Memorandum in Support of Legislation Requiring Default Filters for Internet Capable Devices

Background

A. What this legislation proposes:

The proposed legislation seeks to fulfill the Government's compelling interest in protecting children from exposure to harmful material online while not overburdening Free Speech. This is accomplished by requiring manufacturers of Internet capable devices, smart phones and tablets, to install and activate technology that enables parents to make filtering decisions for their children. This legislation recognizes the serious harm that comes to children from online pornography exposure and allows the government to encourage the use of filters and empower parents to determine what Internet material is appropriate for their children to access. *Ashcroft v. ACLU*, 542 U.S. 656, 670 (2004). Without this legislation it is not possible for parents to effectively protect their children from the massive amounts of harmful material inundating them online. This is because both smart phones and tablets are capable of connecting to the Internet in various ways, each with their own set of filtering limitations. By placing Internet filtering requirements at the manufacturer level, the devices themselves will be capable of filtering harmful content as they move in and out of different Internet networks.

Under this legislation, manufacturers of smart phones and tablets are required to install filtering software capable of filtering material that is harmful to minors and enable these filters by default when the device is activated. Material that is harmful to minors is defined as any sexually explicit picture, video, image, graphic image file, visual representation, or other sexually explicit material that can be viewed that:

(i) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest of minors;

(ii) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act, sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post pubescent female breast; and

(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.[1]

To be effective at protecting minors while being unrestrictive on adults, filtering software must be installed and active on the device at the time it is manufactured and be incapable of being tampered with by a minor or changed without the consent of their parent or legal guardian. The software must be capable of filtering both wireless and mobile internet connections. By placing the software on the device, itself, instead of the network, the filter will be able to protect minors online wherever the device is used instead of only on the filtered Internet network.

Each device manufactured will establish a passcode during device activation allowing the filter to be adjusted or removed by a parent or legal guardian. This gives parents the final say on what their children may access online. Adult users will create a passcode that enables them to adjust or remove the filters from their device(s). Thus, this legislation does not restrict adult access to speech they are entitled to under the First Amendment, does not restrict adults to only online content that is suitable for children, and does not place limits or restrictions on speech from the source.

B. *Previous legislative efforts and Supreme Court decisions show that filters are the most effective and the least restrictive means to protect minors online*.

Previous legislative efforts to protect minors from harmful material online have faced Constitutional challenges. Most notably, the Child Online Protection Act (COPA), which prohibited any person from knowingly posting, for commercial purposes, content on the World Wide Web that included material that is harmful to minors, was rejected by the Supreme Court because it was not the most effective and least restrictive way to protect minors from harmful online content. *Ashcroft*, 542 U.S. at 673. In its decision, the Supreme Court in *Ashcroft v. ACLU* held that a more effective and less restrictive solution was the use of Internet filters because they "impose selective restrictions on speech at the receiving end, not universal restrictions at the source." *Id.* at 667.

The Court concluded that through the use of filters, adults who seek to protect minors are able to do so while adults without children, or adults who share a device with a minor, may access unfiltered speech by turning the filter off on their own device or the device shared with a minor. *Id*. Additionally, filters can be enabled to prevent minors from seeing pornography posted online from any part of the world, not just the United States, and can apply to all Internet communications not just web pages. *Id*. It was also noted by the Supreme Court that filters do not label certain categories of speech as illegal and therefore do not chill free speech. *Id.* at 667.

[1] This definition is drawn from the harmful to minors statute upheld in *Ginsberg v. N.Y.*, 390 U.S. 629 (1968) and the obscenity test established in *Miller v. California*, 413 U.S. 15 (1973).

Argument:

I. Requiring manufacturers to install active filtering software on each device is necessary because the government has a compelling interest in protecting children from harmful online material and the multitude of Internet sources and ever-changing technology make it impossible for parents to manage the dangers alone.

The Supreme Court has recognized that the State may restrict minors' access to sexually explicit material and that material that is suitable for adults is not necessarily suitable for children. *Ginsberg v. State of N.Y.,* 390 U.S. 629, 636-38 (1968). The Court has also found that the State has a compelling interest in protecting minors from speech that is harmful to them, such as obscenity. *Id.* at 638-40. Furthermore, the Court has recognized that parents are entitled to laws which support their ability to safeguard their children from harm. *Id.* at 639. It is in this vein that this legislation is proposed. It is meant to assist parents, and fulfill the governmental interest, in protecting children from exposure to harmful material online. Some may argue that this legislation is unnecessary and redundant as today's parents and legal guardians have Internet filter and parental control options that that they can employ voluntarily. However, these piecemeal, and often easily circumvented, options are insufficient to effectively protect minors from harmful online materials due to the number of ways the Internet is accessed by smart devices and the manner in which each of these options currently operate.

