when activated in the state, that prevents the user from accessing or downloading material on certain networks and applications that is harmful to minors.
Massachusetts	None			
Michigan	None			
Minnesota	H 1894	Public Safety	Pending - Carryover	Relates to public safety; establishes the Human Trafficking and Child Exploitation Prevention Act; provides for rulemaking; requires a report.
Minnesota	S 846	Public Safety	Pending - Carryover	Relates to public safety; establishes the Human Trafficking and Child Exploitation Prevention Act; provides for rulemaking; requires a report.
Mississippi	H 151	School Districts Wireless Learning Environments	Failed	Requires each school district to develop and implement a wireless technology infrastructure to serve all the schools and classrooms in the district; requires the districts to develop a strategic plan to provide for a two-year phase in period for complete implementation; requires districts to conduct thorough needs assessments to determine existing ability and network capacity and recommendations for future network traffic.
Mississippi	H 1315	Pornographic Media Exposure to Children in K-12	**Enacted**	Regulates pornographic media exposure to children in K-12; regulates digital and online resources provided by K-12 vendors.
Mississippi	H 1341	Digital or Online Resources or Databases	Failed	Relates to digital or online resources or databases; requires vendors to verify technology protection measures for persons under the specified age.

Missouri	S 308	Authentication of Access to Obscene Websites	Failed - Adjourned	Requires internet service providers to authenticate access to obscene websites and provide subscribers the ability to create an authentication to access such websites.
Montana	H 349	Electronic Devices Obscenity Filter Requirements	Failed	Establishes obscenity filter requirements for electronic devices; provides that a person who is not a minor's parent or legal guardian may not provide a minor with the passcode to remove the obscenity filter on an electronic device; provides for legislative intent.
Nebraska	L 635	Access to Digital and Online Resources	Pending - Carryover	Provides requirements regarding access to digital and online resources provided for students by school districts, schools, and the State Library Commission.
Nevada	None			
New Hampshire	None			
New Jersey	A 2952	Human Trafficking and Child Exploitation Prevention Act	Pending	Concerns the Human Trafficking and Child Exploitation Prevention Act; requires Internet-connected devices to have blocking capability in certain circumstances.
New Mexico	None			
New York	S 379	Parental Controls for Internet Services	Pending	Offers parental controls for internet services.
North Carolina	H 786	Youth Health Protection Act	Pending	Protects minors from administration of puberty blockers and cross-sex hormones and other related actions, procedures, and treatments; prohibits obscenity on smart phones for minors.
North Carolina	S 2360	Safety Policies and Technology Protection Measures	Vetoed	Provides that digital or online library database resources offered by a school district, state agency, or public library to students in certain grades must have safety policies and technology protection measures that prohibit and prevent a user of the resource from sending, receiving, viewing, or downloading materials constituting an obscene performance or explicit sexual material and filter or block access to explicit material; provides that an employee who violates this is guilty of a class B misdemeanor.
N. Mariana Islands	Not available			
Ohio	None			

Oklahoma	H 1050	Human Trafficking and Child Exploitation	Pending - Carryover	Relates to human trafficking and child exploitation; creates the Human Trafficking and Child Exploitation Prevention Act; defines terms; directs retailers of Internet-enabled devices to equip products with certain filters; requires retailers of Internet-enabled devices to ensure functionality of filters; establishes reporting requirements; directs retailers to submit reports of child pornography to certain tipline; prohibits retailers from blocking access to certain websites.
Oregon	None			
Pennsylvania	H 1501	Filtered Devices	Pending	Provides for filtered devices required, for manufacturer liability, for damages and for civil action for enforcement and penalties.
Pennsylvania	S 187	Child Internet Protection Act	Pending	Amends the act known as the Child Internet Protection Act; provides for title and for definitions; makes editorial changes.
Puerto Rico	H 1020	Computer Privacy Citizen Orientation Office Duties	Pending	Amends Law 5 of 1973, the Organic Act of the Department of Consumer Affairs, in order to group and consolidate into a single Act, the functions, powers and duties of the Citizen Orientation Office on Protection of Computer Privacy, and Against Obscenity and Child Pornography on Radio, Television and the Internet; arranges for the transfer of all property, documents, unspent amounts of allowances, items and other funds held and under the custody of the Office to the Department of Consumer Affairs.
Rhode Island	None			
A. Samoa	Not available			
South Carolina	S 591	Childrens Default to Safety Act	Pending - Carryover	Enacts the children's default to safety act; provides protections for children against unfiltered devices; provides necessary definitions; requires manufacturers of smart phones and tablets to automatically enable and passcode protect the filters blocking material harmful to minors on devices activated in this state; subjects manufacturers to civil and criminal liability for violations of this article; subjects individuals to criminal and civil liability for violations of this article.
South Dakota	None			
Tennessee	H 761	Consumer Protection	Pending - Carryover	Enacts the Youth Mental Health Safety Act.

Tennessee	S 138	Consumer Protection	Pending - Carryover	Enacts the Youth Mental Health Safety Act; relates to devices capable of accessing the internet.
Texas	H 18	Protection of Minors	**Enacted**	Relates to the protection of minors from harmful, deceptive, or unfair trade practices in connection with the use of certain digital services and electronic devices, including the use and transfer of electronic devices to students by a public school.
Texas	H 231	Primary and Secondary Schools Online Library Resources	Failed - Adjourned	Relates to the purchase of online library resources for primary and secondary schools by the state, State Library and Archives Commission.
Texas	H 1853	Parent Access to Public School Library Internet Portals	Failed - Adjourned	Relates to parental access to public school library Internet portals and restriction of access to certain public school library materials for the parent's student.
Texas	H 1936	Electronic Device Filters for Certain Explicit Material	Failed - Adjourned	Relates to electronic device filters for certain explicit material; creates a criminal offense; provides a civil penalty.
Texas	H 1945	Access to Certain Internet Websites in Public Schools	Failed - Adjourned	Relates to access to certain internet websites in public schools.
Texas	H 2673	Use and Transfer of Electronic Devices to Students	Failed - Adjourned	Relates to requirements for the use and transfer of electronic devices to students by a public school.
Utah	None			
Vermont	None			
Virginia	None			
U.S. Virgin Islands	None			
Washington	None			
West Virginia	None			
Wisconsin	None			
Wyoming	None			

Making SmartPhones and Apps Safe.pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

IFS Institute for Family Studies

DECEMBER 21, 2023

How to Make Smartphones and Apps Safer for Kids

by Michael Toscano Brad Wilcox, @BRADWILCOXIFS Elizabeth Self

Highlights

- Given the ubiquity of smartphones among children, the state also has a role in protecting the minds and hearts of the rising generation.
- Engaged parents can only do so much to fend off the worst of smartphones when the app stores themselves are deceptive.
- Devices and the app stores they host are virtually unregulated, especially for child safety, even though they are the most common way minors stumble across pornography.

"These are first-of-their-kind bills in the United States," Utah Gov. Spencer Cox said in March at the signing of SB152, which required social media companies operating in Utah to age-verify users and obtain explicit parental consent for users under the age of 18 to open an account. "That's huge that Utah is leading out in this effort," he said.

The governor's remarks about Utah's leadership were more than true: they were an understatement. Since then, three other states—Texas, Louisiana and Arkansas—signed bills modeled after Utah's work, and the Institute for Family Studies has heard from lawmakers around the country that they aim to follow suit in 2024. Utah's legislative boldness has kicked off a revolution in how lawmakers fight to protect our kids from predatory social media platforms.

But Utah has not stopped there. In October, the governor's office announced it was joining a group of 42 states, red and blue, in a lawsuit against Meta, the parent company of Facebook and Instagram, for developing techniques and adopting practices with the intent of addicting kids for profit. This was the second time Utah, under Cox's leadership, sued a social media company (the previous being against TikTok, probably the worst app for kids); nonetheless, the suit's bipartisan nature and its focus on how the design of a platform can undermine personal wellbeing is once again a watershed in confronting Big Tech on behalf of our children.

The state also passed legislation to keep underage users off pornography sites—which as a matter of practice turn a blind eye to the great mass of adolescents accessing their obscene and addictive wares—by once again requiring age verification. The law was upheld by a federal judge in a landmark decision in August, owing to the law's design, which put enforcement into the hands of parents by granting them a right to sue porn companies for damages should they fail to properly vet their child.

These efforts are exemplary, but they leave untouched one of the principal culprits driving the mental health crisis among American adolescents, as well as the principal means by which they access pornography—the devices themselves, smartphones and tablets.

Devices and the app stores they host are virtually unregulated, especially for child safety, even though they are the most common way that minors access social media and stumble across pornography. Regulators would never grant this same impunity to toy manufacturers, food producers or the providers of numerous other products and services to kids. And yet we give Apple and Google, the two most dominant device manufacturers, the benefit of the doubt to market their products to kids, allowing them to occupy their attention for hours on end and overshadow their mental and social lives without any meaningful oversight whatsoever.

Apple and Google's app stores and devices do not deserve this trust. As a recent policy brief, "Making Smartphones and App Stores Safe for Kids," by the Institute for Family Studies and the Ethics and Public Policy Center, shows, many apps in the app stores have been found to be inappropriately rated for kids, claiming to be child-friendly when they are really for older audiences. They also advertise inappropriate apps to users that these companies should know are kids, and allow apps with sexualized and indecent imagery to be marketed to kids in other apps rated as age appropriate.

As for access to pornography, even Pornhub's own research has shown that more than 80% of traffic to the site comes from handheld devices. Unsurprisingly, according to Common Sense Media, the average child encounters pornography at age 12, and in many cases far younger.

Engaged parents can only do so much to fend off the worst of smartphones when the app stores themselves are deceptive and when personal devices—so easy to slip into one's pocket in a pinch —can be easily used by kids to access apps and sites their parents know nothing about.

The device manufacturers have shown little interest in self-reform. It's no mystery why. They get a 30% commission on the sales of apps in the app stores and make a killing on advertising fees—so making their devices and app stores widely available to kids, a critical market, is in their interest. The more addictive the app, the better. If a child is addicted, his "time on device" is secured, meaning that he will continually generate data (which can be sold) and be primed for advertising access.

If social media platforms are the substance, device manufacturers are the dealers. Both must be held accountable.

What can a state like Utah do?

First, require age verification on the device level. It is critical to realize that Apple and Googlealready conduct age verification on their devices — Google standardizes this practice in the set-up process, and Apple conducts age verification when applicants sign up for an Apple credit card on their iPhone. What Google and Apple do *not* do is use this process for child safety. States looking for several options for how to facilitate verification can require it upon the purchase of a device or can require that age verification be conducted using a government-issued ID upon set up. (Notably, Apple and Google wallets already allow users to securely store their IDs).

Our second recommendation follows the first. Once age verification is complete, age-appropriate settings and parental controls should kick in automatically, on the device and in the app store, especially filters to block obscenity. This fix is a no-brainer, making it simple for parents to set up the device for child safety — which, currently, is uncharacteristically difficult, given the elegance and simplicity of these companies' other products. It would also ensure that only age-appropriate content, according to the various app store ratings, is made available to underage users.

This doesn't solve the tendency toward deceptiveness in the app stores themselves (a problem which will require other remedies perhaps secured by attorneys general as a condition of a future settlement). But it would still go a very long way to aligning underage users with child-friendly material.

Another important aspect of making devices safe-by-default is requiring parental consent for the download of new apps as well as the notification of parents with each download. But if lawmakers in Utah elect not to proceed with age verification, a second option is to require a default filter to block obscenity, not based on required age verification, but the age as determined through devices' existing set-up processes. This is the method endorsed by Protect Young Eyes and the National Center on Sexual Exploitation, two organizations that have endorsed the new policy brief.

Age verification on the device, accompanied with automatic age-appropriate defaults, would add a double layer of protection for kids, who would then be guarded from accessing pernicious apps at the level of the operating system (the device) and also—given the preexistence of SB152 in Utah—on the platform level.

Meta argues that age verification should be done by the device manufacturers *and not* by the platforms. This is self-serving and too risky for kids. The obvious problem is that while, yes, most kids are accessing social media platforms and pornography through their devices, they can also surf their way there on a parent's desktop or laptop.

Device-level regulation cannot be a means by which certain bad actors are empowered to shift blame to other bad actors — it is a means to draw the device manufacturers into the new regulatory reality for our kids, in which companies in Silicon Valley are required to keep their products from preying on children. Requiring device-level age verification on the smartphone or tablet, which would then be applied to various apps accessed through the device in the app store, would simplify the process and close the holes that kids sneak through to access objectionable platforms.

And finally, Utah should open up more litigation to hold device companies accountable by amending its so-called "little FTC act"—Utah Code Section 13-11-4 (1953)—to add "digital transactions" to its scope of jurisdiction.

States possess acts mirroring the federal FTC act (the Uniform Deceptive Trade Practices Act), which, among other things, protects consumers from companies engaging in misleading, fraudulent and abusive advertising. These are important means to protect children from companies that want to lure them into potentially harmful purchases.

