

parents and educators, such as links to wireless carriers' content access controls, and a "model Family Cell Phone Usage Agreement – a contract that parents can use to frame family discussions about safe and responsible use of wireless devices, and to educate the entire family regarding the potential threats to children from harmful content, unwanted contact, and inappropriate conduct."⁴⁵⁸ The wireless industry has also been active in the Family Online Safety Institute ("FOSI"), a Washington-based, international organization established to identify best practices in the field of online safety.⁴⁵⁹ Additionally, CTIA notes that the wireless industry is participating in the National Telecommunications and Information Administration's Online Safety and Technology Working Group.⁴⁶⁰

VI. NON-NETWORKED DEVICES

117. In the *NOI*, the Commission inquired as to the existence and availability of blocking technologies for non-networked devices capable of receiving video or audio programming, particularly DVD players and VCRs.⁴⁶¹ We noted that, unlike wired, wireless, or Internet platforms, which directly distribute video or audio content to consumers, DVD players and VCRs are dependent on video discs or videotapes to distribute content, and that this situation gives parents greater control over DVD players and VCRs than they have over other distribution platforms.⁴⁶² We invited comment on whether blocking technologies exist or are under development for DVD players and VCRs and, if so, how these technologies compare to blocking technologies available for other distribution platforms and networked devices.⁴⁶³ We also sought comment on whether blocking technologies exist for similar non-networked devices, such as digital audio players (MP3 players) and portable media players, and, if so, the extent to which those technologies might be used by parents.⁴⁶⁴ Additionally, we inquired as to what methods would be effective in encouraging the development and use of such technologies.⁴⁶⁵ Finally, we inquired whether the MPAÄ rating system generally used for movies on DVDs and video tapes is effective.⁴⁶⁶

118. Only a few commenters address these issues. CustomPlay, PFF, TVGuardian, Digimarc, DMA, and DWA each discuss blocking technologies that are applicable to various distribution platforms, including DVD players, VCRs, and similar non-networked devices, such as digital audio players and portable media players.⁴⁶⁷ No commenter specifically addresses the effectiveness of the

⁴⁵⁸ See *id.* at 13-14.

⁴⁵⁹ See *id.* at 15; FOSI Comments at 3-5. On April, 22, 2009, The Wireless Foundation and FOSI co-sponsored a wireless online safety conference, with a focus on wireless-specific aspects of online safety such as mobility and location-based services. See FOSI Press Release at <http://www.fosi.org/cms/index.php/pr2009/43-pr-2009/358-wireless-online-safety-conference.html>. Appendix A of FOSI's comments provides a summary chart of the online safety initiatives of its members.

⁴⁶⁰ See CTIA Comments at 16. CTIA notes that the Working Group was established under Section 214 of the Protecting Children in the 21st Century Act. See *id.* (citing Protecting Children in the 21st Century Act, Pub. L. No. 110-385, § 214, 122 Stat. 4096, 4103-04 (Oct. 10, 2008) (to be codified at 15 U.S.C. § 6554)).

⁴⁶¹ See *NOI*, 24 FCC Red at 3355, ¶ 34.

⁴⁶² See *id.* at 3355-56, ¶ 35.

⁴⁶³ See *id.* at 3356, ¶ 36.

⁴⁶⁴ See *id.*

⁴⁶⁵ See *id.*

⁴⁶⁶ See *id.*

⁴⁶⁷ See CustomPlay Comments at 3, 4; PFF Comments at 27-32; TVGuardian Comments at 19-20, 26 and Appendix C; Digimarc Comments at 5; DMA Comments at 6-8; DWA Comments at 5-7. NARM addresses audio-only (continued....)

MPAA rating system with regard to movies on DVDs and video tapes.

119. CustomPlay states that it has developed a content customization system that utilizes the capabilities of random access technologies, such as DVD players and VOD services, to selectively play, skip, or mute portions of a motion picture.⁴⁶⁸ CustomPlay notes that information provided by a source other than the motion picture identifies the content of segments in that picture.⁴⁶⁹ According to CustomPlay, this information enables a random access device to customize, in real time, the presentation of a motion picture, and this customization is responsive to a viewer's content preference for a level of explicitness in 14 separate categories of possible objectionable content.⁴⁷⁰

120. PFF notes that one company, ClearPlay, produces a unique DVD player that eliminates profanity, violence, and nudity from certain movies.⁴⁷¹ PFF states that ClearPlay does not produce pre-edited DVDs, but rather places filters into its DVD player, enabling it to know when to skip or mute while the movie is playing.⁴⁷² Therefore, PFF states, consumers do not have to purchase special DVDs; rather, they only need to purchase a ClearPlay DVD player and download the codes for their movies to activate the filtering controls.⁴⁷³ PFF explains that ClearPlay's MaxPlay DVD player retails for under \$70 and comes loaded with the filters for about 1,000 popular movies, with access to new movie filtering codes available at a monthly membership fee of \$7.95.⁴⁷⁴ PFF reports that ClearPlay's technology has raised copyright concerns and was opposed by many movie directors and studios, but PFF observes that in 2005 Congress exempted services like ClearPlay from any copyright liability.⁴⁷⁵ PFF notes, however, that other types of pre-edited DVD software service – “scrubbed” DVDs – were ruled to violate copyright laws by a U.S. district court judge in 2006 and are no longer available.⁴⁷⁶

121. As discussed above, TVGuardian is an example of a technology that filters language based on closed captioning information.⁴⁷⁷ TVGuardian states that its AFLFT has already been deployed in approximately 12 million DVD Players, VCRs, and combination units.⁴⁷⁸ According to TVGuardian, over the past two years, DVDs have been increasingly distributed with a new caption format, called Subtitles for the Deaf and Hard-of-Hearing (“SDH”), rather than closed-captions in the television format

(Continued from previous page) _____

devices and asserts that Congress did not intend for the Commission to address technologies relating to such devices, including MP3 players and other portable audio devices. See NARM Comments at 1.

⁴⁶⁸ See CustomPlay Comments at 1.

⁴⁶⁹ See *id.*

⁴⁷⁰ See *id.*

⁴⁷¹ See PFF Comments at 42.

⁴⁷² See *id.*

⁴⁷³ See *id.*

⁴⁷⁴ See *id.*

⁴⁷⁵ See *id.* PFF notes that this legislation – The Family Movie Act of 2005, Pub. L. No. 109-9, Title II, 119 Stat. 223 (2005) (codified at 17 U.S.C. § 101 note) – was included in The Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, 119 Stat. 218 (2005), and was signed into law on April 27, 2005. See *id.*

⁴⁷⁶ See *id.* at 43.

⁴⁷⁷ TVGuardian can operate with both networked and non-networked technologies. Accordingly, we also discuss TVGuardian in Section II.C above pertaining to devices for television.