The currently available options to parents include free or paid for filters provided by wireless carriers for mobile devices, home wireless filtering services, and filtering provided in public places such as libraries which receive government funding. While these tools are useful in certain contexts and may be better than nothing, for the reasons set out below this proposed legislation closes the gaps that these former technologies leave open and is the only realistic method of protecting minors from the masses of harmful material inundating them online. As will be explained in more depth, manufacturers already have the capabilities and, in some cases, have even developed strong parental controls, but few parents know about them, and they are difficult to navigate. When devices themselves have built-in software that is capable of filtering material on mobile and wireless networks, and is on by default at activation, minors will be protected from harmful material no matter where they are or what network their device is using. This solves the limitations of filtering technologies currently available and the manner in which they are implemented.

A. *Free or paid for filters provided by wireless carriers for smart phones and tablets are inadequate because they are limited to filtering mobile data, are frequently reported to be ineffective, and are easily disabled or circumvented by minor users.*

While a number of Mobile Internet Service Providers (ISPs) such as Sprint, Verizon, and T-Mobile provide customers with filtering software for mobile devices upon request for free or a monthly fee, this solution is very limited. Currently, filtering provided by Mobile ISPs have to be added in the form of an application and only filter mobile data provided by those ISPs. This is

problematic as users of mobile devices use mobile data, wireless networks or Wi-Fi, and applications to connect to the Internet from their mobile device. Users of mobile devices often have limited data plans or simply use Wi-Fi when available, instead of mobile data, either while at home or in Wi-Fi friendly public areas such as coffee shops. Once a minor turns off their mobile data and connects to a Wi-Fi network, private or public, this network is not filtered by the software offered by Mobile ISPs.[2] Thus, while Mobile ISP filtering services are a start, they are not the solution and cannot fully protect minors from harmful material online.

Filters provided by Mobile ISPs intended to assist parents and legal guardians with protecting minors from harmful material are easily circumvented by websites or minor users. T-Mobile's free service for instance, states on their support page that while "Web Guard" helps filter web content it does not block everything including user generated content such as email or secured web traffic from websites that start with "https." The filtering service is also not available for all devices, may not work at certain times or certain locations, and does not work with third party web browsers or applications.[3] Parents who have used Web Guard to protect minors from harmful material have reported the filter was easy to circumvent by "Googling" the name of major pornography sites, including Pornhub, and they were able to access the sites with the filter activated.[4] This is not to pick on T-Mobile or their efforts to provide parents and guardians with options to protect minors online but rather to demonstrate the need for a better solution.

B. Filters provided by ISPs in homes and businesses are not effective in protecting minors from harmful material online because they fail to protect minors as soon as they leave the home or when minors use alternative Internet sources such as mobile data.

Another effort to protect minors from harmful material online has been to provide optional filtering options for home and business wireless Internet. This optional filtering service is either provided by the wireless Internet service provider (ISP) or by an outside company such as OpenDNS.[5] While this source of Internet filtering is available to adults and legal guardians of minors either for free or a fee, it only protects minors from harmful content while they use the filtered Internet source. Under this effort when a minor uses mobile wireless data, a neighbor's wireless network, or a public wireless network they are often exposed to content that is harmful to minors. Additionally, this filtering service is often unknown to consumers as it is not

---

[2] *FAQs about parental controls using content filters*, https://www.sprint.com/en/support/solutions/device/faqs-about-parental-controls-using-content-filters.html (last visited June 9, 2021). *See also* T-Mobile Web Guard device content filter, https://support.t-mobile.com/docs/DOC-2144 (last visited June 9, 2021).

[3] T-Mobile, *supra* note 2.

[4] *Warning to parents: Web Guard doesn't work*, https://support.t-mobile.com/thread/140089 (last visited June 9, 2021).

[5] *See Open DNS*, www.opendns.com (last visited June 9, 2021).

automatically made available. Parents and legal guardians must seek out this technology, which poses a problem as many parents and legal guardians are unaware that this technology exists.

While some businesses such as Starbucks and McDonalds have chosen to make efforts to ensure Internet access (Wi-Fi) provided to patrons are not used to view pornography, there are many other businesses and places which offer free unfiltered Internet access.[6] Those who argue requiring devices to have built-in filtering capabilities is redundant – because parents have the option to filter wireless networks at home and at places of business are taking precautions as well – fail to take into account the various ways and places that minors access the Internet on smart phones and tablets.

II. Requiring manufacturers of smart phones and tablets to have active filtering technology that is controlled and removable by adult users is the least restrictive and most effective means to protect minors from online material that is harmful to them.

A. This legislation is narrowly tailored to address the Government's legitimate interest in protecting minors from exposure to harmful online materials without restricting adult access to protected speech.