In Utah's little FTC act, the simple addition of the phrase "digital transactions" would help clarify the state's authority and power to bring causes of action against device manufacturers for allowing abusive marketing of apps to kids. As Adam Candeub has written, such a simple amendment offers "a range of potential remedies, including actual damages, enhanced damages, injunctive or declaratory relief, attorneys' fees, court costs, and rescission for unfair and deceptive practices committed in the conduct of trade or commerce." Additionally, the law could be made even stronger by adding amendments that spell out explicitly that the laws prohibit app stores and apps from abusively marketing their goods to children.

Society once thought it wise to put the whole wide world into the hands of our kids. But with everything from pro-Hamas propaganda to pornography easily accessible on these devices, we have relearned the bitter lesson that there are monsters out there. And to give one's child access to the whole world has turned out to be more than reckless—it is foolish.

We strongly encourage parents to resist giving their children smartphones until they are at least 16. But given the ubiquity of smartphones among children, the state also has a role in protecting the minds and hearts of the rising generation.

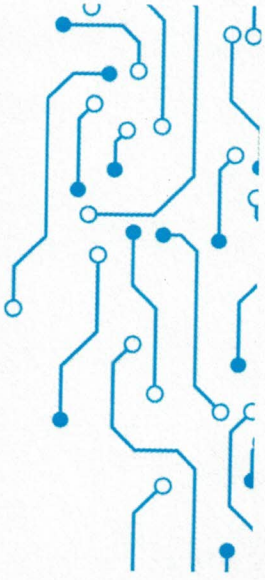
These three proposals, if properly implemented, would help make smartphones safer for kids. If Utah took these up, it would once again be leading a movement that would follow across the 50 states.

Michael Toscano is executive director of the Institute for Family Studies. Brad Wilcox is the Future of Freedom Fellow at the Institute for Family Studies. Elizabeth Self is outreach coordinator at the Institute for Family Studies.

Editor's Note: This article appeared first at Deseret News. It has been reprinted here with permission.

Obsenity and Smartphones.pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

Making Smartphones and App Stores Safe for Kids: Federal, State, and Industry Measures



Published November 16, 2023

PDF

By CLARE MORELL & MICHAEL TOSCANO

Download PDF

Summary for State Legislators Summary for Congress

Executive Summary

This brief will present the current harms to children caused and facilitated by smartphones (and tablets) and the app stores they host, driven by Big Tech companies' financial incentives that misalign with the welfare of kids. The device-and-app-store industry has been virtually unregulated, especially for child safety. We present several possible solutions for lawmakers and industry leaders to implement, which ensure devices and their app stores are safer for children and bring much-needed accountability.

Recently, there has been significant attention given to the harms of social media and online pornography for children, galvanizing lawmakers across several states to enact laws to require age verification of pornography sites[1] (blocking individuals under the legal age of 18 from gaining access) and parental consent for minors to open social media accounts (i.e., form online contracts).[2] At the federal level, three bipartisan bills to better protect kids online have gained momentum, the Kids Online Safety Act (KOSA), COPPA 2.0, and the EARN IT Act.[3] These measures are critical; however, they only address one *level* of the problem: the website (or platform). We fully support[4] and have effectively contributed[5] to this policy work, but will argue that it is now necessary to open up another front to address the threats to child safety online—directing attention toward the *devices* that serve as children's main portals to the internet and social media platforms (and a myriad of other apps).

We strongly advise parents, individually and as groups, to resist providing their kids a smartphone or tablet. Given how unsafe these devices are, they should be avoided and delayed until as close to adulthood as possible. We realize that, in many cases, such strong measures are not possible. This brief thus addresses the question of policy solutions that can be implemented to regulate smartphones and tablets to make them safer for kids and to ensure these devices provide an age-appropriate experience of apps and the internet for children. To that end, this brief takes a comprehensive assessment of the current situation, proceeding with a review of the legal landscape, arguing for device regulation and app store reform, and calling for specific actions by Congress, state lawmakers, and enforcement entities, like the Federal Trade Commission (FTC), and state attorneys general. For some solutions, we appeal to the companies themselves to make certain changes proactively, where lawmakers are limited by the First Amendment from mandating such requirements. Collectively, these measures all seek to accomplish two main goals: (1) make the devices and app stores safer for children by design and (2) correct companies' misaligned incentives that have fostered the current lawless conditions by opening these companies up to both litigation and competition.

We advise Congress to consider the following requirements for device manufacturers and app stores:

- Verify age on the device
- Automatically enable family-friendly device defaults for minor users (especially device filters to block obscenity)
- Prohibit apps and app stores from displaying obscene ads to children
- Amend device certification Federal Communications Commission (FCC) requirements
- Open up litigation by amending the Federal Trade Commission Act; and
- Open up competition in the app store market (requiring interoperability and side-loading of apps and other app stores)

We advise states to legislate the following requirements for device manufacturers and app stores:

- Verify age on the device
- Automatically enable family-friendly device defaults for minor users (especially device filters to block obscenity); and
- Open up litigation by amending existing state deceptive or unfair trade practices statutes ("Little FTC Acts")

We advise device manufacturers and app stores to take the following steps proactively, and failing to do that, we would call upon the Federal Trade Commission (FTC) and state attorneys general to seek such requirements as part of future settlement agreements:

- Adopt new, accurate age-rating systems for informed parental consent and other app store features for child safety
- Prevent mature ads from running in apps rated for minors and stop mature apps from being advertised to children in the app stores
- Provide additional "school mode" and "bedtime mode" settings to be made available as parental controls on devices; and
- Provide a "child safe" setting to be made available on devices (to be implemented on a parent's or family/shared devices).

In the brief that follows, these above recommendations are treated as larger categories encompassing several discrete measures that respond to different facets of the problem. We provide direction on implementation and weigh the various strengths and weaknesses of each approach. As the reader will find, there is no one silver bullet solution to recommend. Rather, a serious approach to addressing these problems will require comprehensive action at multiple levels. If nothing else, this is an opportunity for lawmakers, attorneys general, and even Big Tech itself to do the right thing. This brief serves as a guide for just that.

I. Introduction: Critical Problems and the Need for Solutions

The close association of technology with "progress" in our collective American imagination has granted smartphone companies and social media platforms (i.e., Big Tech) the enviable and unprecedented status of being permitted to service and engage with minors without meaningful safeguards. It is not controversial for lawmakers —recognizing the unique vulnerability of children—to apply regulations to ensure that toys, food, playgrounds, medications, furniture, clothing, television and radio are safe for children to use or consume, or to keep dangerous products from the market altogether.[6] But Big Tech's smartphones have been granted a *de facto* immunity by lawmakers. Smartphones have not been regulated for child safety whatsoever, though they now occupy the attention of minors for several hours per day, totally dominating them mentally and socially.[7]

Smartphones are more than a way of life—they are markets for other goods, made available through app stores, the rules of which device manufacturers define.[8] Even corner shops have legal duties to ensure that children cannot purchase items for which they are too young.[9] In a typical market, a good which is permitted by regulators to make it to the shelves can also be further regulated for age-appropriateness, as in the case of cigarettes, alcohol, tattoos, and numerous other goods.[10] Given the extraordinary power smartphones hold over the lives of children, Big Tech should be held to these same reasonable standards for consumer protection and child safety.

Even for consumers who are considered adults, labels that accurately reflect the contents of the product are required to assist in making an informed purchase.[11] Like the aforementioned, Big Tech's app stores on devices operate under no such rules. Apple and Google have become the "gatekeepers" to what children are accessing online and yet their app stores are extremely deceptive for consumers, especially parents.[12] Consumers assume that ratings and content descriptors will comply with existing consumer protection laws with accuracy and accountability. However, app ratings are neither accurate nor presented in a manner that guarantees informed consent.[13] Many apps in the app stores are very dangerous for kids, rated incorrectly,[14] or are not furnished with accurate descriptions or proper parental warnings; many apps that are rated as age-appropriate for kids can be found displaying ads *for other* apps or products that are sexually explicit or promote mature material.[15]

Existing parental controls lack the innovation, elegance, and consumer-friendly interfaces found in other Apple and Google products. The built-in tools are often difficult for parents to find and set up. Companies are not promoting their parental control tools as aggressively as their other products. Children reared on devices are often more tech-savvy than their parents and find workarounds; the tools themselves are frequently rife with bugs that the companies show little interest in resolving, such as in the case of Apple's parental controls that were prone to resetting without parents' awareness with iOS updates.[16] The bottom line is parents face serious challenges in safeguarding their children due to insufficient information from Big Tech about potential risks from their products and the presence of various backdoors and loopholes in their existing parental controls that they have not addressed. This is not an issue of ability, but of *priority*.

The root issue behind their lack of prioritizing child safety on their devices and app stores is misaligned incentives. Apple and Google make up to a 30% commission for every app sold in the app store (even for apps that are free to download, like social media apps, the app stores still make a commission from their in-app subscriptions).[17] And they also make profits off ads in the app store.[18] The more apps and ads that these app stores sell, the greater commission and profits they get. As a result, they are not incentivized to clean up their app stores, rate apps correctly, or provide clear parental warnings because these actions would undermine their profit model.

Furthermore, if Apple and Google really wanted to protect children, they could voluntarily conduct age verification on their devices and automatically enable certain safety default settings on the device for underage users, such as parental tools, limiting adult websites, and having their app stores only display apps rated

appropriate for their age. These companies possess the technical ability to do so.[19] Apple and Google have effectively integrated age verification into their devices already;[20] for example, the Apple Credit card process conducts age verification on its device to set up the card.[21]

Apple and Google could additionally enter into arrangements with social media platforms and other apps or sites with age thresholds (that are increasingly being required to verify age[22]) to enable their devices to communicate with the sites and platforms that a user satisfies the required age threshold, in order to help provide a more seamless user experience. This way the user could verify his or her age one time on the device, and then be granted access to platforms, sites, and apps as desired from the device, without re-verifying his age for each new app or site. This arrangement, however, will never happen voluntarily, because deploying these capabilities with a view to the public good is bad for their profits. Apple and Google would be helping aid future competitors, like Meta, in markets they want to enter by shouldering the responsibilities of age verification for them. And they do not want to voluntarily take up the responsibilities involved in verification. Thus, Apple, Google, and other smartphone companies have kept their heads down, hoping that all of the legislative attention remains on the social media platforms alone[23] and avoiding inclusion in laws that require age verification on the platform or site level.[24]

This status quo of device manufacturers and app store owners getting off the hook must not be permitted to endure. Just as a traditional market requires the regulation of specific products to function well, rules placed on each of these respective markets offering their goods to children are likewise essential.[25] The app stores offer the apps. The smartphone manufacturers design and sell smartphones (which are the main way children access social media and the internet today). These companies need to be held responsible too.

To give one final example of the need for device-level solutions, in 2023, a spate of laws passed in states around the country (Utah, Arkansas, Louisiana, Texas, Virginia, Montana, Mississippi, and North Carolina) requiring pornography sites and/or social media platforms to age verify users.[26] In the case of the former, the prurient content is unsuitable for minors; in the case of the latter, unfettered access to these sites without parental oversight is driving an unprecedented mental health crisis tormenting America's youth.[27] Unaddressed by these laws, however, is the reality that the smartphone is the most common point of entry to these sites.[28] PornHub reported in its annual 2022 data, for instance, that over 84% of viewers accessed the site through a smartphone.[29] The smartphone is essentially a laptop in kids' pockets, giving them constant, secret access to whatever is hidden away in the innumerable apps and expanses of the internet. The diminutive size of the device and its portability foster the conditions for deception between children and parents, making it very difficult (to near impossible) for guardians to effectively monitor. Thus, more policy action needs to be taken at the device-level to prevent smartphones from being the conduits through which bad content and actors harm our children.

A broader policy response to address these myriad issues at the device level and in app stores is critical, and should be a complement to, not a replacement for, age verification for adult websites,[30] or age verification and parental consent for social media platforms. It is important to still hold platforms and adult websites accountable for age verification since they are the ones hosting the content children are accessing, and, in the case of social media, the ones entering into contracts with our children.[31] Plus, smartphone devices are *not the only way* children can gain access.

This brief will outline several types of possible solutions toward this end to be taken by federal or state policymakers, as well as steps the industry could proactively take in pursuit of the common good. These are: (1) requiring age verification at the device level; (2) requiring default safety settings to be automatically enabled for minor device users; (3) addressing safety gaps in the app stores; (4) encouraging additional device-level safety tools for parents; and (5) amending existing laws to open up avenues of litigation to hold companies accountable for harms to children perpetrated at the levels of the device and app store.