⁴⁷⁸ See TVGuardian Comments, Appendix C at 3.

standard.⁴⁷⁹ TVGuardian states that its technology cannot easily read the SDH format.⁴⁸⁰ TVGuardian states that its technology faces a similar problem with Blu-Ray players.⁴⁸¹ TVGuardian explains that its technology works for movies shown on television (broadcast or pay-TV) because the standard closed-captioning format is required by law.⁴⁸²

122. As discussed above, Digimarc and DWA discuss the potential for digital watermarking to provide advanced blocking for non-networked devices, as well as across multiple media platforms.⁴⁸³ Digimarc recommends that the Commission focus on approaches to parental control in which the data that enables such control is contained in the content itself, such as digital watermarking.⁴⁸⁴ As also discussed above, CEA expresses concern that proponents of digital watermarking are using the issue of parental controls over objectionable content as an avenue to accomplish their goal of requiring televisions and other devices to incorporate DRM functionality.⁴⁸⁵ In addition, CEA argues that watermarking raises a number of intellectual property and other technical issues.⁴⁸⁶

123. While the record reflects that parental control technologies exist for DVD players, VCRs, and similar non-networked devices, the record is lacking data in a number of areas regarding parental control devices for these devices that the Commission intends to explore in a forthcoming *NOI*.⁴⁸⁷

VII. INTERNET

A. Internet

124. The *NOI* asks about “technologies that can improve or enhance the ability of a parent to protect his or her child from any indecent or objectionable video or audio programming” that “may be appropriate across a wide variety of distribution platforms, including ...Internet platforms.”⁴⁸⁸ During the first quarter of 2009, children between the ages of two and 11 spent an average of one hour and 45 minutes per month watching video over the Internet, and teens between the ages of 12 and 17 spent two hours and 50 minutes per month watching video over the Internet.⁴⁸⁹ This section will concentrate on video programming accessible over the Internet, and is informed by previous online safety work. After providing a technical discussion regarding the availability of video on the Internet, we consider the variety of parental controls. We discuss how numerous solutions are available that address different risks, and note that an effective approach to online safety requires multilayered solutions, including

⁴⁷⁹ *See id.*

⁴⁸⁰ *See id.*

⁴⁸¹ *See id.*

⁴⁸² *See id.*

⁴⁸³ *See generally* Digimarc Comments; DWA Comments. Digital watermarking can operate with both networked and non-networked technologies. Accordingly, we also discuss digital watermarking in Sections II.C and V above pertaining to networked devices (television and wireless).

⁴⁸⁴ *See* Digimarc Comments at 1.

⁴⁸⁵ *See* CEA Reply at 10.

⁴⁸⁶ *See id.* at 10-11. *See also* TiVo Reply at 3.

⁴⁸⁷ *See infra* section XI.

⁴⁸⁸ *See NOI*, 24 FCC Rcd at 3356, ¶ 37. *See also* Child Safe Viewing Act at Section 2(b)(1), 2(d).

⁴⁸⁹ *See* The Nielsen Company, *A2/M2 Three Screen Report, 1st Quarter 2009*, at 3, Table 3. In addition, teens aged 13-17 spent an average of 6 hours and 30 minutes per month watching video on a mobile telephone. *Id.*

software solutions, network service provider solutions, content service provider solutions, education, acceptable use policies, and supervision. The record is lacking data in a number of areas regarding Internet parental control technologies, which we intend to explore in a forthcoming *NOI*.⁴⁹⁰

B. Introduction

125. The complexities of the Internet present unique challenges.⁴⁹¹ On the Internet, a multitude of individuals, applications, and content⁴⁹² interact, with no centralized points of control.⁴⁹³ The same content can be hosted at a variety of sites. Individuals can create content, making it available to everyone in the world.

126. The number of suppliers of online video and audio is almost limitless, the supply chain is fragmented, and the content can come from sources outside the jurisdiction of the United States.⁴⁹⁴ Video and audio can be delivered through web pages, email attachments, chat rooms, text messages and tweets, bulletin boards, peer-to-peer file sharing, and video and audio applications.⁴⁹⁵ While there are some video hosts that dominate the video market, such as the top online video site YouTube, anyone with access to online storage can make videos and audio recordings available. Producers of content may be commercial or non-commercial, individuals or corporations.⁴⁹⁶

127. As noted in the *NOI*, the Internet as an open network permits parents to select among a

⁴⁹⁰ See *infra* section XI.

⁴⁹¹ See Dick Thornburgh and Herbert S. Lin, *Youth, Pornography, and the Internet*, Computer Science and Telecommunications Board, National Academies Press (2002), at 3 (“NAS Report”) (“[C]ompared to other media, the Internet has characteristics that make it harder for adults to exercise responsible supervision over children’s use of it.”); *Final Report of the COPA Commission Presented to Congress* (2000), <http://www.copacommission.org/report/executivesummary.shtml>, at 13 (“COPA Report”) (“unlike one-way broadcast media, the Internet is inherently multi-directional and interactive.”).

⁴⁹² See COPA Report at 13 (“thousands of access providers and millions of potential publishers provide content online.”).

⁴⁹³ See Dr. Tanya Byron, *Safer Children in a Digital World: the Report of the Byron Review* (2008) (“Byron Review”) at 5 (“there is no obvious single point at which editorial control can be exercised. This means that it is very difficult for national Governments to reduce the availability of harmful and inappropriate material”); NTIA Study of Technology Protection Measures pursuant to the Children’s Internet Protect Act, Report to Congress, Children’s Internet Protection Act, Pub. L. 106-554, Study of Technology Protection Measures in Section 1703, Sec. I (2003), http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/CIPAreport_08142003.htm (“CIPA Study”) Sec. II.A (describing Internet as “decentralized”). Examples of governments having difficulty imposing control over Internet content, including video content, abound. See, e.g., Brian Stelter & Brad Stone, *Web Pries Lid Off Iranian Censorship*, N.Y. Times (Jun. 22, 2009), <http://www.nytimes.com/2009/06/23/world/middleeast/23censor.html>.

⁴⁹⁴ See COPA Report at 13 (“Material published on the Internet may originate anywhere, presenting challenges to the application of the law of any single jurisdiction.”); *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775, 789 (E.D. Pa. 2007) (“*Gonzales*”) (discussing amount of adult websites that are outside the United States).

⁴⁹⁵ Specific types of video and audio applications are discussed below. See NAS Report at 6 (discussing different applications that can distribute offensive content).

⁴⁹⁶ See NAS Report at 4 (Congress requested that the National Academies of Sciences “conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet.”) at 4. See also *Gonzales*, 478 F. Supp. 2d at 798-799; *American Civil Liberties Union v. Mukasey*, 534 F.3d 181, 200 (3rd Cir. 2008) (“*Mukasey*”) (discussing commercial and non-commercial content).

wide variety of parental control technologies available in a competitive market.⁴⁹⁷ On the Internet, safety solutions can operate independently without coordination with, cooperation with, or permission from content producers or network service providers. As discussed below, the disaggregation of content, sources, applications, access, and networks on the Internet means that there is no single Internet safety solution. As the COPA Report stated, “[m]ethods to protect children from content harmful to minors must be effective in this diverse and decentralized environment.”⁴⁹⁸ As many others have concluded, online solutions are complex.⁴⁹⁹

128. The Commission asked in the *NOI* how the value of the Internet as an educational and informational tool for children can be balanced against efforts to ensure children’s online safety.⁵⁰⁰ Commenters note the importance of recognizing that the Internet provides a positive opportunity for children, giving them educational opportunities, information, social interaction, and the ability to become creators of content.⁵⁰¹ The recent Internet Safety Technical Task Force (“ISTTF”) Report stated that “[m]any youth in the United States have fully integrated the Internet into their daily lives. For them, the Internet is a positive and powerful space for socializing, learning, and engaging in public life.”⁵⁰² Commenters also note, however, that the Internet also poses risks to children.⁵⁰³ As one expert has noted, “[d]ata is beginning to reveal risks to young people in terms of increased exposure to sexually inappropriate content, contributions to negative beliefs and attitudes, stranger danger, cyberbullying and access to inappropriate content from sites which may promote harmful behaviors. Moreover, there are issues relating to commercial content and contact with young people.”⁵⁰⁴ While a number of online risks exist, the Child Safe Viewing Act specifically directs the Commission to address indecent or offensive video and audio programming.⁵⁰⁵

129. Commenters urge, and we agree, that it is important to balance the benefits of being online with the risks. CDT states that “[t]he opportunities and benefits for minors of one of the primary

⁴⁹⁷ See *NOI*, 24 FCC Rcd at 3360, ¶ 42.

