Making Smartphones and App Stores Safer for Kids

What States Can Do

Clare Morell, Ethics and Public Policy Center
Michael Toscano, Institute for Family Studies

ETHICS AND PUBLIC POLICY CENTER
Shaping Policy, Renewing Culture.

IFS
Institute for Family Studies

Background

Needed attention has been given to the harms of social media and online pornography for children, galvanizing lawmakers in several states to enact laws to require age verification on pornography sites (blocking individuals under the age of 18 from gaining access) and parental consent for minors to open social-media accounts (i.e., form online contracts). These measures are critical, but they only address one level of the problem: the website or platform. It is now necessary to direct attention toward the devices that serve as a child's main portal to the Internet and social-media platforms along with many other apps.

Objectives

Implement policies to regulate smartphones and tablets to make them safer for kids and ensure they provide an age-appropriate experience of apps and the Internet. The regulatory goals are: (1) design safer devices and app stores and (2) correct the misaligned incentives that foster these conditions by opening companies up to more litigation. We advise states to require by legislation the following for device manufacturers and app stores:

1. Require manufacturers to verify user age on the device

Age verification at the device level is the best technical anchor for any subsequent device-level protections. In setting up a new smartphone or tablet, users already are required to establish an Apple or Google ID and enter their birth date. Age verification could be added to the existing setup process. No method of age verification is impervious to deception; nevertheless, confirming the ages of users by offering them several reasonable age-verification methods should align the vast majority of minors with age-appropriate products. These could include the upload or scan of a government ID, Apple credit card process, in-store verification, or other commercially reasonable methods. Some, such as Meta, have argued for age verification on the device level to replace site-level verification. But device-level age verification functions better as a complement rather than an alternative, because the very same sites that device-level verification may block can be easily accessed on any Web browser. The two levels should be integrated to offer a more seamless user experience and reduce the potential burden on adult speech as a First Amendment concern. For device-level verification to be used to satisfy website and platform verification requirements, 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 on the device. Apple has already developed the technology to securely transmit anonymous age information through its 'Verify with Wallet' feature.

2. Automatically enable family-friendly device defaults for minor users (especially filters to block obscenity)

The second policy objective is to require companies to automatically enable family- and child-friendly defaults on the device based on the age-verification process. If,

however, age verification is not obligatory, lawmakers could still require manufacturers to automatically enable certain age-appropriate settings on the device based on the age of the user, determined during the device activation process. We would recommend the following automatic settings:

A. Device filter to block obscenity

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 devices (smartphones and tablets) manufactured after a certain date, unless age verification proving the user is over the age of 18 has been completed. Such a bill could apply only to smartphones and tablets activated in the state on, for example, January 1 of the year following the bill's passage; or, taking a broader approach, a bill could require manufacturers to include in their next operating system update an age-verification process that would automatically enable the device filter for users not over the threshold of 18 years old. Even simpler, a default filter to block obscenity could be required for minors' devices, not based on required age verification but the age determined through the devices' existing setup processes. We recommend the "Children's Device Protection Bill" composed by the organizations Protect Young Eyes and the National Center on Sexual Exploitation, which uses this approach.

B. Parental notification and consent 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 device users under 18.

C. Content restrictions automatically set to the appropriate age of the user

Apple and Google have "Content Restrictions" settings already available that a parent can select to set which media, according to age appropriateness, should be accessible on the device. A parent can decide that only apps rated 4+, 9+, 12+, or 17+ be made available. Depending on the age of the user determined by one of the two processes recommended above, the device should automatically block apps with ratings that are not age aligned. The same process should filter various movies and TV shows. Music, podcasts, and books should all be defaulted to "Clean," unless user age directs otherwise. Apple already offers a one-step activation of a suite of safety settings based on a child's age. These settings, however, are inactive by default and buried under layers of menus.

3. Open up litigation by amending statues for deceptive or unfair trade practices ("Little FTC Acts")

Many apps that app stores advertise as safe for children are in reality harmful and exploitative. Content descriptors and ratings, furthermore, are often inaccurate and concealed, limiting the power of parents to make informed decisions about which apps are truly safe for their children. Most states already have laws dealin with deceptive trade practices. 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 states to take actions to protect children. App stores and innumerable apps, such as social-media platforms and others, market themselves to children. Arguably, these "Little FTC Acts" as written could be leveraged against app stores and apps due to abusive marketing to children, since most laws apply to all "consumer transactions." These laws could be strengthened by amending them to make *explicit* that they prohibit app stores and apps from abusively marketing to kids. Whether new legislative language is needed may vary from state to state depending on the wording of each state's statute. If needed to strengthen a state's consumer protection laws over this specific market sector, we suggest adding clarifying language to definitions for "consumer transaction," such as "including by computer or digital device" or "including computer or mobile applications." These would reinforce the state's powers of enforcement to make apps and app stores safer for kids.