II. Current legal landscape/background

"...the Internet is not as 'invasive' as radio or television... [and] that [c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content by accident... [and] odds are slim that a user would come across a sexually explicit sight by accident." Reno v. ACLU, 1997

With these naïve words, the Supreme Court struck down key provisions of the Communications Decency Act of 1996, by which Congress sought to protect minors from being sent "obscene or indecent messages," or from encountering them on websites they may engage.[32] *Reno*'s preference for an ungoverned internet, which left kids unprotected online, formed the mold for all subsequent court decisions, which have tilted unrelentingly in Big Tech's favor.[33] It is hard to underscore how spectacularly wrong these factual predicates have proven to be over the last 20 years.[34] Needless to say, the smartphone and other devices (as well as social media) totally obliterate them. The internet, now resting in the palm of our hands, has become so "invasive" that it has overthrown the preeminence of television and radio and even threatens to blur the lines between communications technology and the human person.[35]

This and otherrulings have created the conditions in which Big Tech companies are virtually unaccountable to lawmakers and parents alike. For example, *Ashcroft v. ACLU* struck down the subsequent Child Online Protection Act (1998), which required age verification for adult websites, on the grounds that "filters are more effective than age-verification requirements" and less burdensome to free speech (another set of factual predicates that have proved disastrously wrong).[36] Our libertarian jurisprudence has freed Big Tech to ignore child safety in the design of their products and has left parents alone to contend with one of the most powerful forces in human history.

Section 230, the provision of the Communications Decency Act that remains—which "protect[s] children from sexually explicit internet content"— has also failed to help, since its interpretation has been over-expanded by the courts to essentially immunize Big Tech from any liability whatsoever.[37] This includes liability for harms from its own product design, such as algorithms that help connect human traffickers with their victims, and liability for knowingly hosting illicit content on its platforms.[38] As one of this brief's authors has previously written, "Section 230 was meant to not only be a shield for internet service providers but also a sword against illicit content, allowing platforms to remove content like pornography to protect children, without being held liable for doing so."[39] In other words, Section 230 was passed on Congress's hope and expectation that it would encourage Big Tech to remove content harmful to kids by shielding platforms from publisher and speaker liability whenever they remove "obscene, lewd, lascivious, filthy, excessively violent, harassing" or similar material.[40] But several court rulings have since expanded Section 230 to protect Big Tech companies from liability *for knowingly failing to remove* pornographic and illegal content, even when such failure rises to the level of complicity, including for child sexual abuse material.[41] This leaves victims without any means of legal recourse other than to beg the platforms to take it down and renders parents helpless against the onslaught of pornography their children routinely access through social media.[42] In view of the obvious need to protect kids online, section 230 is all carrot and no stick.[43]

A final example of largely ineffective federal laws written to help families protect their children online is the Children's Online Privacy Protection Act, otherwise known as COPPA (1998).[44] COPPA was passed to bar companies from collecting data from children ages 12 and under without a parent's consent, setting the de facto age for social media use at 13. But COPPA only holds social media and other apps accountable for a minor (12 and under) being on their platforms if they possess "actual knowledge" of their age, rather than "constructive knowledge" (what they reasonably should know and could easily infer from an analysis of the aggregation of their user data). Thus, even the low age of 13 has not been enforced.[45] Under COPPA's current knowledge standard, enforcement actions by the FTC are extremely rare.[46] What was written to empower parents has made them

inconsequential, as underage minors can easily access these platforms, and the platforms are not held accountable. The lack of accountability has put companies in a race to the bottom to gain the youngest users for the sake of their own profits.

The sum total of our jurisprudence is granting these companies so much power we must beg them to police themselves. But that is a fool's bargain. Our kids can't suffer it any longer. These companies have shown beyond a doubt that they do not care to protect our children. So, government regulation—and a fundamental reconsideration of our jurisprudence informing it—is critical.[47]

III. Possible solutions

Any serious effort to address these issues will need to provide remedies at the device and app store levels and in so doing seek to correct the underlying misaligned incentives ultimately driving the current lack of safety for children on these devices.

1. Device-Level Age Verification (Federal or State)

These solutions could be enacted either at the federal or state level. When we speak of devices in the solutions that follow, we specifically mean smartphones and tablets.

Age verification at the device level is the best technical anchor for any subsequent device-level protections. In setting up a new smartphone, the user is *already required* to establish an Apple or Google ID and enter their birth date. Age verification could easily be tacked on to this set-up process for any smartphone or tablet. After a user enters her birth date, the next step in the device set-up process could be an age-verification requirement. No method of age verification is impervious to deception; nevertheless, confirming the ages of users by offering several reasonable age-verification methods to users should help align the vast majority of minors with age-appropriate products.[48] We suggest here several possible options that could be offered for accomplishing age verification on the device that also preserve user privacy:

a. Secure Upload/Scan of Government ID:

The user uploads official ID to the Apple or Google Wallet, or scans a photo of the ID using the device's camera during the age-verification step in device set-up, that matches the name associated with the device ID. Once the device scans the uploaded ID and the user's age is verified, the device automatically deletes the scan or photo of the ID, unless the user is choosing to store their Government ID in the Apple or Google Wallet, both of which already allow users to securely store their Government IDs.[49]

b. Apple Credit Card Age/ID Verification Process:

When a user applies for the Apple credit card, Apple uses the name, address, and birthdate the user provided for the Apple ID and Apple Pay to verify age with only the last four digits of the Social Security Number. The process takes 60 seconds. Apple has already developed the technical capacity to do this, though it has not yet publicly declared what its business purposes are.[50] This method could be easily applied to verify user age upon device setup.

c. In-Store Age Verification:

An employee of Apple or Google could conduct in-person age verification for those who do not want to provide additional information. An ID could be presented to an employee of Apple, Google, or the mobile phone provider. Upon successful verification, an "over 21" or "over 18" acknowledgment could be attached to the user's Apple or Google ID associated with the device.

d. Other Commercially Reasonable Methods:

While not as ideal in terms of effectiveness, legislators could also include a provision for any commercially reasonable method that relies on public or private transactional data, such as credit cards or bank information, to verify the age of the person attempting to access the material.

To ensure user privacy—which will be both essential, and in our technological age, feasible—it should be required that once age is verified, using whichever of the above methods, any underlying user information collected in the process (e.g., scan of government ID, etc.) must be immediately and permanently deleted. Thenceforward, the device can instead save the user's birth date as part of their device ID. (Or the device could generate a "cookie" or "token" in the age-verification process to use to subsequently communicate whether the user is over a certain age to apps, sites, and platforms that the user is trying to access, instead of retaining or transferring any underlying information about the user. See below for more details on how device verification could be used to satisfy website or platform verification requirements).

Age verification at the device level is critical—and, importantly, it is also a common practice by Google, one of the largest smartphone and device companies. Google already requires age verification when there is a change to the original Google ID birth date that would affect the adult status of the user. In this instance, age verification is completed by uploading a valid government ID or with a credit card.[51] As mentioned above, Apple's credit card application process has also demonstrated that it has similar capacity.[52]

One further consideration is how to implement age verification on smartphones or tablets that have already been set up, prior to the availability of such methods and requirements. Once such a law is enacted it would become the practice going forward for any new smartphone or tablet to require age verification in its set-up process. Age verification would be conducted by the device operating system and so the law could also be written to require manufacturers to push out an operating system update (e.g., Apple's iOS updates) to existing devices that are still being supported by the manufacturer that would then prompt users to undergo an age-verification process in order to continue using the device.[53] A final matter to note is that once a device is initially set up for one user (for example, an adult) it may not continue to be used by that same user (i.e., it gets passed down to a child), so legislators may want to additionally consider some type of re-authentication requirement at certain time periods (i.e., require that every two years an operating system update is pushed out to devices to require re-authentication of the user's age for the device).

Not every child is operating a Google, Apple, or Amazon device. For age verification to be uniformly accomplished at the device level, *all* existing smartphones and tablets, and those that enter the market in the future must be required to have these capabilities built in, which may necessitate some companies developing this infrastructure. This is the price that such companies will have to pay for serving minors.

Some have argued for age verification on the device level to replace site-level verification.[54] But, as mentioned above, device-level age verification is better understood as a complement rather than an alternative, for the simple reason that the very same sites that device-level verification may block can also be accessed on any web browser. It is important for the sites hosting adult content or social media platforms forming contracts with children to be held responsible themselves. A simple principle of defense is that where there are several vulnerable points of access, all are guarded to the best of our ability. Site-level and device-level verification requirements together offer the most comprehensive protection for children.

The two levels could also be integrated[55] to offer a more seamless user experience. For device-level verification to be used to satisfy website and platform verification requirements, device manufacturers must be willing—or, barring that, be legally required—to integrate their device-verification feature with other websites, apps, or platforms, which could be done by using a stored token or a Zero Knowledge Proof key[56] on the device. A device age-verification integration requirement should also prohibit app store providers, like Apple and Google, from blocking signals from apps or sites seeking access to the device's ZKP key or age-verification token when verifying a user's age. These measures would certainly make for a more seamless experience for the user, who would then only need to verify his age once at the device level. Thereafter the device (using a stored token or ZKP key) could communicate to apps, platforms, and websites his verification status automatically on his behalf, enhancing user privacy.

However, despite the benefit to users, no device companies will willingly provide verification information to platforms in order to help them satisfy their own age-verification requirements. This would be against their own profit interests, by relieving the burdens of such requirements on their competitors and handing them more business. So, if legislators are interested in integrating the two levels of age verification for the benefit of users, they will have to require such measures by law. If legislatures don't want to take on this integration battle, simply requiring device-level age verification (in addition to any adult website or social media platform verification), with corresponding age-appropriate defaults enabled (as explained next under solution #2), will by themselves go a long way in protecting children online.

2. Automatically Enable Family-Friendly Device Defaults for Minor Users (Federal or State)

The second piece accompanying this first solution is to require companies to automatically enable certain defaults on the device based on the age-verification process. However, if age verification at the device-level is not obligated, lawmakers could still require companies to automatically enable certain age-appropriate settings on the device based on the age of the user, determined during activation and account set up. (Current device set-up processes already ask for a user's birth date to associate with the Apple or Google ID and question whether the device is being enabled for a child. For birth dates registered under 18 or affirmation that the device is being set up for a child, default requirements for minor users would then be automatically enabled). Even if they are not being held liable for verifying the age of the user, companies could then be held liable for failing to enable specific default settings for minors based on user age determined during set up. While age verification will be most effective in protecting minors (as well as our preferred approach for child safety), much good would be achieved by simply requiring age-appropriate settings for device users. Thus, legislators should require the following default requirements to make devices more suitable for minors:

a. Device Filter to Block Obscenity Automatically Enabled:

Built-in device filters on smartphones, e.g., Google's "Block Explicit Sites" and Apple's "Limit Adult Websites," should be the automatic default setting for all new devices, smartphones, and tablets, unless age verification proving the user is over the age of 18 has been completed. Apple and Google already have the ability to block pornography (videos, website, images) on device browsers.[57] It should be the mandated default that obscenity is blocked for all device users not verified as over 18. This is the *most important* device default to require. If a state or Congress is only interested in requiring one default, let it be this one. This would force obscenity filtering to the "ON" setting for any device where the user is under 18; if consumers want to change their age (to confirm their adult status), or if a parent wants to deactivate the filter, they would then have to provide age verification. One final consideration: the bill could apply only to smartphones and tablets activated in the state on, for example, January 1st of the year following the bill's passage; or taking a broader approach, the bill, as mentioned above, could require manufacturers to include in their next operating system update an age-verification process that would then automatically enable the device filter for users not verified to be over the threshold of 18-years old.

A second option is to require a default filter to block obscenity, not based on required age verification, but the age as determined through devices' existing set-up processes. The organizations Protect Young Eyes (PYE) and the National Center on Sexual Exploitation (NCOSE) have put together a model device filter bill using this approach called the "Children's Device Protection" bill.[58] This legislation requires companies to determine the age of the user during activation and account set-up (but does *not* require they conduct age verification) and then requires operating systems on smartphones and tablets to automatically turn "ON" filtering technology to block obscenity when a device is activated for minors. Once a filter is engaged, it can only be turned "OFF" by an adult who provides reasonable age verification (this is the only instance in which verification is required). Parents, guardians, and state's attorneys general would be able to bring civil actions against manufacturers of devices that do not comply.

The advantage of PYE and NCOSE's approach is that it leverages what device manufacturers already do and the capabilities they already have. This would require nothing new of the companies; it would simply force them to automatically enable device filters whenever a device is set up for a minor. There is no reason that lawmakers should not be able, at the very least, to require this.

b. Parental Notification and Consent Enabled for App Downloads:

The existing parental control settings to require parental approval for any new app to be downloaded from the app store—called "Ask to Buy" for Apple and "Approve All Content" for Google—should be enabled automatically as the default for all users under 18. If they desire, a parent or guardian can turn this feature to "OFF"; having this setting automatically enabled for the devices of minors protects them from potentially dangerous or harmful apps and informs parents to make the best decisions for their children.

c. Content Restrictions Automatically Set to the Appropriate Age of the User:

Apple and Google have "Content Restrictions" settings already available where a parent can select the age ratings allowed for various forms of media on the device. For apps, a parent can decide that only apps rated 4+, 9+, 12+, or 17+ are to be made available to their child. Depending on the age of the device user determined by the age-verification process, or during the set-up process (if age verification is not required), the device should automatically make apps unavailable that are not age aligned according to ratings. The same goes for the content restrictions for the various movie and TV show ratings. Music, podcasts, and books should all be defaulted to "Clean" (as opposed to "Explicit"). A parent should be able to change these settings, especially if they want to make them even more restrictive than the child's current age. But, the content settings on the device should be defaulted to the age-appropriate content restrictions for minor users.