⁴⁹⁸ COPA Report at 13.

⁴⁹⁹ See, e.g., NAS Report at 11 (“Contrary to statements often made in the political debate, the issue of protecting children from inappropriate sexually explicit material and experiences on the Internet is very complex.”)

⁵⁰⁰ See *NOI*, 24 FCC Rcd at 3361, ¶ 43.

⁵⁰¹ See, e.g., USTelecom Comments at 3; Verizon Comments at 9; CDT Comments at 15. See also CIPA Study, Exec. Sum. (“In homes, schools, and libraries across the nation, the Internet has become a valuable and even critical tool for our children’s success. Access to the Internet furnishes children with new resources with which to learn, new avenues for expression, and new skills to obtain quality jobs.”); Byron Review at 2, 6 (noting specifically the advantages that IT offers for individuals with disabilities); NAS Report at 1 (“The Internet provides convenient access to a highly diverse library of educational resources, enables collaborative study, and offers opportunities for remote dialog with subject-matter experts. It provides information about hobbies and sports, and it allows children to engage with other people on a near-infinite variety of topics.”).

⁵⁰² *Final Report of the Internet Safety Technical Task Force: Enhancing Child Safety and Online Technologies*, Berkman Center for Internet & Society (2008) (“ISTTF Report”) at 4.

⁵⁰³ See AT&T Comments at 4-5; CIPA Study, Exec. Sum.; Byron Review at 2, 4; NAS Report at 3; *What are the Risks for Children Online*, GetNetWise, <http://kids.getnetwise.org/safetyguide/danger/>.

⁵⁰⁴ Byron Review at 4. See also ISTTF Report at 4 (noting “dangers of sexual exploitation, online harassment, and bullying, and exposure to problematic and illegal content” and noting “in most cases [risks are] not significantly different than those they face offline.”).

⁵⁰⁵ See Child Safe Viewing Act at Section 2(d).

‘new media platforms’ – the Internet – far outweigh the risks.”⁵⁰⁶ Moreover, as discussed below, a growing number of technologies assist parents in minimizing the risks while introducing children to the vast benefits of the Internet.

C. Previous and Current Online Safety Work

130. Several commenters encourage the Commission to be aware of the existing body of online safety reports and relevant case law.⁵⁰⁷ As AT&T, for example, states “[m]embers of the Internet community, parents groups, state and government officials and other organizations already have compiled a substantial body of work regarding the risks children face online, and the variety of parental control and online child protection tools and methods already available, as well as those on the horizon.”⁵⁰⁸

131. As noted in the *NOI*, the safety of children online has been a primary concern of families and Congress since the Internet was first available for public use.⁵⁰⁹ Congress has addressed this issue through numerous laws.⁵¹⁰ Commenters urge the Commission to be sensitive to the constitutional issues previous federal laws have raised.⁵¹¹ There have also been several federally mandated reports:⁵¹² (i) the

⁵⁰⁶ CDT Comments at 15. *See also* CIPA Study, Exec. Sum.; Byron Review at 4; NAS Report at 1 (“[W]e must approach our need to protect children with care to avoid placing unnecessary restriction on the many positive features of the Internet.”).

⁵⁰⁷ *See, e.g.*, AT&T Comments at 4-5; CDT Comments at 10.

⁵⁰⁸ AT&T Comments at 2.

⁵⁰⁹ *See NOI*, 24 FCC Rcd at 3357, ¶ 38.

⁵¹⁰ *See, e.g.*, Telecommunications Act of 1996, Sec. 501 *et. seq.*, The Communications Decency Act, Pub. L. No. 104-104, 110 Stat. 56 (1996), *codified at* 47 U.S.C. § 230 (ruled unconstitutional in part in *Reno v. ACLU*, 521 U.S. 844 (1997)); Children’s Online Protection Act (COPA), Pub. L. No. 105-277, 112 Stat. 2681-2736 (1998), *codified at* 47 U.S.C. § 231 (2000) (struck down as unconstitutional on First Amendment grounds in *ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008), *cert. denied*, (129 S. Ct. 1032 (2009)); Children’s Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277, 112 Stat. 2581-728 (1998), *codified at* 15 U.S.C. §§ 6501-6508 (2000); Children’s Internet Protection Act (CIPA), Pub. L. No. 106-554, 114 Stat. 2763, 2763A-335 (2000), *codified at* 47 U.S.C. § 254(h), 20 U.S.C. § 9134 (2000); Dot Kids Implementation and Efficiency Act of 2002, Pub. L. No. 107-317, 16 Stat. 2766, *codified at* 47 U.S.C. § 941 (2002); Truth in Domain Names Act of 2003, Pub. L. No. 108-21, *codified at* 18 U.S.C. § 2252B (2003); Providing Resources, Officers and Technology to Eradicate Cyber Threats to Our Children Act of 2008, Pub. L. No. 110-401, 121 Stat. 4229 (2008) (to be *codified at* 18 U.S.C. §§ 2258A-E; 42 U.S.C. §§ 17601, 17611-16) (hereinafter PROTECT Our Children Act of 2008); Child Protection and Sexual Predator Punishment Act of 1998, Pub. L. No. 105-314, 112 Stat. 2974 (1998); Reporting of Child Pornography by Electronic Communication Service Providers, Pub. L. No. 101-647, 104 Stat. 4806, *codified as* 42 U.S.C. § 13031 (requires IPSs, when they become aware of potential child pornography, to report this to the National Center for Missing and Exploited Children); Keeping the Internet Devoid of Sexual Predators Act of 2008 (hereinafter KIDS act of 2008), Pub. L. No. 110-400, 122 Stat. 4224 (2008), *codified as* 42 U.S.C.A. § 16915 (2008) (requiring sex offenders to register their online identifiers); Protecting Children in the 21st Century Act, Broadband Data Improvement Act, Pub. L. No. 110-385, Sec. II, Protecting Children in the 21st Century Act (2008); *see also*, Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (2006) (*codified as amended in scattered sections of* 42 U.S.C.) (mandated Internet access to state sex offender registries, facilitating public access to information); Child Pornography Prevention Act, Pub. L. No. 104-208, § 121, 110 Stat. 3009 (1996), *codified as* 18 USC § 2252 (1996).

⁵¹¹ *See* CDT Comments at 13-14 (stating “the constitutional limits on government regulation of online content do not change depending on whether the content previously had been broadcast over the air.”); Industry and Public Interest Groups Joint Comments at 3-4; EFF Reply at 3.