Under this legislation, adults are not limited to only that speech which is appropriate for minors. *Butler v. Michigan*, 352 U.S. 380, 383 (1957). Adult purchasers of smart phones and tablets establish their device's passcode at the time of activation which allows them to change the settings of the active filter or deactivate the filters entirely. In contrast to previous efforts, which have required adults to contact Internet providers or a government agency to unblock a website or deactivate filters, this legislation gives each adult the capability of doing so themselves. This creates little burden on adults' access to speech while effectively protecting minors. By giving adults the power to determine if preinstalled, active filters will be used or how they will be used on their own devices, this legislation does not reduce adult's access to speech online to a pool of child-friendly speech but rather gives them an easy route to full Internet access. *Id.*

Other efforts to protect children online through filtering software have been upheld by the Supreme Court. For instance, the Children's Internet Protection Act requires libraries to use software that prevents Internet users from accessing obscenity or child pornography online as a condition of receiving federal funds. 20 U.S.C. § 9134(f)(1)(A)(i) (2005); *see also* 47 U.S.C. § 254(h) (2005). Challenged by the American Library Association, the Supreme Court held that requiring filters on library computers in exchange for funding was constitutional because the government had appropriated funds to establish a program for libraries and was entitled to

---

[6] The Washington Post, *Starbucks will soon start blocking porn on its public Wi-Fi* (Nov. 29, 2018, 1:16 PM), https://www.washingtonpost.com/news/voraciously/wp/2018/11/29/starbucks-will-soon-start-blocking-porn-on-its-public-wifi/?utm_term=.d2a1913c4478.

broadly define the program limits and insist that the public funds be spent for the purpose for which they were authorized. *United States v. Am. Library Ass'n*, 539 U.S. 194, 211-12 (2003). In that case, the Court determined Internet software filters restricting adult access to speech and the concern of possible over-filtering was inapplicable as the software could easily be disabled by library staff at the request of an adult patron. *Id.* at 209-210.

Compared to the Children's Internet Protection Act, this legislation is less restrictive and less burdensome for adult users as they have the ability to change filter settings or deactivate filters themselves. If it is only a small burden for an adult to ask a librarian to turn off a filter at a library, requiring an adult to turn off a filter on their own device, using a passcode created at activation, poses little burden on their access to speech online while providing protections for children. Additionally, an adult user merely has the option to use the active filter. There is no requirement for adults to use the active filters, a fee to disable the filters, or time delay on having a webpage or filter removed. Thus, there is no barrier that prevents adults who seek access to speech that is harmful to minors and no delay outside of the time it takes to enter a passcode to deactivate or adjust the filter.

This legislation also provides that emancipated youth, members of the armed forces, and minors who are married or reach the age of 18 shall create the passcode for their devices. Therefore, minors who become adults or minors who become emancipated are also empowered to decide for themselves what content to filter or to remove filters entirely.

B. There is no chill on free speech under the proposed legislation as it does not target specific kinds of speech at the source but rather empowers the listener to determine what speech should reach minors in their care.

The proposed legislation does not restrict speech from the source but allows parents and legal guardians to decide what speech is appropriate for the minors in their care. Previous efforts to protect minors online were found to be unconstitutional, in part because they were vague and threatened speakers with criminal action, thus creating a chill on speech. *Ashcroft,* 542 U.S. at 660; *Reno v. ACLU,* 521 U.S. 844, 845 (1997). No such chill on Free Speech is implicated here as no individual speaker is penalized under this statute. This proposed legislation is not vague, which will be addressed further below, and it completely avoids any possible chilling effect by targeting manufacturers responsibilities for safety rather than prohibiting any particular speech from occurring. Those who place content online which would be considered harmful to minors face no deterrence or consequence under this legislation. Instead, parents and legal guardians are empowered to decide for minor children, as well as for themselves, what kinds of speech they want to enter their homes and businesses through their smart phones and tablets. Parents and guardians themselves are able to adjust the filters for specific content or remove filters entirely if they deem them unnecessary.

C. *The proposed legislation is not vague in defining material that is harmful to minors as it is consistent with federal obscenity law and community standards are unlikely to differ regarding what material is harmful to minors.*

Under this legislation, manufacturers of devices are only required to install and activate filtering software that is capable of filtering content that is harmful to minors in accordance with Industry standards. The ultimate decision is left to parents and legal guardians. However, if challenged, the definition of material that is harmful to minors is not vague as it closely tracks Supreme Court precedent and "therefore gives 'men in acting adequate notice of what is prohibited.'" *Ginsberg*, 390 U.S. at 643 quoting *Roth v. United States,* 354 U.S. 476, 492 (1957). Additionally, community standards regarding what is harmful to minors is not likely to vary so much as to cause uncertainty among those working to comply with this legislation and community standard language alone is not unconstitutionally overbroad or vague. *Ashcroft*, 535 U.S. at 583-85. Furthermore, each parent from each community has the freedom under this legislation to decide what is appropriate within their community and modify their filters to be more or less restrictive. And lastly, the final determination of what content is prohibited for minors is not in the hands of the manufacturers. The only determination to be made by a manufacturer seeking to comply with this legislation is to choose which filtering software they want to use with their products.