3. Encourage App Stores to Adopt New, Accurate Age-Rating Systems for Informed Parental Consent and Other App Store Features for Child Safety (Voluntary by Industry or Settlement Agreements; with Limited Options for Congress)

a. App Store Ratings Reform:

One consistent problem that parents face when seeking to improve the experiences of their children is that app ratings are often inaccurate and ineffective in signaling to parents what to expect from the content of a given app. Lack of a uniform age-rating system among app stores can cause confusion as apps are age-rated differently between the Google Play and Apple App Stores;[59] even worse, numerous ratings have been found to be consistently inaccurate,[60] giving parents false confidence that a product is safe for their children, only to find them encountering illicit content in the very app they recently approved.[61] Age verification can provide a

technical mechanism for better aligning consumers with age-appropriate content (see above)—but it is practically for naught if apps are improperly rated. While app rating standards and requirements cannot be mandated for companies because of First Amendment protections against compelled speech, we would highly encourage the app stores to voluntarily adopt standardized app ratings, much as the video game industry did in 1994. The recommendations that follow, however, particularly that of an app ratings board, should be targeted as provisions in any potential settlement agreements with app store companies, either from the FTC for unfair trade practice actions brought against the app stores or from state attorneys general for suits filed against the app store companies for unfair or deceptive trade practices (more on this in solution #5 below). Here are our recommendations for app stores to voluntarily adopt or for federal or state enforcers to include in any future settlement agreements with app stores:

I. STANDARDIZE APP STORE RATINGS OVERSEEN BY A NEW RATINGS BOARD:

The different rating systems used by Apple and Google can be confusing for users, similar to the situation Nintendo and Sega faced before the establishment of the Entertainment Software Ratings Board (ESRB) in 1994.[62] There must be a uniform set of standards, which implies the need to establish a new app ratings board for app stores. This will ensure that any new app stores that enter the market—or if, in the future, apps are allowed to be side-loaded onto smartphones without going through the default app store—would all abide by the same universal rating system imposed upon all apps.

II. IMPROVE THE ACCURACY OF RATINGS:

Apps in the Apple, Google, or other future app stores must have accurate age ratings and accurate content descriptors that explain interactive elements, similar to those of the ESRB or other types of media. Establishing specific, objective standards for rating apps, overseen by a ratings board, would improve the accuracy of ratings. Parental controls rely heavily on app age ratings in default safety settings. Consequently, deceptive app ratings mislead parents to believe their children are shielded from harmful or explicit content, when, in fact, they are not. Apps containing graphic content, harmful algorithms, targeted ads, or apps that allow strangers to direct message children should be rated as Mature (Google) or 17+ (Apple), or whatever the new uniform standard may be.

III. ALIGN APPLE'S 12+ RATING WITH COPPA:

Apple's 12+ rating for most social media apps fails to align with COPPA's mandate that children must be at least 13 to use apps that collect their data. A simple fix would elevate Apple's 12+ rating by one year to 13+.

IV. INFORM PARENTS ABOUT THE U.S. SURGEON GENERAL'S WARNING IN THE APP STORE:

In 2023, the United States Surgeon General Vivek Murthy issued an advisory warning about the harmful effects of social media on children.[63] No such warning appears for any social media apps in any app store. Rather, most social media apps are rated as safe for children over 12 and carry muted content warnings.[64] Murthy has also suggested raising the eligible age of social media use.[65] In the meantime, app store ratings could more accurately reflect the appropriateness of these platforms for children by giving them an even higher age rating than 12 or 13, such as 15 or 16. Congress could go one step further by enacting laws to require that certain apps must come with a U.S. Surgeon General's warning just like all cigarette packages have come with a health warning since 1965.[66]

V. MAKE APP STORE RATINGS AND DESCRIPTORS EASY TO LOCATE:

The app store ratings and descriptors are often buried, appearing in small font and far down on the screen, when a parent gets an alert for a request for a new app download.[67] This makes it hard for parents to make informed decisions.These must be made highly visible so parents can be fully cognizant of risks. Ratings, content descriptors,

and child contact risks (i.e., adults interacting with kids) must be prominently placed *above* the "approve" and "decline" options given to parents for new app downloads, rather than far below those buttons, to ensure parents have seen and understand all potential risks to their children.

In summary, these recommendations for app stores are aiming for a complete shift in the structure of the app stores, from being designed to most effectively market apps to being designed with the safety of children in mind.

b. Other App Store Improvements for Child Safety:

Age verification, automatic age-appropriate device defaults, and app store ratings reforms would solve many of the issues for parents in addressing the inherent current challenges to providing a child a smartphone. But there are a few remaining issues with app stores that targeted fixes could address (again, these would be mainly volunteered by the industry or included in settlement agreements), such as:

I. PREVENT MATURE ADS FROM RUNNING IN APPS RATED FOR MINORS:

Perhaps no single practice underscores the reality of Big Tech's unboundedness from moral obligation than its senseless practice of allowing sexually lurid and violent ads to be placed in apps rated as appropriate for minors.[68] In-app ads should not promote mature content or other apps that are rated Mature/17+ in apps that are rated lower than 17+ (Apple App Store) or Mature (Google Play). Evidence from parents has shown that ads promoting gambling, drugs, and sexual content are shown to children in a 12+ rated app, thus rendering the age ratings useless.[69] Even parents who pay for the ad-free versions of apps in a gaming app rated 12+ have been alarmed to see their children offered to view mature or explicit ads[70] to earn more tokens or points in the game.[71] The parental control content restrictions for apps become practically meaningless if any type of ad, including obscene ads, can appear in apps rated appropriate for children. App stores should prevent the apps it hosts from running explicit or mature ads inside apps rated appropriate for children. One specific, narrow requirement that Congress could impose by law to help this issue is to prohibit apps rated as appropriate for children from displaying obscene ads, since obscenity is not protected speech under the First Amendment and the government has a compelling interest in protecting children from it.[72]

II. STOP MATURE APPS FROM BEING ADVERTISED TO CHILDREN IN THE APP STORES:

Similar to the above, the practice of app stores advertising mature (17+) apps to minors undermines the whole project of app ratings.[73] App stores should not show or advertise mature (17+) apps to children age 16 and under, as determined by the device age-verification process, or Apple or Google ID birth date. The Apple App Store advertises dangerous 17+ chat roulette apps to users searching for 12+ apps.[74] It also directed a 10-year-old to download mature apps such as TikTok, Tinder, and YouTube as "Must Have Apps."[75] These apps are not appropriate for young children. Parental control content restrictions on the device that block access to apps rated above a certain age—which should be enabled by default for minor users (see above)—should also apply to the advertisements run for apps in the app stores. Apps that are available for download and apps that are *advertised* in the store should satisfy the rating level set by the device's content restrictions. Again, app stores will have to do this voluntarily or be forced to as a provision in a settlement agreement; but Congress could narrowly prohibit app stores from displaying obscene ads to children, or promoting and advertising obscene apps to children, since obscenity is not protected by the First Amendment.

4. Improving Devices for Child Safety (Voluntary by Industry or Settlement Provisions or FCC Certification)

a. Other Device Features Needed:

In addition to age verification, enabling defaults for minors, and addressing issues in the app stores, there remain several gaps in child safety at the device level that should be addressed with a few additional settings. It will be difficult to require these by law because of First Amendment protections; the public should agitate for companies to adopt these, and the FTC and state attorneys general should include these as provisions in future settlement agreements. These include:

I. PROVIDE "SCHOOL MODE" AND "BEDTIME MODE" SETTINGS TO BE MADE AVAILABLE AS PARENTAL CONTROLS:

Smartphone developers should be required to make both a "school mode" and a "bedtime mode" setting easily available as parental control options on the device. Apple and Google already have some of these settings, but they are buried deep in their Downtime feature; it is a user experience nightmare to navigate for parents. Simplicity (the specialty of these companies) and ease-of-use are needed. Downtime should be its own prompted step in ScreenTime setup with specific labels of "school mode" and "bedtime mode," each engageable with a single click by a parent. An easily engaged "school mode" would have certain defaults, such as automatically disabling all phone functions, except perhaps for call and calculator, from 8 am to 3 pm on weekdays. A "bedtime mode" would likewise have defaults to shut down all but a few functions, like the alarm clock, at night. Such features should be intuitive and easily engaged. Push notifications should be sent to remind parents to engage bedtime or school modes on smartphones for children under 18 (e.g., once a month) until they are executed, the same way companies relentlessly send push notifications for users to set up other device features more aligned with their priorities.

II. PROVIDE A "CHILD SAFE" SETTING TO BE MADE AVAILABLE (TO BE IMPLEMENTED ON SHARED/FAMILY DEVICES OR A PARENT'S PHONE):

More and more parents, increasingly aware of the mental health crisis among teens, proactively choose not to purchase a smartphone for their child, but allow them to borrow their device on occasion. Since it will be registered to an age-verified adult, the default device settings for under 18 would not be automatically enabled, nor would an adult likely want those settings enabled continually. Therefore, smartphone developers should create a "shared device" mode or "child safe" mode embedded in its operating system. For example, Netflix, Amazon Prime Video, and many other platforms allow for various age-appropriate experiences by enabling different users to log in on the same device.[76] Apple and Google should do the same. The "child safe" mode could then be enabled when a child is using a device that belongs to an adult. This temporary mode should block explicit websites and 17+ apps and turn on the other default settings required for smartphone users under 18 as outlined above.

b. Amend Device Certification Federal Communications Commission (FCC) Requirements:[77]

Another more overarching approach to improve devices for child safety would be amending the FCC's device certification requirements. The FCC plays an integral role in ensuring wireless devices are safe to use.[78] Google and Apple both develop and manufacture wireless devices.[79] Each one of those devices must go through an FCC authorization before they can enter into the market.[80] In other words, if Apple and Google want to provide users with mobile phones, tablets, streaming devices or routers,[81] they must go through the FCC first.

Congress could amend the Communications Act to mandate that any device requiring certification from the FCC must be equipped with an operating system that has certain mechanisms in place to protect children, such as built-in parental controls (including the additional settings mentioned directly above), device filters for obscene content (see solution #2 above), and other mechanisms to prevent children from accessing apps with harmful features.

5. Open Up Litigation by Amending Existing Deceptive Trade Practices and/or Open Up Competition in the App Store Market (Federal and State)

These amendments could be made at the federal or state level, though it will be more feasible to amend deceptive trade practice statutes at the state level and it will only be possible to open up competition in the app store market at the federal level.