Final Report of the COPA Commission;⁵¹³ (ii) the National Academies of Science Report;⁵¹⁴ and (iii) the NTIA Study of Technology Protection Measures pursuant to the Children's Internet Protect Act.⁵¹⁵ There has also been federal law enforcement activity and educational programs. As AT&T noted, a great deal of work has also been done by non-U.S. Government entities which have examined and worked towards child online safety.⁵¹⁶

132. Most recently, in the Broadband Data Improvement Act, Congress directed NTIA to establish the Online Safety and Technology Working Group ("OSTWG")⁵¹⁷ "to review and evaluate the status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children."⁵¹⁸ OSTWG's online safety mandate is broad, covering all online content and applications. The OSTWG includes 34 expert participants (many of whom have commented in this proceeding) from a diversity of corporations, organizations, and government agencies concerned with online safety.⁵¹⁹ OSTWG has until June 4, 2010 to submit a report to Congress, which we expect will expand on many of the issues raised in this *Report*.

D. The Availability of Video on the Internet

133. As noted in the *NOI*, online video and audio can be delivered in many different ways.⁵²⁰ Many sites stream video and audio to an audience. An individual goes to a host site and requests a

(Continued from previous page) _____

⁵¹² In addition, PROTECT Act of 2008 requires the Department of Justice to file several reports on topics such as its strategy for protecting children, its forensic resources and capabilities, and the progress of the Internet Crimes Against Children Task Forces. See PROTECT Act of 2008, Pub. L. 110-401 (2008).

⁵¹³ COPA Report, Executive Summary (Congress directed the COPA Commission to "identify technological or other methods that . . . will help reduce access by minors to material that is harmful to minors on the Internet.").

⁵¹⁴ See NAS Report (Congress requested that the National Academies of Sciences "conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet").

⁵¹⁵ See Report to Congress, Children's Internet Protection Act, Pub. L. 106-554, Study of Technology Protection Measures in Section 1703, Sec. 1 (2003), http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/CIPAreport_08142003.htm (Congress directed NTIA "to evaluate whether currently available Internet blocking or filtering technology protection measures and Internet safety policies adequately address the needs of educational institutions").

⁵¹⁶ See AT&T Comments at 4-5. See, e.g., ISTTF Report; Byron Review; *Making Wise Choices Online*, Family Online Safety Institute (2008) ("FOSI Report"); *Safer Internet for Children: Qualitative Study of 29 European Countries*, Directorate General Information Society and Media, European Commission (2007); *Protecting Children in the Internet Age*, New York State Senate Task Force on Critical Choices (2007).

⁵¹⁷ See *NOI*, 24 FCC Rcd at 3358, ¶ 38; Online Safety and Technology Working Group, National Telecommunications and Information Administration, Department of Commerce, <http://www.ntia.doc.gov/advisory/onlinesafety/>.

⁵¹⁸ Broadband Data Improvement Act, Pub. L. 110-385, Sec. 214(b) (2008); See also CDT Comments at 10 ("The Commission does not have any independent authority or experience with content on the Internet, and in light of the OSTWG effort the Commission should not reach out beyond the terms of the Act to address Internet content generally.").

⁵¹⁹ Online Safety and Technology Working Group: Participants, National Telecommunications and Information Administration, Department of Commerce, <http://www.ntia.doc.gov/advisory/onlinesafety/participants.html>.

⁵²⁰ See *NOI*, 24 FCC Rcd at 3356-57, ¶ 37.

specific video; the host streams the video to the individual while it is being played, and the video is not otherwise stored on the individual's computer. The host may use a proprietary application embedded in the webpage to display the video, with copyright protection built in, limiting the ability of the individual to view the video in any other way. In order to view the video, the individual generally must be online. Examples of sites using this delivery method include YouTube, Hulu, and Fox Interactive.

134. Another delivery method is for the individual to download the video or audio file onto the individual's computer and play it on demand. The individual may search and find video or audio files and elect to download them. Alternatively, the individual might subscribe to a video or audio feed. Whenever a new video or audio file is released, it is automatically downloaded to the individual's computer and is available to be played; this is known as podcasting and vodcasting.⁵²¹ Generally, the file is stored on the individual's computer, and the individual can play the files whenever and for as long as the individual wants. Some television sets have the ability to download shows and movies built directly into the set.⁵²²

135. An alternative means of video and audio file download distribution involves peer-to-peer ("P2P"). P2P applications allow individual computer users to transmit data directly to another user, without the use of an intermediate network service. The P2P software and services⁵²³ permit individuals to search the computers of other participants for the desired content, and individual members act as hosts, distributing content from their computers. This is a highly decentralized system of content distribution.⁵²⁴

136. Finally, audio and video files can be transferred across the Internet in the same way that any other data can be transferred: email, file transfers, bulletin boards, social networks, and more.⁵²⁵ Files can also be ripped and burned from the network and then distributed on CDs or DVDs.

⁵²¹ Generally, podcasting is a series of audio recordings that can be subscribed to by individuals using RSS ("Really Simple Syndication"). Having subscribed, whenever the content creator releases a new recording, that recording will automatically be downloaded to the individual's computer or MP3 player. Likewise, vodcasts are a series of video recordings that can be subscribed to by individuals and automatically downloaded.

⁵²² Examples of sites where video and audio content, such as TV shows or movies, can be downloaded include iTunes, Amazon, and Audible. See, e.g., <http://www.apple.com/itunes/>; <http://www.amazon.com/Video-On-Demand/b?ie=UTF8&node=16261631>; <http://www.xbox.com/en-US/live/>. Services such as Netflix and Blockbuster now allow customers to download movie rentals. <http://www.netflix.com/HowItWorks#faq8>; <http://www.blockbuster.com/download>.

⁵²³ See, e.g., BitTorrent, <http://www.bittorrent.com/>; Kazaa, <http://www.kazaa.com/>; Limewire, <http://www.limewire.com/>.

⁵²⁴ See OECD Glossary of Statistical Terms (Aug. 29, 2003), <http://stats.oecd.org/glossary/detail.asp?ID=6095> ("Peer-to-peer is a communication structure in which individuals interact directly, without going through a centralized system or hierarchy."); Clay Shirky, *What is P2P . . . And What Isn't*, O'Reilly OpenP2P (Nov. 24, 2000), <http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html>; Ed Felten, *More on Berman-Coble's Peer-to-Peer Definition*, Freedom to Tinker (Sept. 10, 2002), <http://www.freedom-to-tinker.com/blog/felten/more-berman-cobles-peer-peer-definition>; Rudiger Schollmeier, *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*, Computer Society (2002). *P2P File Sharing*, iKeepSafe.org, http://www.ikeepsafe.org/PRC/topics/?action=display_article&article_id=52.

⁵²⁵ See Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process*, in *Proceedings of the 2003 ACM Workshop on Digital Rights Management*, October 27, 2003, Washington, DC. (discussing sources for and methods of content distributed online); Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, *The Darknet and the Future of Content Distribution*, Microsoft, <http://msl1.mit.edu/ESD10/docs/darknet5.pdf>.