D. *Requiring filtering software to be built into the devices when manufactured and active by default is the most effective way to equip parents and legal guardians to protect minors from harmful online material.*

As discussed in section I, if filtering is to be effective at protecting minors from harmful material online the filtering software must be on the device itself and be capable of filtering both Wi-Fi and mobile data networks. Otherwise, to be even partially effective a parent or legal guardian would be required to filter both their home Wi-Fi network as well as their mobile networks. Even then, as soon as a minor leaves the home, or while at home connects to a neighbor's unfiltered Wi-Fi network, the filters provided on the home network and on the mobile network are useless. Placing a filter on the device itself, as this legislation requires, ensures that wherever the device is used, and however the user accesses the Internet, material that is harmful to minors can be filtered. It closes the gaps that filters on specific Wi-Fi networks or mobile networks alone leave open. Lastly, better than other solutions such age verification requirements for websites, filters are able to protect minors from accessing material that is harmful from websites around the world, instead of just websites within the United States. *Ashcroft*, 542 U.S. at 667. Having filtering technology installed and active on devices effectively limits the child's access rather than putting the burden on speakers to restrain themselves therefore it is the most effective and least restrictive means of protecting minors online.

III. The technology required to filter both mobile and wireless internet service on smart phones and tablets exists, and it would not be burdensome to require manufacturers to install such technology on their products as they currently install other forms of active technology at the time of manufacturing.

Manufacturers of smart phones and tablets currently preinstall a range of applications and programs on their devices such as Internet search engines, antivirus software, photo editing software, maps, and music programs.[7] These applications vary depending on the manufacturer and the device but illustrate those manufacturers are already preinstalling programs and would not be overly burdened if required to include filtering software as a part of their default settings. Some manufacturers have already developed their own parental control and filtering software, such as Apple[8] and Google,[9] therefore all this legislation would require is to have these settings on by default and provide the process for adults and parents to remove/modify these settings by passcode. Additionally, phone manufacturers such as Apple are beginning to offer optional filtering and parental control settings on the phones themselves demonstrating such technology is indeed possible. Apple's latest iOS release includes built-in, but not default, parental filtering software in the iOS 12 upgrade.[10] This built-in parental control software has many features including customizable filtering capabilities that work on wireless, mobile, and application internet connections.[11] Apple's software, while not active at the time of purchase, offers built-in categories and suggested filter settings but leaves the determination of what content and websites will be filtered on each device up to the adult user, which is in line with what this legislation proposes.[12] Apple's software, while not active by default, offers built-in categories and suggested filter settings but leaves the determination of what content and websites will be filtered on each device up to the adult user, which is in line with what this legislation proposes.[13] Apple's decision to include optional parental controls in iOS software is an excellent illustration of how other companies and manufacturers can install active filtering capabilities into their products and that the requirements this legislation proposes are not overly burdensome or unrealistic for manufacturers to accomplish. Additionally, while Apple has taken the initiative to provide these tools to parents and legal guardians, most are unaware of these options which illustrate the need

---

[7] *See, e.g.*, *MacOS Big Sur*, https: www.apple.com/macos/big-sur/ (last visited June 10, 2021); *Galaxy S10e S10 S10+ S105G*, https://www.samsung.com/global/galaxy/galaxy-s10/specs/ (last visited June 9, 2021).

[8] *Use parental controls on your child's iPhone, iPad, and iPod touch*, https://support.apple.com/en-us/HT201304 (last visited June 9, 2021).

[9] *Help your family create healthy digital habits*, https://families.google.com/familylink/ (last visited June 9, 2021).

[10] *Use parental controls on your child's iPhone, iPad, and iPod touch*, https://support.apple.com/en-us/HT201304 (last visited June 9, 2021).

[11] *How Do I Set Up IOS 12 Screen Time Controls?*, https://protectyoungeyes.com/how-do-i-set-up-ios-12-screen-time-controls-definitive-guide-for-parents/ (last visited June 9, 2021).

[12] *Id.*

[13] *Id.*

for filtering software to be activated by default. Additionally, those children who are most vulnerable are at risk when manufacturers leave navigating these settings to already overburdened parents who are not tech savvy or even aware of all the dangers a smart device poses to their children. This legislation rightly places the burden on manufacturers to make their high-risk devices safe for children.