As stated above, the underlying problem that has led to many of the specific device and app store issues today is Big Tech's drive to utilize minors as a major source of revenue. The financial incentive structure, in other words, pushes companies to prioritize financial rewards above the welfare of children. And there has been no corrective for this, because the traditional means of holding companies accountable for consumer protection—litigation—has been closed by the judicial expansions of Section 230.[82] To correct for this, a creative solution to open up channels of litigation is amending deceptive trade practice statutes, either the Federal Trade Commission Act's "unfair or deceptive trade practices" section, or any of the various state "Little FTC Acts." Another approach is to open these companies to greater competition in the app store and/or device market. We offer three possible solutions below:

a. Amend the Federal Trade Commission Act:

The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[83] This law is meant to protect consumers by preventing companies from engaging in deceptive or abusive advertising practices. Advertising and marketing to children is judged under a more protective standard, in appreciation of a child's limited ability to distinguish true from false and make reasoned decisions.[84] For example, the FTC used its authority under this Act to regulate advertising to children in the famous Joe Camel complaint.[85] Big Tech has become the new Big Tobacco by marketing its addictive and harmful products to young children.[86] App stores market to and serve children. And certain apps, like social media platforms and others, intentionally market themselves to children.[87] Apple has already been officially on notice about their deceptive app age ratings since 2019 when a Congressional Hearing was held to address app age ratings and child exploitation.[88] Child advocacy groups also wrote letters to Apple in 2021 and 2023, asking executives to fix the deceptive app age rating system.[89]But so far, no serious action has been taken to correct these abuses. Congress could encourage more aggressive FTC enforcement actions against app stores and apps, like social media, by amending the Federal Trade Commission Act's prohibition against "unfair or deceptive acts or practices in or affecting commerce"[90] to include an explicit prohibition for app stores and apps from abusively marketing their goods to children and deceptively age rating their apps.

b. Require Interoperability and Side-Loading to Open Up the App Market:

Another solution that can be achieved by Congress is to pass a law requiring interoperability to open up the app store market. Many of the current problems with the app stores, especially their harms to children, stem from their centralized authority.[91] Apple and Google are a duopoly in the app store market. Congress could pass legislation to help break up this duopoly and open up app stores to competition. One such federal bill that has already been introduced is the Open App Markets Act (OAMA) by Senators Blumenthal and Blackburn, which seeks to address the problem of overly-centralized authority.[92] The bill would require app market operators to allow for the download of third-party applications and app stores (requiring interoperability of third-party apps and app stores with their device software), which would decentralize the control of app stores (and the preferencing and promoting of their own apps) to break Apple and Google's control of every app that goes on a device.[93] This decentralization would then allow for more family-friendly and child-safe app stores to arise as competitors. Third-party app stores could become a viable option and could decide to be more like a toy store than a general store and curate and offer only kid-safe apps.[94] Parents could then choose such a family-friendly app provider and download it to their child's device rather than being forced to go through Apple and Google's built-in

default app stores. Because smartphone devices have been synonymous with their app stores, opening up the app store market could also indirectly help open up the smartphone market to other competitors who could introduce more family-friendly devices.

c. Amend State "Little FTC Acts":

A final approach is to use and amend existing state law. Most states already have deceptive trade practices laws. "Over forty states have state laws that mirror the FTC Act's protections, the so-called 'Little FTC Acts.'"[95] The wording of these laws typically copies the FTC Act, the Uniform Deceptive Trade Practices Act, or the Uniform Consumer Sales Practices Act. These "Little FTC Acts" allow the states, as with the federal government, to take action specifically to protect children. While "Little FTC Acts" often proceed from common law concepts, they usually allow causes of action that expand on historical fraud or misrepresentation actions. "They offer a range of potential remedies, including actual damages, enhanced damages, injunctive or declaratory relief, attorneys' fees, court costs, and rescission for unfair and deceptive practices committed in the conduct of trade or commerce."[96]

App stores market to and serve children. And certain apps, like social media platforms and others, market themselves to children. Arguably, these "Little FTC Acts" could already be applied to and leveraged against app stores and apps due to abusive marketing to children, since most laws apply to all "consumer transactions." These laws could be further strengthened by adding amendments that would make explicitly clear that these laws prohibit app stores and apps from abusively marketing their goods to children. The question of whether new legislative language is needed would vary from state to state given the specific wording of each state's statute. For example, to strengthen a state's consumer protection laws over this specific market sector and to motivate changes by app stores, or even give greater momentum to enforcement agencies, we suggest adding clarifying language to definitions in these "Little FTC Acts"; for example, adding to "consumer transaction" a note such as, "including by computer or digital device," or "including computer or mobile applications."[97]

IV. Conclusion

Lawmakers at both the federal and state level are coming to realize that the status quo, in which Big Tech companies are shielded from liability and granted *de facto* impunity to do whatever they please to America's kids, may fill the coffers of Silicon Valley, but it drains the lives of our kids and families. Their wealth comes at our children's expense. These same lawmakers have given Big Tech much latitude and the benefit of the doubt to correct their scandalous and predatory practices—and these companies have taken that slack and run with it, proving beyond a shadow of a doubt that they have no interest in correcting their behavior. It is time for action.

There are several measures, at both the federal and state level, that lawmakers can take to make devices and app stores safer for our children and require Big Tech companies to ensure their products are safe for children and simple for parents. There are also several measures that these companies could take voluntarily to demonstrate that they truly care about child safety or be made to care by public pressure from parents and other advocates. The Federal Trade Commission (FTC) and state attorneys general could also make many of these recommendations part of future settlement agreements. All of these measures would hinder the device and app store companies from dodging their own responsibility for child safety and dumping all the blame on the social media companies and adult websites. All of the above have proven their culpability and unwillingness to comply to basic standards of decency. We cannot allow the device and app store companies to avoid scrutiny because of the great attention recently given to these other bad actors. Restrictions and protections at the platform and site level are still certainly needed,[98] but this brief has sought to show that both state and federal policymakers and relevant enforcement entities (FTC and state AGs) must not neglect the harms at the device and app store-levels, especially since these devices and their app stores are the most common mechanisms by which children are accessing social

media platforms or adult websites. Parents need help to protect their children from the myriad dangers coming through these devices and their app stores. It is time to demand safer smartphones and app stores for America's children.

NATIONAL CENTER ON
SEXUAL EXPLOITATION

This brief is endorsed by the National Center for Sexual Exploitation (NCOSE) and Protect Young Eyes (PYE).

---

[1] Marc Novicoff, "A Simple Law Is Doing the Impossible. It's Making the Online Porn Industry Retreat," *Politico*, Aug 8, 2023, https://www.politico.com/news/magazine/2023/08/08/age-law-online-porn-00110148.

[2] Sapna Maheshwari, David McCabe, and Natasha Singer, "As Red States Curb Social Media, Did Montana Go Too Far?" *New York Times*, Oct 12, 2023, https://www.nytimes.com/2023/10/12/technology/red-states-montana-tiktok-ban.html.

[3] Chris Griswold, "Big Tech Is Exploiting Kids Online. Congress Has to Step In," *Newsweek*, Nov 6, 2023, https://www.newsweek.com/big-tech-exploiting-kids-online-congress-has-step-opinion-1840276.

[4] Michael Toscano, "Protecting Kids Online," American Compass, https://americancompass.org/rebuilding-american-capitalism/supportive-communities/protecting-kids-online/.

[5] Adam Candeub, Clare Morell, and Michael Toscano, "Protecting Kids Online: Legislative Summary," Institute for Family Studies, https://ifstudies.org/ifs-admin/resources/briefs/10-23-model-social-media-bill-summaryweb-2.pdf.

Smartphone Dilemma .pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

2021

The Smartphone Dilemma

Craig W. Cardillo

In pertinent part:

participate in the lottery and horse racing.[156] The minimum age to enter a casino in New York is eighteen; and twenty-one in New Jersey.[157] These regulations on the minimum gambling age are valid state actions due to the compelling interest of protecting minors.

In *Latour v. State*, the Louisiana Supreme Court upheld a law that raised the gambling age in Louisiana to twenty-one.[158] The court stated that the legislation was "substantially related to the protection of the general welfare of the state."[159] Based on this rationale, the court upheld the age increase as they believed it protected young adults and protected the general public health and welfare.[160]

States have seen the harmful impacts that gambling can have on minors and implemented laws to protect them. While there have not been many court cases challenging the minimum age of gambling, the same constitutional analysis applies. Like the other three public health issues, there is a compelling state interest to protect minors from gambling. Even if the courts give special weight to the parents' considerations, these types of laws are well within the states powers to regulate so long as they are narrowly tailored.

VI. Smartphones

Like the other four public health issues discussed above, smartphones are extremely popular in America. However, the popularity of something does not mean that it should be accessible to children of all ages. I posit that the negative health impact on minors provides a compelling state interest that would allow the states to regulate smartphones, even over parents' objections.

---

[156] *Id.*
[157] *Id.*
[158] Latour v. State, 778 So. 2d 557, 557 (La. 2001).
[159] *Id.*
[160] *Id.* at 564.

i. Smartphone Health Issues

The use of a smartphone has many health implications. These health issues should be a major concern to all parents of children under the age of eighteen. One of the worries regarding smartphones is the addictive nature of device. Studies show that 54% of teens stated that they spent too much time on their cell phones, while 60% of U.S college students consider themselves to have a cell phone addiction.[161] In a study conducted by Common Sense Media, teens averaged nine hours of screen time a day, with Snapchat and Instagram being the most popular sites.[162]

Much of this screen time may be the fault of social media giants such as Facebook, Snapchat and Instagram. "Likes" on these sites lead to a surge in dopamine, the "feel good" hormone.[163] According to a report from Harvard University, this stimulation is as rewarding as hitting a small jackpot for gamblers and leads to the potential for addiction.[164] The more screen time on these sites, means more money for the companies and they will continue to try and keep people's eyes on the screen.[165] A 60 Minutes interview discussed how Instagram takes advantage of minors' dopamine-driven desire for social validation.[166] For example, Instagram notification algorithms withhold "likes" on minors' photos and deliver them later in larger bursts.[167] This causes the mind to respond robustly to the sudden influx of "likes." Minors crave

---

[161] *Id.*
[162] Chrisanna Mink, *How Growing Screen Time is Impacting Teen's Mental Health*, (Sep. 22, 2019, 5:00 a.m.), https://www.modbee.com/living/health-fitness/article234323582.html.
[163] Trevor Haynes, *Dopamine, Smartphones and You*, (May 01, 2018), http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/.
[164] *Id.*
[165] *Id.*
[166] Anderson Cooper, *What is "Brain Hacking?" Tech Insiders on Why You Should Care*, (Apr. 9, 2017), https://www.cbsnews.com/news/brain-hacking-tech-insiders-60-minutes/.
[167] *Id.*

feelings like this and they keep checking their smartphones which in-turn leads to more screen time.[168]

This addiction has also led to arguments between parents and children regarding the minor's smartphone usage. Research has shown that 35% of parents and 32% of teens stated that they argue daily about the device use while 43% of parents and 38% of teens stated that they argued a few times a week.[169] This means that 78% of parents and 70% of teens believe that they argue over the minors use of their smartphone at least a few times a week.[170] This type of environment is not good for the family dynamic.

Recently, the American Academy of Pediatrics has issued guidelines limiting screen time for children of all ages.[171] The recommendation of the Academy pertained to all screen time and not just smartphones as the Academy recognized the impact screen time can have on minors.[172]

In addition to being addictive, social media creates the perfect environment for cyberbullying. Nearly 60% of teens reported some sort of cyberbullying with name calling and spreading of false rumors being the most common offense.[173] A vast majority of teens, 90%, believe that online harassment is a problem that affects people their age and 63% believe it is a major problem.[174] The likelihood of teens facing harassment varies based upon the amount of time the teen goes online. Strikingly, 45% of teens said they are constantly online and those

---

[168] *Id.*

[169] Michael B. Robb, *The New Normal: Parents, Teens, Screens, and Sleep in the United States*, https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-new-normal-parents-teens-screens-and-sleep-united-states.pdf, (lasted updated 2019).

[170] *Id.*

[171] AMERICAN ACADEMY OF PEDIATRICS, *Media and Children Communication Toolkit*, https://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/Pages/Media-and-Children.aspx, (last visited Oct. 20, 2020).

[172] *Id.*

[173] Monica Anderson, *A Majority of Teens Have Experience Some Form of Cyberbullying*, (Sep. 27, 2018), https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/.

[174] *Id.*

teens were more likely to be cyberbullied.[175] In addition to name calling and false rumors, 7% of teens have said that someone has shared an explicit picture of them without their consent.[176] On top of this, 20% of boys and 29% of girls have stated that they have received explicit pictures that they did not ask for.[177]

The time spent on their phones has led teens to be more anxious, depressed, and even suicidal.[178] A study conducted between 2010-2015 found that teens who reported spending more time on social media and their phones were more likely to report mental health issues than those who spent time on non-screen activities.[179] In fact, this study showed that depressive symptoms and suicide among adolescents all increased during the 2010s.[180] The study showed a clear pattern, linking screen activities with higher levels of depression systems and suicide outcomes than non-screen activities.[181] Surprisingly, this risk was seen after only two hours or more of electronic screen time.[182] Another study conducted in 2019 stated that there is a relationship between cell phone usage and adolescent's mental or physical health.[183] Roughly 40% of adolescents said they felt anxious if they left home without their cellphones and 56% said that they associated absence of cellphones with at least one of these three emotions: loneliness, being upset, or feeling anxious.[184]

---

[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] Jean M. Twenger, *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time*, (Nov. 14, 2017), https://journals.sagepub.com/doi/full/10.1177/2167702617723376.
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *See* Shoukat, *supra* note 3.
[184] Kari Paul, *This is What Happens When You Take Phones Away From Teenagers*, MARKETWATCH (Aug. 25, 2018, 10:22 p.m.), https://www.marketwatch.com/story/this-is-what-happens-when-you-take-phones-away-from-teenagers-2018-08-22.