137. There is a great diversity of video and audio content online from a wide variety of sources. Many sources of video and audio programs traditionally seen on television are making their content available over the Internet.⁵²⁶ Services such as Hulu permit individuals to watch television programs and movies that are streamed to computer screens.⁵²⁷ A wealth of educational video is also available online.⁵²⁸

138. The ease and affordability of video and audio content creation has resulted in an explosion of content creators. New digital cameras, editing software, and video hosting services allow anyone, including children, to become creators of content.⁵²⁹ Some cameras and editing software are affordable and high quality. Digital cameras are now ubiquitous. People are producing video and audio content prolifically; YouTube reports that 20 hours of video is uploaded to its service every minute.⁵³⁰ Online safety organizations praise online material that helps show parents how to teach their children how to create content with new media tools.⁵³¹

139. Individuals can also create short video messages.⁵³² Video chatting is the use of short recorded videos or real time video to engage in conversations. Many forums, including YouTube, permit participants to post video comments as well as write comments. Social networks permit the uploading of video, some of which may be more formal productions, and some of which amount to an individual simply recording a message. Other chat features allow two or more people to talk to each other in real time much like a telephone call. These opportunities raise their own set of parental concerns.⁵³³

E. Discussion

140. In the *NOI*, the Commission invited comment on technologies available or under development to control children's access to Internet content, as well as any other parental empowerment tools currently available.⁵³⁴ We agree with those commenters who recognize that there is no one solution

⁵²⁶ See, e.g., <http://www.cbs.com/video/>; <http://abc.go.com/>; <http://www.fox.com/>; <http://www.nbc.com/>; <http://www.pbs.org/video/>; <http://mlb.mlb.com/mlb/subscriptions/index.jsp>.

⁵²⁷ Hulu is a joint effort of NBC Universal, News Corp, ABC, and Providence Equity Partners. See <http://www.hulu.com/>. See also <http://www.veoh.com/>; <http://www.joost.com/>.

⁵²⁸ See NAS Report at 9 (commenting on the importance of having "compelling, safe, and educational Internet content that is developmentally appropriate, educational, and enjoyable"). Examples of sites providing educational video include Smithsonian Kids, Discovery Education, iTunes University, Disney Educational Production. A number of educational videos can be found on hosting sites such as YouTube.

⁵²⁹ See ISTTF Report at 5; *Top 10 Safety Tips for Video-Sharing*, ConnectSafely (Sept. 3, 2007), <http://www.connectsafely.org/Safety-Tips/top-10-safety-tips-for-video-sharing.html> ("Many kids today are video-literate – able to communicate in a medium once reserved for highly trained professionals with expensive equipment.").

⁵³⁰ See Ryan Junee, *Zoinks! 20 Hours of Video Uploaded Every Minute!*, YouTube Blog (May 20, 2009), <http://www.youtube.com/blog?entry=on4EmafA5MA>

⁵³¹ See *Creating with Digital Media*, <http://www.common sense media.org/creating-digital-media>. See, e.g., *A Common Sense Approach to Internet Safety*, Common Sense Media, YouTube (May 29, 2008), <http://www.youtube.com/watch?v=cQ1ZqiYzSTw>.

⁵³² See PFF Comments at 90 (noting chat capabilities).

⁵³³ *Video Chatting*, <http://www.common sense media.org/video-chatting>

⁵³⁴ See *NOI*, 24 FCC Rcd at 3360, ¶ 41.

at present to address online safety concerns.⁵³⁵ As discussed above, there is a wide array of content, applications, sources, experiences, and risks online. Different parents have different concerns, and the same parents may have different concerns for children of different ages.⁵³⁶ Numerous solutions are available that address different risks. With this complexity, an effective approach requires multilayered solutions including public education and consumer empowerment technologies and methods, among others.⁵³⁷

141. Commenters state that there is an unprecedented abundance of parental control tools available in the market today. PFF filed in the record a comprehensive list of such parental control technologies.⁵³⁸ Commenters assert the competitive marketplace of parental control tools fosters innovative solutions and a diversity of choices for parents.⁵³⁹

142. Commenters point to the recent COPA District Court decision which found that parents have easy access to affordable⁵⁴⁰ parental control tools.⁵⁴¹ The COPA District Court found that filters

⁵³⁵ See AT&T Comments at 5 (there is “growing consensus that there is no single silver bullet to keep children safe online, nor is there an “easy technological fix to shield children from harmful content or to keep them from behaving inappropriately online”); FOSI Comments at 5-6 (“The ISTTF’s report found that there is no one silver bullet to keeping kids safe online and that education is essential to protecting kids online.”); PFF Comments at 72. See also ISTTF Report at 6 (“Technology can play a helpful role, but there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors.”); NAS Report at 13 (“Though some might wish otherwise, no single approach – technical, legal, economic, or educational-will be sufficient. Rather, an effective framework for protecting our children from inappropriate materials and experiences on the Internet will require a balanced composite of all of these elements, and real progress will require forward movement on all of these fronts.”).

⁵³⁶ See CIPA Study at Sec. IV.A. (recommending “Establish flexible policies that accommodate different ages and implement education settings with varying degrees of supervision”); NAS Report at 2.

⁵³⁷ See PFF Comments at 99. See also ISTTF Report at 6 (stating “a combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers may assist in addressing specific problems minors face online”); *Gonzales*, 478 F. Supp. 2d at 794 (explaining that filtering technology has improved in part because the services “provide multiple layers of filtering”). COPA Report at 7-9 (“no single technology or method will effectively protect children from harmful material online” but “[r]ather. . . a combination of public education, consumer empowerment technologies and methods, increased enforcement of existing laws, and industry action are needed to address this concern”).

⁵³⁸ See PFF Comments at 78-79. See also Advertisers Comments at 4; AT&T Comments at 7; Joint Comments of CDT et al at 12 (“The Internet is a major ‘parental empowerment’ success story, with effective and easy-to-use tools that offer parents a wide variety of approaches to online safety.”); Comcast Reply at 2; FOSI at 5-6; EFF Reply at 2 (“The record is abundantly clear that these technologies continue to be created, deployed, and extensively advertised”).

⁵³⁹ See PFF Comments at 6 (“A marketplace of controls and filters can then develop that is more closely tailored to the diverse values of the citizenry”); EFF Reply at 2; Comcast Reply at 2; AT&T Comments at 6 (mandating a single solution would “‘stifle future progress in this area’ by encouraging service providers to build to the standard or rule rather than continuing to innovate and invest to meet new online threats and challenges as they appear”). See also *Gonzales*, 478 F. Supp. 2d at 795 (“There is a high level of competition in the field of Internet content filtering. That factor, along with the development of new technologies, has also caused the products to improve over time.”); CIPA Study, Sec. III (“NTIA also found that more companies are increasingly entering the market for Internet content protection technology” and companies are “increasing the amount of money that they put into their research and development divisions”).

⁵⁴⁰ See COPA Report, Sec. II (reviewing costs of online safety tools).

are “easy to install, configure, and use and require only minimal effort by the end user to configure and update.”⁵⁴² While there are many different tools offering different types of solutions, these tools may be bundled together in the operating system or by the network service provider, offering parents the ability to open, click, and turn on parental control tools without having to purchase or download additional software. Parental control tools are built into several operating systems, including Windows Vista and Mac OS X. Windows 7 will also reportedly have parental control tools built in.⁵⁴³ Network service providers frequently offer parental control tools bundled into the software package provided to new customers.⁵⁴⁴ They are frequently offered for free.⁵⁴⁵ Off-the-shelf tools can be purchased in stores⁵⁴⁶ and are available online for download. As several commenters note, online safety organizations, such as GetNetWise, also make online safety tools easy to find, with online searchable directories that can help parents find the specific tools that they need.⁵⁴⁷ Given this range of options, commenters assert that there is no single solution to provide Internet safety; rather, many solutions can be used together to tailor an approach appropriate for each family.⁵⁴⁸ We will discuss many of these options below, including software filters, monitors, safe applications, labels, flags, safe search, and parent and caregiver driven solutions.

