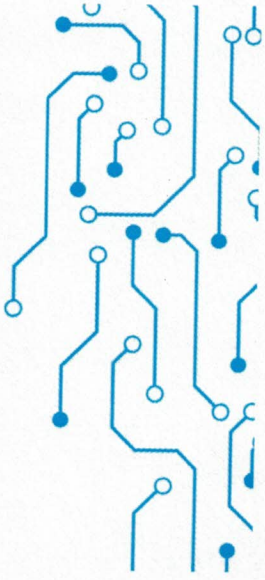
Making Smartphones and App Stores Safe for Kids: Federal, State, and Industry Measures



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.