Furthermore, there are also physical side effects from smartphone usage. Sleep duration and quality are disrupted from smartphone usage.[185] There is also mixed evidence, which requires further studies, on the impact of smartphones on physical activity and obesity. While some studies have found a correlation between increased smartphone usage and obesity, other studies have not.[186]

In addition to these health effects, there has been concern over smartphones and cancer. Cell phones emit radio frequency which can target radiation to the brain when the cell phone is held to the ear. Both the World Health Organization review panel and the American Academy of Pediatrics concluded this is a "possible" risk for cancer but more studies were needed.[187]

Lastly, motor vehicle accidents are the number one cause of death among adolescents.[188] Using a phone while driving has been shown to have a three to four fold increase in risk of crash or near crash.[189] Studies have shown that drivers aged sixteen to nineteen are most likely to die in distracted driving crashes.[190] Although this age group only accounts for 6% of total drivers, they have accounted for 10% of all drivers determined to be distracted at the time of crash and 11% of all drivers killed in crashes related to cell phone usage.[191] In addition to motor vehicle accidents, the American Academy of Pediatrics has also seen a surge in distracted pedestrian injuries from smartphone usage, which may now be responsible for 10% of pedestrian injuries.[192]

---

[185] Sara E. Domoff, *Excessive Use of Mobile Devices and Children's Physical Health*, (Apr. 16, 2019), https://onlinelibrary.wiley.com/doi/full/10.1002/hbe2.145.
[186] *See* Mink, *supra* note 162.
[187] *Id.*; Ruth. A. Etzel, *More Study Needed on Rick of Brain Tumors from Cell Phone Use,* (Oct. 2011), https://www.aappublications.org/content/32/10/28.
[188] M. Kit Delgado, *Adolescent Cellphone Use While Driving: An Overview of the Literature and Promising Future Directions for Prevention*, (June 16, 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5041591/.
[189] *Id.*
[190] *Id.*
[191] *Id.*
[192] Dr. William Raszka, *Heads Up: Cell Phone Use and Pedestrian Injury.*, (Mar. 25, 2016), https://www.aappublications.org/news/2016/03/25/Cell-Phone-Use-and-Pedestrian-Injury-pediatrics-0316.

While smartphones are still relatively new, the research to determine the impact on minors is steadily growing. In a new report, two psychology professors examined forty reports on the impact between social media use and both depression and anxiety among adolescents.[193] They concluded that right now the link is small and inconsistent.[194] While they do not argue that intensive use of smartphones does not matter, they do challenge the belief that smartphones are responsible for broad societal problems among minors.[195]

With that being said, those in Silicon Valley, have started to look at cell phones and their own adolescents differently.[196] Tim Cook, the CEO of Apple, stated that he would not let his nephew join social networks.[197] Bill Gates, the co-founder of Microsoft, banned cellphones for his children until they were teenagers and even then, his wife stated they wished they had waited longer.[198] Even the late Steve Jobs, the co-founder of Apple, would not let his young children near iPads.[199]

In 2019, Senators and Representatives reintroduced a bill, the *Children and Media Research Advancement Act* (CAMRA), that would commission research on children's technology use and outcomes including addiction, bullying, and depression.[200] While this bill has not yet made much movement within the House or Senate, there seems to be more elected officials who are beginning to recognize the dangers of smartphones.

---

[193] Nathaniel Popper, *Panicking About Taking Your Kids Smart Phone Away? New Research Says Don't,* NEW YORK TIMES (Jan. 1, 2020), https://www.nytimes.com/2020/01/17/technology/kids-smartphones-depression.html.
[194] *Id.*
[195] *Id.*
[196] Nellie Bowles, *A Dark Consensus About Screens and Kids Begins to Emerge in Silicon Valley*, NEW YORK TIMES (Oct. 26, 2018), https://www.nytimes.com/2018/10/26/style/phones-children-silicon-valley.html?action=click&module=RelatedLinks&pgtype=Article.
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] Ed Markey, *Children and Media Research Advancement Act* (CAMRA), https://www.markey.senate.gov/news/press-releases/senators-markey-sasse-blunt-schatz-bennet-and-collins-and-reps-raskin-and-budd-reintroduce-bipartisan-bicameral-legislation-to-study-impact-of-technology-and-media-on-children, (last visited July 6, 2020).

ii. Cell Phone Legislation

Recently, legislation has been introduced in states to limit and or ban smartphones from those under a certain age. In 2017, a Colorado parent, Timothy Farnum, led the charge for a ballot initiative that would ban the sale of smartphones for children under thirteen.[201] As written, the ban would require cellphone companies to ask the age of the primary user. [202] These companies could face fines if they sell phones to someone underage.[203] Unfortunately, they were unable to get enough signatures to be on the 2018 ballot.[204] Some opponents of the bill stated that the government should not be involved in telling a parent if their child should have a cell phone.[205]

In 2020, Vermont State Senator John Rodgers introduced Vermont Bill S.212 which would make it illegal for anyone under the age of twenty-one to use or possess a cellphone.[206] The bill outlines the dangers of cell phones to include cyberbullying and use while driving (which causes automobile accidents) among others.[207] Senator Rodgers himself stated, "I have no delusions that it's going to pass. I wouldn't probably vote for it myself."[208] His reasoning behind introducing this bill was that the legislature seemed intent on regulating gun use and based on the information,

---

[201] Alicia Stice, *Colorado Group Wants to Ban Sale of Smartphones for Kids Under 13*, USA TODAY (June 19, 2017), https://www.usatoday.com/story/tech/nation-now/2017/06/19/colorado-group-wants-ban-sale-cellphones-smartphones-kids-under-13/407898001/.
[202] *Id.*
[203] *Id.*
[204] Colorado Ballot, *Colorado Prohibit Sale of Smartphones to Persons Under Age 13 Initiative (2018)*, https://ballotpedia.org/Colorado_Prohibit_Sale_of_Smartphones_to_Persons_Under_Age_13_Initiative_(2018), (last visited July 5, 2020).
[205] Ashton & Price, *Proposed State Law Bans Use of Smart Phones for Children Under 13*, http://ashtonandprice.com/proposed-state-law-bans-use-smart-phones-children-13/, (last visited July 6, 2020).
[206] VERMONT GENERAL ASSEMBLY, *S.212*, https://legislature.vermont.gov/bill/status/2020/S.212, (last visited July 6, 2020).
[207] *Id.*
[208] Eric Blaisdell, *Bill Would Ban Cellphone Use for Those Under 21*, (Jan. 08, 2020), https://www.timesargus.com/news/local/bill-would-ban-cellphone-use-for-those-under-21/article_2e4064f1-892f-5a83-95a2-d8a4272942d9.html.

cell phones are more dangerous than a gun.[209] While Senator Rodgers may have used this bill for publicity, others took it more serious and debated the merits of such a ban.

In addition to attempting outright bans, schools have banned cell phones among students while in school. California recently passed legislation that allows schools to restrict or prohibit devices in class, although it is not required.[210] Studies have shown that students in schools where cell phones were banned performed better on exams.[211]

This is not an issue that is just affecting the United States. In July 2018, the French government was concerned over the use of cell phones among children which led them to pass a bill banning cell phones in school.[212] In 2019, Victoria, Australia banned cell phones in school as well.[213] Dr. Neil Selwyn, a professor at Monash University, stated that in a survey of 2,000 adults, 75% supported the school ban and about 33% supported an outright ban.[214]

While still a new technology, the debate will only continue to grow on whether there is such a thing as too much screen time for children. If research continues to support the negative impact on children, the support for bans on smartphones will likely continue to grow as well.

iii. Proposals

Although parents have a fundamental right to raise their children, this right can be infringed on by the state when there is a compelling state interest. Courts have found that health and safety are compelling interests for the state to intervene. While at first glance smartphone regulation. may seem outlandish, the impacts on minors suggests that at least some regulation is warranted.

---

[209] *Id.*

[210] Alyson Klein, *Schools Say No to Cellphones in Class. But Is It a Smart Move?*, (Sep. 6, 2019), https://www.edweek.org/ew/articles/2019/09/11/schools-say-no-to-cellphones-in-class.html.

[211] *Id.*

[212] *Id.*

[213] Henrietta Cook, *Mobile Phones to be Banned in State Primary and Secondary Schools*, https://www.theage.com.au/national/victoria/mobile-phones-to-be-banned-in-state-primary-and-secondary-schools-20190625-p5217a.html, (last visited July 3, 2020).

[214] *Id.*

Much like we have seen with smoking, alcohol, gambling, and pornography, the harms of smartphones to minors are significant and would rise to the level of a compelling interest. Moreover, as with distracted driving, minors can cause harm to others while on the smartphones and this legislation would be for the general public welfare.

As with many of the other public health issues, the state regulation on smartphones will infringe on the rights of the parents. In *Ginsberg*, the court acknowledged that while it is the parental right to raise a child, the state can also help with this obligation in order to protect children.[215] The damage that is caused by smartphones can be detrimental to a minor. Since smartphones are relatively new, more research may be needed to determine if this damage will be long lasting. However, steps can still be taken now in order to protect minors.

As some school districts have already done in America, outlawing smartphones in schools is a good first step. School is meant for learning and the more distractions that are in front of the students prevent or impede them from accomplishing this goal. As mentioned above, studies have already shown that banning cell phones in school has helped improve grades.[216]

The next step would be to determine what age is appropriate for minors to get smartphones. After looking at the current research, banning the sale of smartphones for those under eighteen seems to be warranted. While the world is becoming more connected with technology, it does not mean that we should allow harm to minors if it can be avoided.

States should pass a bill like the one that was introduced in Colorado in 2017.[217] This bill would ban the sale of smartphones if the primary user is below the age of eighteen. Retailers would be required to inquire who would be the primary user of the smartphone. Retailers will be

---

[215] *Ginsberg*, 390 U.S. at 639.
[216] Klein, *supra* note 210.
[217] *See* Stice, *supra* note 201.

fined if they do not follow the regulations. This type of regulation is similar to the one in *Ginsberg*, which banned the sale of adult magazines to minors, however, the Court stated that parents could still buy the magazines for their children.[218] These types of regulations help parents understand the risks associated with buying a smartphone for the minor and ensure that minors cannot go into the store to buy the smartphones on their own accord. As research continues to mount, if the harm to minors is more akin to alcohol and smoking, then states should further regulate smartphones and ban the possession of smartphones for all minors under the age of eighteen. Both of these actions by the state would be within their police powers to regulate smartphones for minors.

Minors would still be allowed to have cell phones that do not have access to the internet. This would allow them to call and text their parents, friends, and emergency numbers if needed. However, they would not be allowed to access the more damaging applications like Snapchat, Instagram, TikTok, etc.

VII. Conclusion

Smartphone bans should be among the other age-based regulations that protect children. While the smartphone ban will undoubtedly receive public backlash, the precedent is there for the state to protect minors from harmful conduct. States have already banned minors from smoking, drinking alcohol, gambling, and viewing pornography because they are detrimental to minors. Smartphones should be next.

---

[218] *Ginsberg*, 390 U.S. at 639.

Testimony HB1311.pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

Susan K. McComas
Legislative District 34B
Harford County

Deputy Minority Whip

Appropriations Committee
Subcommittees
Public Safety and Administration
Oversight Committee on Pensions

Joint Committees
Administrative, Executive, and Legislative Review
Legislative Ethics

Past President
Women Legislators of Maryland

Annapolis Office
The Maryland House of Delegates
6 Bladen Street, Room 411
Annapolis, Maryland 21401
410-841-3272 · 301-858-3272
800-492-7122 *Ext.* 3272
Fax 410-841-3202 · 301-858-3202
Susan.McComas@house.state.md.us

The Maryland House of Delegates
Annapolis, Maryland 21401

SUPPORT FOR HB1311
CRIMINAL LAW – OBSCENE MATERIAL – DEVICE FILTERS

HB1311 takes strides in proposing the protection of our minor children from exposure to obscene material on smartphones and tablets via the internet. After clearly defining the terms within, HB 1311 proposes that after January 1, 2025, phones and tablets manufactured thereafter, when activated in Maryland, automatically enable a filter capable of blocking "obscene material" as defined. This filter would prevent a user of the device from accessing material meeting the obscene definition. A copy of the Federal definition of obscenity is uploaded for your perusal. The filter would also enable adult users to deactivate the filter for the device or for specific content as the adult so choses.

HB1311 enables the Attorney General to bring civil actions against manufacturers of devices that do not comply with the bill as proposed. Parents and guardians of children would also be permitted to bring civil actions against manufacturers and others that violate the provisions set forth in HB1311. Finally, this bill makes it a criminal offense for any person other that the parents or guardians of a minor child to provide the passcode to remove the filter on a device in the possession of a minor.

Obscenity is not protected under the First Amendment rights to free speech, and violations of federal obscenity laws are criminal offenses. Federal law strictly prohibits the distribution of obscene materials to a minor under the age of 16 to include material distributed over the internet. The Child Exploitation and Obscenity Section of the U.S. Department of Justice is charged with the enforcement of the federal obscenity statutes. Although the distribution of obscene materials over the internet via smartphones and tablets blurs the traditional standards of jurisdiction, Maryland can make a stand to protect our youth by implementing the protections afforded and proposed by HB1311.

Please enter a Favorable Vote for HB1311.