143. Studies have found that Internet parental control tools on the market are effective⁵⁴⁹ and that those who use these tools are generally pleased with their performance.⁵⁵⁰ Some commenters point out that these tools are not foolproof.⁵⁵¹ CDT and other commenters observe, however, that while these

(Continued from previous page)

⁵⁴¹ See *Mukasey*, 534 F.3d at 201; *Gonzales*, 478 F. Supp. 2d at 793; COPA Report, Sec. II.B. Filtering/Blocking. See also Industry and Public Interest Groups Joint Comments at 13-14.

⁵⁴² *Mukasey*, 534 F.3d at 201; *Gonzales*, 478 F. Supp. 2d at 793.

⁵⁴³ See Microsoft Comments at 7; PFF Comments at 79-81; FOSI Comments at 8. See also Microsoft VISTA Parental Controls, <http://www.microsoft.com/protect/products/family/vista.mspx>.

⁵⁴⁴ See PFF Comments at 77; NCTA Comments at 12-13 (noting efforts of broadband Internet providers). See *Gonzales*, 478 F. Supp. 2d at 793 (“Because most ISPs offer filtering products, a parent does not have to do anything to obtain a filter other than to activate it through the ISP’s Web site or to call the ISP.”).

⁵⁴⁵ See *Gonzales*, 478 F. Supp. 2d at 793 (“AOL’s filter is now even available for free to anyone who wants to use it, even non-AOL subscribers.”).

⁵⁴⁶ See *Gonzales*, 478 F. Supp. 2d at 793 (“Non-ISP filtering products vary in cost, ranging from approximately \$20 to \$60.”).

⁵⁴⁷ See GetNetWise Tools for Families, <http://kids.getnetwise.org/tools/>. See CDT Comments at 5; PFF Comments at 75 (noting GetNetWise’s comprehensive list). See also Internet Filter Software Review 2009, <http://internet-filter-review.toptenreviews.com/> (providing side by side comparison of top ten filtering products). Many others provide information and reviews of online safety products, including Filtering Facts, <http://filteringfacts.org/filter-reviews/>, PC Magazine, <http://www.pcmag.com/category2/0,2806,1639158,00.asp>, Monitoring Software Reviews, <http://www.monitoringsoftwarereviews.org/>, and Filter Review, <http://www.filterreview.com/>; PFF Comments at 76.

⁵⁴⁸ See FOSI Comments at 5-6, 13; AT&T Comments at 5.

⁵⁴⁹ See *Gonzales*, 478 F. Supp. 2d at 795-797 (“filters generally block about 95% of sexually explicit material”).

⁵⁵⁰ See CIPA Study, Exec. Sum., Sec. V (concluding “currently available technology measures have the capacity to meet most, if not all, of [educational institutions’] needs and concerns.”); *Gonzales*, 478 F. Supp. 2d at 794 (“A study done by AOL found that 85 percent of parents are highly satisfied with their AOL Parental Control products, and that 87 percent of parents find them easy to use. Surfcontrol has also found that customer response is positive and 70 to 80 percent of their customers renew their subscriptions to Surfcontrol’s filter.”).

⁵⁵¹ See PFF Comments at 2; EFF Reply at 7 (noting that the content to be reviewed by filtering companies is vast, and much of the review is not done by humans but by automated reviews).

tools are not perfect, they have undergone significant improvements over the past ten years and parents are increasingly using them.⁵⁵² There have been a number of studies, including the COPA Report and the CIPA Review,⁵⁵³ that examined the strengths and weaknesses of different technologies and different specific solutions.

1. Software Solutions

144. Software solutions can be downloaded, installed, and implemented by parents on their home computers and networks, and used by care givers at schools and other locations. Types of software solutions include filters; white lists; and monitors, reports and time controls.

145. *Filters.* The Commission asked in the *NOI* about filtering solutions, and many commenters discuss this technology.⁵⁵⁴ Filters act as gatekeepers, controlling the flow of content.⁵⁵⁵ Filters generally follow one of three strategies: (i) blacklist: any content on the filter's list is blocked;⁵⁵⁶ (ii) white list: any content on the list is permitted;⁵⁵⁷ and (iii) dynamic: content is analyzed dynamically and in real time to determine whether it should be permitted.⁵⁵⁸ An April 2007 study by the Pew Internet & American Life Project found that 53 percent of parents of online teens have filtering software installed on the computer their child uses at home.⁵⁵⁹

⁵⁵² See Industry and Public Interest Groups Joint Comments at 13-14; FOSI Comments at 5-6.

⁵⁵³ See CIPA Review Sec. I.A. ("Even the most sophisticated and current technology tools are not one hundred percent effective.") and Sec. II.A. (exploring how filtering technology both overblocks – blocks content that should be permitted – and underblocks – fails to block content that should have been blocked).

⁵⁵⁴ See *NOI*, 24 FCC Rcd at 3358, ¶ 39; see Industry and Public Interest Groups Joint Comments at 5; Advertisers Comments at 4; AT&T Comments at 9; Comcast Comments at 5; Cox Comments at 2; Microsoft Comments at 7; NCTA Comments at 12; USTelecom Comments at 7; Verizon Comments at 9; Google Comments at 5; CFIRS Comments at 2; PFF Comments at 7.

⁵⁵⁵ See PFF Comments at 73; *Mukasey*, 534 F.3d at 199; *Gonzales*, 478 F. Supp. 2d at 789; COPA Report, Sec. II.B.

⁵⁵⁶ See Microsoft Comments at 7; *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d at 790 ("Black lists are lists of URLs or Internet Protocol ("IP") addresses that a filtering company has determined lead to content that contains the type of materials its filter is designed to block."); see also COPA Report, Sec. II.B. Filtering/Blocking.

⁵⁵⁷ See PFF Comments at 82-84; *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d at 790 ("White lists are lists of URLs or IP addresses that a filtering company has determined do not lead to any content its filter is designed to block, and, thus, should never be blocked. A very restrictive filter, like a 'walled garden' filter, might block all URLs except those included on a white list.").

⁵⁵⁸ See *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d at 790 (stating that "dynamic filters analyze the words on the page, the metadata, the file names for images, the URLs, the links on a page, the size of images, the formatting of the page, and other statistical pattern recognition features, such as the spatial patterns between certain words and images, which can often help filters categorize content even if the actual words are not recognized").

⁵⁵⁹ See Pew Internet and American Life Project, *Teens, Privacy and Online Social Networks*, April 2007, at v, available at http://www.pewinternet.org/~media/Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf ("2007 Pew Study"). A March 2005 study by the Pew Internet & American Life Project found that 54 percent of parents of online teens have a filter installed on their home computer, up from 41 percent in December 2000. See Pew Internet and American Life Project, *Protecting Teens Online*, March 17, 2005, at 7-8, available at http://www.pewinternet.org/~media/Files/Reports/2005/PIP_Filters_Report.pdf.pdf ("2005 Pew Study"). The questions regarding filtering were asked differently in the 2005 and 2007 studies, thus they cannot be directly compared. *2007 Pew Study* at v n.1.

146. As noted in the *NOI*, the list of what is blocked (or permitted) may be generated through an automated analysis, human review, or by user options.⁵⁶⁰ Individuals can select different blocking services that may block based on different criteria, permitting parents to select a service that addresses their concerns.⁵⁶¹ Most software products allow parents to configure the software further to block the type of content to which the parent objects. In addition, filtering software will often permit the parent to add specific sites that they desire to be blocked.⁵⁶² Frequently, different accounts can be created for different children in a household, with appropriate settings for each.⁵⁶³ The list of blocked (or permitted) content may be updated regularly by the filtering service or by a third party service that reviews Internet content. Generally filters give parents the ability to use a password to turn off the filters when desired.⁵⁶⁴

147. We recognize that filtering technology has its limitations. There is a wide body of literature on the limitations of filters.⁵⁶⁵ The amount of content on the Internet is vast, making it difficult for humans to review each site.⁵⁶⁶ Filtering technology both overblocks (blocks access to sites that should otherwise be accessible) and underblocks content (permits access to sites that should be accessible).⁵⁶⁷

148. While online parental controls continue to improve and are able to inform parents when children attempt to tamper with or alter the settings,⁵⁶⁸ children can still circumvent them by moving to an unfiltered device, moving to another location without filters, using a proxy server, or accessing websites that create ways to bypass content filters.⁵⁶⁹ Filters are not generally restricted to one type of Internet application or one type of content, such as video or audio programming. Instead, generally,

⁵⁶⁰ See *NOI*, 24 FCC Rcd at 3358, ¶ 39.

⁵⁶¹ See FOSI Comments at 6.

⁵⁶² See PFF Comments at 73; AT&T Comments at 9; Comcast Comments at 5; NCTA Comments at 12-13. See also *Gonzales*, 478 F. Supp. 2d at 790, 792.

⁵⁶³ See PFF Comments at 79-81; Microsoft Comments at 7.

⁵⁶⁴ See COPA Report, Sec. II.B; see also CSTB Report, p. 6-7; GetNetWise Tools Filtering Out Sexually Explicit Content, <http://kids.getnetwise.org/tools/blocksex>.

⁵⁶⁵ See PFF Comments at 2-4; see also COPA Report, Sec. II.B. Filtering/Blocking (discussing strengths and weaknesses of filtering technology); Nancy Kranich, "Why Filters Won't Protect Children or Adults," Library Administration and Management, Vol. 18, No. 1, Winter 2004, <http://www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/whyfilterswontprotect.cfm>; *REPORT: See No Evil: How Internet Filters Affect the Search for Online Health Information*, Kaiser Family Foundation (Dec. 13, 2002), <http://www.kff.org/entmedia/20021210a-index.cfm>; *Internet Blocking in Public School*, EFF (Sept. 9, 2002), http://w2.eff.org/Censorship/Censorware/net_block_report/.

⁵⁶⁶ See EFF Reply at 7; NAS Report at 6 (stating that "the volume on the Internet is so large that it is impractical for human beings to evaluate every discrete piece of information for inappropriateness").

⁵⁶⁷ See CIPA Study, Sec. II.A & B (noting that "the technology measures also sometimes block online educational content sought by teachers."); NAS Report at 10 (discussing limitations of technology).

⁵⁶⁸ See *Gonzales*, 478 F. Supp. 2d at 795.

⁵⁶⁹ See Tom A. Peter, "Internet Filters Block Porn, But Not Savvy Kids," *Christian Science Monitor*, April 11, 2007, <http://www.csmonitor.com/2007/0411/p13s02-lihc.htm>; see also NAS Report at 11-12 ("Technology can pose barriers that are sufficient to keep those who are not strongly motivated from finding their way to inappropriate material or experiences. Further, it can help to prevent inadvertent exposure to such materials. But, as most parents and teachers noted in their comments to the committee, those who really want to have access to inappropriate sexually explicit materials will find a way to get them.").

filters are designed to work on any application or content with which a child might interact, including website visits, e-mail, instant messaging, websites visited, chat rooms, and other activities.⁵⁷⁰

149. Pursuant to Section 2(b)(3) of the Act, the *NOI* specifically asked about advanced blocking technologies that “can filter language based upon information in closed captioning.”⁵⁷¹ Broadcast TV closed captioning is not required for Internet video services and is generally not available. Some services offer video producers a closed captioning feature, but it is not based on the same standards as broadcast TV closed captioning.⁵⁷² Because several different captioning technologies are used on the Internet, solutions based on filtering closed captioning would have to be adapted to work for different Internet content sources in order to be effective.

150. *White Lists.* The Commission also asked in the *NOI* about child safe zones that “white list” safe content and block out unwanted content. The Commission asked whether parents know about this option and find it effective.⁵⁷³ PFF comments that child friendly applications are available on the market that allow children to do only things that are safe or approved by parents.⁵⁷⁴ These include web browsers that permit children to access only content within a walled garden or on a white list, browsers with filtering technology built in, and messaging programs that permit children to message and e-mail only individuals added to the address book by the parent.⁵⁷⁵ Examples of such applications include Firefox’s Glubble, which, once loaded, locks the Firefox browser so that a password is required before a user can access the Internet. Parents can then establish a user account for their children that allows them access only to a set of prescreened, kid-friendly websites.⁵⁷⁶ Other video applications have been designed specifically for children, such as the Kideo Player and Totlol.com.⁵⁷⁷

151. *Monitors, Reports, and Time Controls.* The Commission asked in the *NOI* about monitoring and recording devices.⁵⁷⁸ Solutions that commenters mention include tools that can monitor a child’s activities, deny access to certain applications or pieces of hardware (e.g., a webcam), report to

⁵⁷⁰ See AT&T Comments at 9; PFF Comments at 73; Verizon Comments at 9.

⁵⁷¹ *NOI*, 24 FCC Rcd at 3352, ¶ 24 (quoting Child Safe Viewing Act at Section 2(b)(3)).

⁵⁷² See *New Captions Feature for Videos*, YouTube Blog (Aug. 28, 2009), http://www.youtube.com/blog?gl=GB&hl=en-GB&entry=7RN6iHLHX_w (enabling a feature that permits, but does not require, video producers to add captioning to their videos); Hulu – Support, http://www.hulu.com/support/content_faq (“The closed-captioning data that’s used for broadcast TV isn’t easily translated for online use, so we’re investigating alternative solutions to boost our closed-captioning coverage.”). See also TVGuardian Frequently Asked Questions, <http://tvguardian.com/gshell.php?page=FAQ&PHPSESSID=86cdfbdd52e288ad79b69695a8b82e10> (describing TVGuardian as a solution that filters based on closed captioning from TV and DVDs).

⁵⁷³ See *NOI*, 24 FCC Rcd at 3359, ¶ 41.

⁵⁷⁴ See PFF Comments at 82-84. See also *Gonzales*, 478 F. Supp. 2d at 790.

⁵⁷⁵ See PFF Comments at 82-84. See also Advertisers Comments at 4; Comcast Comments at 5; Microsoft Comments at 7; 9.

⁵⁷⁶ See PFF Comments at 82.

⁵⁷⁷ Kideo Player, <http://www.kideoplayer.com/>, describes itself as a “A fun and safe way to ‘channel surf’ YouTube.” Totlol – Video for Kids, Babies, Toddlers, Pre and School Kids, Tweens and Parents, <http://www.totlol.com/>, describes itself as “a video website designed specifically for children. It is community moderated. It is constantly growing. It is powered by YouTube.”