Susan K. McComas

Utah Smartphones and Obsenity.pdf
Uploaded by: Darlyn McLaughlin
Position: FAV

UTAH POLITICS

This Utah lawmaker passed the porn age verification law. Now he's taking on smartphone filters for obscene material

A similar bill passed a few years ago, but hasn't gone into effect. Sen. Todd Weiler doesn't want to wait anymore

Published: Jan 23, 2024, 5:54 p.m. MST

Eliza Anderson, Deseret News

By Hanna Seariac
Hanna is a reporter for the Deseret News where she covers courts, crime, policy and faith.

The legislator behind Utah's law requiring pornography websites to verify their users are adults not children has introduced another piece of legislation aimed at protecting children from accessing obscene material on their phones or tablets.

Sen. Todd Weiler, R-Woods Cross, introduced a bill known as the Children's Device Protection Act, or SB104, which is aimed at requiring tablets or smartphones to automatically enable a filter blocking obscene content when used by a minor. Adult users and parents could disable the filter through a password.

"Let me just say that this bill is similar to a bill that Rep. (Susan) Pulsipher and Sen. (Wayne) Harper passed a few years ago. But that bill, that filtering device bill, said that it wouldn't go into effect unless four or five other states passed similar legislation, so Utah wasn't an outlier," Weiler said Tuesday in the Senate Judiciary, Law Enforcement and Criminal Justice Committee meeting. "Well, in the years between, since then, we've made ourselves an outlier when it comes to social media and porn websites."

"And so, it begs the question: Why are we waiting for other states on this one?" Weiler continued.

Back in 2021, Rep. Pulsipher, R-South Jordan, and Sen. Harper, R-Taylorsville, passed HB72 which was set to require "a tablet or a smartphone (a device) sold in the state ... to, when activated in the state, automatically enable a filter capable of blocking material that is harmful to minors." The bill was set to go into effect until at least five states passed similar legislation, which hasn't happened yet.

Alabama, Pennsylvania, Georgia and Tennessee all attempted to pass a similar law in years past, but efforts failed. Both Florida and South Carolina are considering device filter bills for minors as well during the 2024 legislative session.

"The idea is to provide minors with the protection and opportunity that they deserve as children to prevent them from developing an addiction to pornography before they're even an adult and allow them time to develop good online habits while they're still young, which will positively impact their future," Weiler said. "It also requires parents to be cognizant of their children's online presence."

If passed, the bill would allow "private civil actions by parents and guardians of minors against manufacturers and others who violate provisions of this bill; and makes it a

criminal offense for any person, with the exception of a parent or guardian, to enable the removal of the filter on a device in the possession of a minor."

RELATED

What Billie Eilish has to do with Utah's porn law

Utah County resident Katheryn Snyder, the development and fundraising manager for the National Center on Sexual Exploitation, spoke in favor of the bill during the committee meeting. "In 2016, the Utah State Senate adopted a resolution recognizing pornography as a public health hazard," Snyder said. "Big Tech is fully capable of making this change."

Snyder also said, "Just in June of 2023, Apple activated filters to automatically blur explicit content on smartphones and tablets for users under the age of 12. And we know that Apple and Google have the estimated age of each user per the device, per the ID birthdate. That's been given, so there's no reason why they shouldn't protect our children."

One concern raised during the meeting by Dave Davis on behalf of the Utah Retail Merchants Association was the obligation of retailers. "We're against pornography getting into the hands of children," Davis said, explaining that he wanted clarity on if or how retailers would be held accountable.

Jodi Hart, representing AT&T, and Justin Stewart, with Verizon, raised a similar concern. "We're not necessarily opposed to the bill," Hart said. "But ... the liability for our stores, for our retail stores, the penalty is quite high, but we're not the manufacturers of these devices."

Benjamin Bull, general counsel for the National Center on Sexual Exploitation, said that he was one of the original drafters of this legislation years ago and that "there is zero liability for retailers. Instead, the law is directed toward requiring manufacturers to enable the filter.

"We wanted to draft something that we knew would make a difference, but we also were confident that it would pass constitutional muster in federal court if challenged," Bull said about the development of the past law. "This is that law."

Dylan Hoffman, TechNet executive director for California and the Southwest, said his organization is a bipartisan network of tech companies.

"Our companies and our organization are very strongly in support of trying to protect kids from harmful content, including pornographic material. We fully agree with the intent of this author," Hoffman said. "However, we must respectfully oppose this bill on the basis that we don't believe that this is technically feasible to comply with."

Hoffman pointed toward content filtering and blocking solutions that can be purchased or found for free that are already on the market. He said that these could be used to prevent children from seeing obscene materials and "blocking and filtering capabilities like the bill calls for would impose immense liability."

Chris McKenna, founder of Protect Young Eyes, spoke in favor of bill, saying he worked on the technical side of it while Bull had worked on the constitutional aspects of it. "What's so helpful about this bill is it's surgical and technically elegant."

McKenna said that the bill is "intentionally simple" and doesn't interact with a variety of areas online — it deals with "the browsers where that early accidental exposure can be so damaging."

"We agree that we don't want the manufacturers to have to sell different phones to different states. That's where software, that's where technically this takes over," McKenna said. "The bill cares about activation, not where it was sold."

"Just like we don't sell separate phones to or manufacturers don't sell separate phones to Arizona because they don't observe daylight savings time ... the software knows," McKenna explained. "And the activation sequence knows where you are because you have to connect to WiFi."

After hearing the public testimony, Weiler said he wanted to talk to some of the stakeholders about the penalties associated with the bill and also needs to clarify the text to explain that retailers would not be held liable.

"In a future meeting, I'll bring back a substitute bill that I hope we could have a little bit more consensus on," Weiler said. "I'm absolutely dedicated to the cause, but I don't want to pass a bill out of the committee that may need a little bit more work."

RELATED

Required pornography filters on cellphones? A good step in the right direction

so helpful about this bill is it's surgical and technically elegant."

McKenna said that the bill is "intentionally simple" and doesn't interact with a variety of areas online — it deals with "the browsers where that early accidental exposure can be so damaging."

"We agree that we don't want the manufacturers to have to sell different phones to different states. That's where software, that's where technically this takes over," McKenna said. "The bill cares about activation, not where it was sold."

"Just like we don't sell separate phones to or manufacturers don't sell separate phones to Arizona because they don't observe daylight savings time ... the software knows," McKenna explained. "And the activation sequence knows where you are because you have to connect to WiFi."

After hearing the public testimony, Weiler said he wanted to talk to some of the stakeholders about the penalties associated with the bill and also needs to clarify the text to explain that retailers would not be held liable.

"In a future meeting, I'll bring back a substitute bill that I hope we could have a little bit more consensus on," Weiler said. "I'm absolutely dedicated to the cause, but I don't want to pass a bill out of the committee that may need a little bit more work."

RELATED

Required pornography filters on cellphones? A good step in the right direction

DeseretNews.

Opinion

Opinion: This bill would make protecting children from obscene material the standard, not an afterthought

Todd Weiler

February 1, 2024 · 2 min read

SB104, under consideration in the Utah Legislature, would require manufacturers to turn on existing filters that block obscene material when a minor activates a device. | Adobe.com

Technology is an important part of daily life. According to 2023 Pew Research, 95% of teens have smartphones and 65% have tablets. "Smart" devices can solve infinitely complex equations, measure sleep quality and

It's a well-established fact that pornography harms children. A meta-analysis of 37 studies found that exposure to violent or rape pornography increased a child's odds of experiencing sexual exploitation by nearly three times. Research shows that children are more susceptible than adults to addictions and developmental effects on the brain.

What if a simple software update could prevent a child from being exposed to traumatizing, highly addictive and obscene material? What if a filter is already installed on a device but is turned off?

As adults, we want to make things as safe as possible for children. That's why medicine bottles are so hard to open. We don't purchase cars with seatbelts hidden in the trunk, hoping the owner figures out how to install them. We don't allow minors to buy cigarettes because, like obscenity, we've recognized that tobacco is harmful.

SB104 simply requires manufacturers to turn on existing filters that block obscene material when a minor activates a device. It defaults the filter to "on" instead of "off" for children. Utah has a moral obligation to protect children from this harm.

Related

- Opinion: Keeping kids safe online is important, but Utah policymakers are going too far

Some say it's not feasible, but the technology is already there. Utah has always put families and children first and has never let precedence get in the way. By mandating safeguard capabilities from the get-go, we make protecting children the standard, not an afterthought.

Others might object to the bill because "protecting kids is a parent's responsibility." And I wholeheartedly agree. We're not asking Apple and Google to do the job of Utah parents. We're asking them to make it less difficult for parents to do so.

It's not a silver bullet. It doesn't prevent all digital harm. Instead, it's surgical, technical and simple. It doesn't impact retailers, cellular network providers, film, television or streaming services.

SB104, the "Children's Device Protection Act," is responsible, careful, narrow legislation. If enacted, it can prevent early, accidental exposure to potentially life-altering and obscene content for children. Utah has never

HB-1311- testimony.pdf
Uploaded by: Mary Modderman
Position: FAV

Mary Joan Modderman, OTR/L
509 Schuyler Road
Silver Spring, MD 20910
Email: Mary.OT@outlook.com
Cell: 301-412-6435
03/05/2024

HB 1311 -Del. Susan McComas (R). pdf – FAVORABLE
regarding default filtering of obscenity on internet- FAVORABLE

Dear Representatives, I am speaking today to support this bill. Del McComas has written an excellent bill to attempt to slow down and possibly halt the access of pornography on the phones of children.

I am a Pediatric Occupational Therapist who has worked with children in schools – both public and private settings for 31 years. I have seen firsthand how use of cell phones have affected children for good and for bad. The cell phone has affected the social well being and emotional development of many children throughout the States and throughout the world.

The National Center on Sexual Exploitation has done extensive research on the impact on the negative impacts of pornography consumption which often includes, incest, racism, and extreme violence themes.

The Children's Device Protection Bill mandates that smartphones and tablets automatically enable existing filters for all minors and allows for civil action if manufacturers fail to comply.

Virtually all devices have filters, but they are "OFF" when the device is activated. As a result, children are vulnerable to unwanted or damaging exposure to hardcore pornography.

Pornography harms the brain, particularly for those still neurologically developing, and fuels addiction. This material can ruin lives, and children are at most risk. This evidence should inform state telecommunications policy.

Smart devices already have filtering capabilities and parental control software available on devices, but they are overly complicated for parents and guardians to navigate. Through the status quo of defaulting filtering technology to "OFF," devices leave the most vulnerable in society particularly at-risk to online harms, such as children without tech-savvy, highly involved, caregivers.

I am representing the Maryland Coalition Against Pornography to ask that you vote FOR this bill to protect our children and their families.

Thank you for your favorable consideration of this bill.

HB1311 Peggy Cairns FAV.pdf
Uploaded by: Peggy Cairns
Position: FAV

Maryland Coalition Against Pornography, Inc.

P.O. Box 2868
Silver Spring, MD 20915-2868
mcapinc@mcap1.com
www.mcap1.com
TOGETHER WE CARE

(301) 439-8475

March 5, 2024

Chairman C.T. Wilson, House Economic Matters Committee
Maryland House of Delegates

In support of HB 1311

MCAP appreciates this bill which seeks to solve a huge problem facing families today that is beyond solving by parents alone - the dangers to the safety of children presented by unfiltered internet-connected devices.

The approach taken by this bill offers a technically simple, elegant solution: turn **on** filtering by default.

To grasp the problem, I recommend that you watch a **free** 2020 documentary video entitled CHILDHOOD 2.0. Here's a sample of disturbing trends and statistics:

53% of American children get a cell phone by age **11**. They spend many hours daily on these devices which are worse, addictively, than slot machines. 27% of all unfiltered Internet content is explicit or pornographic, and nearly 50% of children have been exposed to it by age **8**. In 2019, porn sites received more Internet traffic than Amazon, Twitter and Netflix combined. Social media apps are saturated with explicit material that can be shared via back door methods like chats.

In 2021 alone, the National Center for Missing and Exploited Children received nearly 85 **million** images, videos, and other files related to child sexual abuse and exploitation – and those are only what were **reported**. Much of today's porn contains physical and verbal aggression and violence.

Regarding smart phones and tablets - technology is best when it's easy and intuitive to use. This is NOT the case with filtering technology today. Families need help.
We parents know that manufacturers **can** turn on the filtering. Government regulates safety for other materials harmful to minors, like tobacco and alcohol. We don't put those potentially dangerous products freely in the hands of minors? No. Why should internet connectivity for minors be so **un**regulated?

We urge a favorable report on HB 1311.

Respectfully submitted,
Peggy Cairns
Education Chairperson
Maryland Coalition Against Pornography

Tibbals_ SUPPORT HB 1311_ Criminal Law - Obscene
Uploaded by: Trudy Tibbals
Position: FAV

HB 1311: Criminal Law - Obscene Material - Device Filters: Please SUPPORT this bill!!

Dear Economic Matters Committee Chair Wilson, Vice Chair Crosby and all other esteemed Committee Members:

We all know how damaging pornographic and obscene material is for our minor children. Actually, studies have shown that the developing brain is not fully mature until age 25, so obscene material is damaging to young people up until their mid-20s. There are not a lot of studies out there advocating for pornographic and obscene materials to be distributed to minors or young adults because it is beneficial. At least not that I've ever seen, and I doubt that any of you have run across that either.

I am including in this written testimony a copy of my previous written testimony on Senate Bill 355: Display of Obscene Material to Minors. It will demonstrate why we have to be vigilant in trying to keep pornographic and obscene material away from our minor children. This bill will require all manufacturers of "devices" to have a "filter" in place to prevent obscene material to be viewed by minors, and will allow criminal and civil charges to be filed due to civil and criminal liability of the manufacturer, if the manufacturer does NOT have a filter in place on all "devices" upon activation. The synopsis of the bill is: "...Requiring, beginning January 1, 2025, all devices activated in the State to enable a certain filter to prevent minors from accessing obscene material; prohibiting a certain person from deactivating the filter; providing that a manufacturer of a device and certain persons are subject to civil and criminal liability for certain conduct related to device filters; authorizing the Attorney General to take certain actions against persons who violate the Act; authorizing parents or legal guardians of minors who access obscene material to file a private cause of action against a certain manufacturer.."

Thank you for your courtesy and cooperation in SUPPORTING this bill to make certain that obscene material is not going to be able to be viewed by our minor children and, if it is, there are penalties for not having the required "filters" in place as required by this bill.

Trudy Tibbals
A Very Concerned Mother and maryland resident

P.S. This is a copy of my written testimony on SB 355:

Senate Bill 355: Criminal Law - Display of Obscene Material to Minors - Prohibition: Please support this bill!!

Dear Chair Smith & Vice Chair Waldstreicher and all other esteemed Committee Members:

Regardless of your political affiliation, I think we can all agree that pornographic, obscene, inappropriate material, whatever term you want to use, is very damaging to minor children! Here are a few objective resources and their citations.

"Pornographic content can harm children. Exposure to pornography at a young age may lead to poor mental health, sexism and objectification, sexual violence, and other negative outcomes. Among other risks, when children view pornography that portrays abusive and misogynistic acts, they may come to view such behaviour as normal and acceptable."
https://www.unicef.org/harmful-content-online#:~:text=Pornographic%20content%20can%20harm%20children&text=Exposure%20to%20pornography%20at%20a,violence%2C%20and%20other%20negative%20outcomes.

"Consumption of pornography is associated with many negative emotional, psychological, and physical health outcomes. These include increased rates of depression, anxiety, acting out and violent behavior, younger age of sexual debut, sexual promiscuity, increased risk of teen pregnancy, and a distorted view of relationships between men and women. For adults, pornography results in an increased likelihood of divorce which is also harmful to children. The American College of Pediatricians urges healthcare professionals to communicate the risks of pornography use to patients and their families and to offer resources both to protect children from viewing pornography and to treat individuals suffering from its negative effects…

Sexual predators have purposefully exposed young children to pornography for the purpose of grooming the children for sexual exploitation.[14] Pornography exposure at these young ages often results in anxiety for the child.[15] Children also report feelings of disgust, shock, embarrassment, anger, fear, and sadness after viewing pornography.[16] These children can suffer all of the symptoms of anxiety and depression. They may become obsessed with acting out adult sexual acts that they have seen, and this can be very disruptive and disturbing to the child's peers who

witness or are victimized by this behavior. Children under twelve years old who have viewed pornography are statistically more likely to sexually assault their peers.[17] In sum, children exposed to pornographic material are at risk for a broad range of maladaptive behaviors and psychopathology…

There is evidence that society's acceptance of pornography creates unique problems for women. The use of pornography can result in violent and sexually aggressive attitudes towards women. Men who consume pornography are more likely to adopt rape myth ideology, which is that women cause rape or actually enjoy rape or sexual assault…

Pornography use by adolescents and young adults often leads to a distorted view of sexuality and its role in fostering healthy personal relationships. These distortions include the overestimation of the prevalence of sexual activity in the community, the belief that sexual promiscuity is normal, and the belief that sexual abstinence is unhealthy.[34] These perspectives are likely to make it more difficult for young people to form lasting, meaningful relationships with the opposite sex, which will ultimately result in more anxiety, depression, and overall life dissatisfaction…

Children suffer many negative effects due to modern society's exposure to and acceptance of pornography. These negative effects include mental disturbance and unrest for the young school age child, including acting out and violent behavior. Because of its harmfulness to children, pornography must never be used as a tool to teach children human sexuality. For older adolescents and young adults, pornography teaches a false narrative regarding human sexuality and how men and women form healthy sexual relationships. This makes it more difficult for young men and women to form authentic, stable relationships. For parents, pornography is divisive resulting in a decreased quality of marriage and increasing the likelihood of divorce and separation which has been well documented to be harmful to children…"
https://acpeds.org/position-statements/the-impact-of-pornography-on-children

According to an article from The Bark Team date January 30, 2023:

"Here are just a few of the effects porn has on young brains:

- **Porn alters the structure and development of immature brains.** Studies show that porn can damage a developing prefrontal cortex. The area of your brain is critical for decision-making and impulse control—when damaged, children are more likely to act impulsive and make rash decisions. Porn can also damage the dopamine reward system, making it more difficult to find excitement or fulfillment in healthy relationships.
- **Viewing porn skews reality thanks to mirror neurons.** Dr. Sharon Cooper, a forensic pediatrician and faculty member at the University of North Carolina School of Medicine, argues that children are more vulnerable to pornographic images than adults because of mirror neurons in the brain. Mirror neurons play an important role in how children learn and convince people that they are actually experiencing what they see. Because these observed encounters seem so real to children, they are likely to believe this is how sex and relationships work in the real world—when that's often far from the truth.
- **Mainstream porn normalizes and reinforces sexist ideas and harmful gender roles**. Experts say that by age 10, gender stereotypes are established in the minds of children. Considering the average age kids are exposed to porn is between 9-11 years old, much of what they see can be cemented into their long-lasting ideas on gender roles. Unfortunately, these images aren't usually positive. A study of adolescent porn use concluded that the major messages presented by porn are male domination, hypermasculinity and making male sexual pleasure the top priority. These stereotypes, when pushed to the extreme, as they often are in porn, include men being dominating, unemotional and controlling and women being submissive, emotional and weak. When acted upon, these gender stereotypes can lead to an increase in violent and risky behavior for boys and depression and exposure to violence for girls.

The Dangers of Porn

The effects of porn on the brain can lead to real dangers and damages in the present and long term. Surveys show that the earlier children are exposed to porn, the more likely they will regularly view it and experience more of its effects and dangers.

Here are a few of the potential dangers that come from early exposure to porn:

- **Porn can keep people from forming and maintaining healthy relationships.** Because porn skews children's view of what a normal relationship, sexually and otherwise, looks like, they are often bound to expect things that aren't reasonable or healthy from their partner. When these expectations aren't met or enforced without consent, one or both sides of the relationship will fail.

Sexual violence is perpetuated by porn. A review of mainstream porn has shown that physical aggression occurred in 88.2% of scenes and verbal aggression in 48.7%. Men committed 70.3% of all aggressive acts and 94.4% of aggression was directed toward women. This repetitive reinforcement of gender stereotypes, violence and a male-centered narrative in pornography can lead to an increase in sexual violence toward women in the future.

- **Brains that have been rewired by viewing porn can lead to poor decision-making.** In relationships and beyond, desensitization to high dopamine levels can make even the highest-best moments a little less exciting. Plus, increased impulsivity means that when important decisions are to be made, people are more likely to jump to conclusions than make an informed decision."

  https://www.bark.us/blog/porn-dangers-damages/

I could have listed many more citations, but I felt like this was certainly enough for all of you to get the idea of how dangerous obscene pornographic, inappropriate material is for minor children. In my research, I have not seen any website or other resource where there were positive outcomes from minor children being exposed to pornographic material.

Therefore, I implore you to **SUPPORT** this bill and keep this pornographic material away from our children. Their futures depend on you doing so.

Thank you for your courtesy and cooperation.

[MD] HB 1311 device filters_TechNet_pdf.pdf
Uploaded by: margaret durkin
Position: UNF

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622
www.technet.org | @TechNetMidAtla1

March 1, 2024

The Honorable C.T. Wilson
Chair
House Economic Matters Committee
Maryland House of Delegates
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

RE: HB 1311 (McComas) - Criminal Law - Obscene Material - Device Filters.

Dear Chair Wilson and Members of the Committee,

On behalf of TechNet, I'm writing to offer comments on HB 1311 related to device filters.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.2 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, and Washington, D.C.

While the intent of HB 1311 is laudable, we are concerned with the operational challenges this bill requires, as well as the subjective nature of terms within the legislation.

Currently, there are many paid and free content filtering and blocking solutions available to the public that enable consumers to protect their families from illegal or inappropriate content. These solutions are widely available as both integrated and independent solutions for a wide range of technologies. Completely reliable identification, blocking, and filtering capabilities like the bill calls for, however, are not technologically feasible, and therefore compliance with HB 1311 would be difficult. For example, an inevitable but unintended consequence of HB 1311 would be the inadvertent blocking of legal, non-obscene content, which would limit Maryland's citizens access to legitimate information.

Additionally, the legislation would place device manufacturers in the impossible

role of deciding what content is obscene and whether or not it should be restricted, especially given the subjective nature of the definition of "obscene". If a private company inadvertently blocked lawful content, the company would face public backlash from website owners and users, including potential civil liability and monetary damages. The courts, working closely with law enforcement, are the only lawful authority in the position to make these determinations.

The bill also calls for "Reasonable Age Verification". Age-verification is a complex challenge for our industry to address and requires consideration of how to properly balance the interests of privacy and security. Stringent age-verification requirements would require the collection of more personal information such as birthdates, addresses, and government IDs, which conflicts with data minimization principles. Efforts are ongoing to develop more privacy protective ways to verify age online. But until there are industry-wide tools available, age-verification will continue to have tradeoffs and be difficult to implement in practice. Unfortunately, no system is infallible.

The bill contains a private right of action, which encourages an abundance of frivolous lawsuits and costly litigation. Companies should be focusing their resources on supporting digital citizenship and online safety education, as opposed to focusing time and resources on expensive and time-consuming litigation.

Finally, products are not manufactured in a manner that tailors them to consumers living in a specific state. Tablets and smart phones are the result of years-long design efforts, incredibly complicated international supply chains, mass production, and global shipping to consumers. Manufacturers are unable to design operating systems on a state-by-state basis.

Our members work with law enforcement, educational institutions, government agencies, and a wide range of organizations to provide consumer education to help protect children and adults from illegal and distasteful content on the internet. An educated consumer armed with technology is always the best protection against unwanted online interactions. For the above state reasons, TechNet is opposed to this bill. Thank you for your time and we look forward to continuing these discussions with you.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

Testimony in opposition to HB1311.pdf
Uploaded by: Richard KAP Kaplowitz
Position: UNF

HB1311_RichardKaplowitz_UNF

3/05/2024

Richard Keith Kaplowitz
Frederick, MD 21703

TESTIMONY ON HB#/1311 - POSITION: UNFAVORABLE

Criminal Law - Obscene Material - Device Filters

TO: Chair Wilson, Vice Chair Crosby and members of the Economic Matters Committee
FROM: Richard Keith Kaplowitz

My name is Richard Keith Kaplowitz. I am a resident of District 3. I am submitting this testimony against HB#/1311, Criminal Law - Obscene Material - Device Filters

This bill is another that seems to be supporting the conservative's political agenda for control of the free expression of ideas and words that they object to. Because I am offended by something then you have no right to it, my opinion is the only one that counts when it comes to what your minors should be permitted to read or view. What gives them the right to censor for all, who makes the determination of what is or is not obscene?

There are many excellent reasons to oppose this bill. The EveryLibrary Institute states "The effort to criminalize bona fide professions is happening alongside a movement to redefine what content of books, ebooks, and materials is considered obscene. The concept of what is appropriate or inappropriate is hotly debated at board meetings, on social media, and in the public square. **The concept of "appropriateness" is often defined by the offended party rather than contemporary community standards**. (Emphasis added) The "relevance" of a book to a topic or population should drive library collection development practices and material retention policies." [1]

This bill is unnecessary and only serves to respond to a political agenda in which a small group wants to control the majority and suppress anything that troubles them for everyone else.

I respectfully urge this committee to return an unfavorable report on HB#/1311.

[1] https://assets.nationbuilder.com/votelibraries/pages/5762/attachments/original/1674613743/Opposing_Changes_to_State_Obscenity_Laws_2023_-_EveryLibrary_Institute_PB2.pdf?167461374398/Opposing_Changes_to_State_Obscenity_Laws_2023_-_EveryLibrary_Institute_PB.pdf?1674485398