⁵⁷⁸ See *NOI*, 24 FCC Rcd at 3359-60, ¶ 41.

the parent on what the child has done online, and limit time on the computer.⁵⁷⁹ Monitors can record the specific addresses of pages visited by children; thus, in the case of a video service like YouTube, parents can know specifically what videos have been watched.⁵⁸⁰ Time control software can control how much time a child is online, and when a child is online.⁵⁸¹ Each member of a family can have a separate account that is configured according to his or her needs.⁵⁸² Microsoft notes that such features are built into Windows Vista and reports that they will be included in Windows 7.⁵⁸³ These features are also built into Apple OS X.⁵⁸⁴ An April 2007 study by the Pew Internet & American Life Project found that 45 percent of parents of online teens have monitoring software that records what their children do online.⁵⁸⁵

152. While these tools can be very useful to caregivers, they too have their limitations. The COPA Commission observed:

Monitoring and time-limiting technologies can be effective when used in the home because they influence children's activities and require involvement of parents. These technologies can be effective for email and other non-Web communication, and for access to global content. Monitoring and time-limiting technologies encourage greater parental involvement in the child's online experience; however, because a parent learns of activities only after the fact, effectiveness in reducing accidental access to harmful to minors materials may be limited.⁵⁸⁶

2. Network Service Provider Solutions

153. Many commenters provide information on how network service providers help promote online safety. Many network service providers include parental control software in the materials provided to new subscribers, in addition to making this software available on their websites.⁵⁸⁷ They

⁵⁷⁹ See FOSI Comments at 5-6; AT&T Comments at 9; Comcast Comments at 5; Cox Comments at 5; Verizon Comments at 9; PFF Comments at 74. According to GetNetWise, "monitoring tools inform adults about a child's online activity without necessarily limiting access. Some of these tools simply record the addresses of Web sites that a child has visited. Others provide a warning message to a child if he/she visits an inappropriate site." GetNetWise, *Tools that Monitor Computer Activity*, <http://kids.getnetwise.org/tools/monitors> (providing a list of available monitoring applications). See also *Gonzales*, 478 F. Supp. 2d at 792; NAS Report at 11; COPA Report, Sec. II.F.15 (discussing monitoring and time-limiting technologies as "Use (typically at the PC) of software that creates logs showing details of a child's online activities and, optionally, enforces rules regarding the amount of time that may be spent online. Such systems may track both web use and email and instant messaging activities.").

⁵⁸⁰ See PFF Comments at 73, 75; AT&T Comments at 9; Verizon Comments at 9. See also *YouTube and Your Teen*, <http://www.common sense media.org/youtube-and-your-teen>. See also Marian Merritt, *YouTube is Top Kid Destination; How to Enjoy it Safely*, (Jun. 24, 2009), <http://community.norton.com/t5/Ask-Marian/YouTube-Is-Top-Kid-Destination-How-To-Enjoy-It-Safely/ba-p/111256> ("OnlineFamily.Norton will report on the videos that children are watching or searching for.").

⁵⁸¹ See PFF Comments at 81; AT&T Comments at 9; Comcast Comment at 5; Microsoft Comments at 7.

⁵⁸² See Microsoft Comments at 7; PFF Comments at 81; NCTA Comments at 13.

⁵⁸³ See Microsoft Comments at 7.

⁵⁸⁴ See Microsoft Comments at 7; PFF Comments at 81.

⁵⁸⁵ See *2007 Pew Study* at v.

⁵⁸⁶ COPA Report, Sec. II.F.15.

⁵⁸⁷ See PFF Comments at 77; NCTA Comments at 12-13; USTelecom Comments at 7; FOSI Comments at 7; AT&T Comments at 9; Comcast Comments at 5; Verizon Comments at 10. See also GetNetWise *How ISPs are Helping*, <http://kids.getnetwise.org/tools/ispoptions>. See also 47 U.S.C. § 230(d) ("A provider of interactive computer service (continued....)

provide educational material on their websites and host educational events.⁵⁸⁸ Network service providers also support the work of online safety nonprofit organizations.⁵⁸⁹ Many of these network service providers have participated in government working groups such as NTIA's OSTWG⁵⁹⁰ and the COPA Commission,⁵⁹¹ as well as private sector efforts such as the Internet Safety Technical Task Force ("ISTTF") at the Berkman Center.⁵⁹²

3. Content Service Provider Solutions

154. Commenters discuss content service providers' efforts to promote online safety, which provide additional parental tools.⁵⁹³ Content service providers offer a series of solutions, many of which also increase the parents' ability to make their children's online experiences positive.

155. *Acceptable Use Policies.* The Commission asked in the *NOI* about acceptable use and "takedown" policies.⁵⁹⁴ Commenters explain that content hosting sites and services may have acceptable use policies and terms of service that indicate what content is acceptable and when unacceptable content will be taken down.⁵⁹⁵ If content is found that violates the acceptable use policy, the service may take it down from the site and may terminate the account of the individual that posted it. Sites may actively review their content, or they may review the content when notified by a visitor that the content is problematic.

156. *Labels.* The *NOI* also asked about labeling capabilities.⁵⁹⁶ Content creators can label
(Continued from previous page) _____
shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors."); Internet Tax Freedom Act, Sec. 1101(f)(1), codified at 47 U.S.C. § 151 nt. (Internet Tax Freedom Act "shall also not apply with respect to an Internet access provider, unless, at the time of entering into an agreement with a customer for the provision of Internet access services, such provider offers such customer (either for a fee or at no charge) screening software that is designed to permit the customer to limit access to material on the Internet that is harmful to minors.").

⁵⁸⁸ See AT&T Comments at 9-10; NCTA Comments at 13-14; Cox Comments at 2; Comcast Comments at 8; FOSI Comments at 10-11. See also AT&T Parental Controls and Online Safety, <http://www.att.com/gen/landing-pages?pid=6456>; *Power to Learn: a service of Cablevision*, Internet Smarts, http://www.powertolearn.com/internet_smarts/index.shtml; Charter Communications, <http://www.charter.com/Visitors/NonProducts.aspx?NonProductItem=65>; Comcast.net Security Channel, <http://security.comcast.net/>; COX Take Charge Smart Choices for your Cox Digital Home, <http://www.cox.com/takecharge/>; Verizon Parental Control Center, <http://parentalcenter.verizon.radialpoint.net>

⁵⁸⁹ See USTelecom Comments at 8-9; <http://www.cox.com/takecharge/>; Sprint Comments at 3.

⁵⁹⁰ See USTelecom Comments at 8-9

⁵⁹¹ See COPA Commission Commissioners, <http://www.copacommission.org/commission/commissioners.shtml>.

⁵⁹² See CDT Comments at 15; Internet Safety Technical Task Force, Members, Berkman Center, <http://cyber.law.harvard.edu/research/isttf/members>.

⁵⁹³ See, e.g., AT&T Comments at 9-10; Google Comments at 6.

⁵⁹⁴ See *NOI*, 24 FCC Rcd at 3360, ¶ 41.

⁵⁹⁵ See Google Comments at 4, 6. See also YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines. See, e.g., Flickr Community Guidelines, <http://www.flickr.com/guidelines.gne>; Second Life Safety Tips for Teens and Parents, <http://secondlife.com/policy/security/teensafety.php>.

⁵⁹⁶ See *NOI*, 24 FCC Rcd at 3359, ¶ 40.

their content,⁵⁹⁷ providing semantic information about the content or a reference number for the content.⁵⁹⁸ This reference number can be used to look up the content in a database and determine whether it is appropriate.⁵⁹⁹ A number of hosting sites require content uploaders to identify their content.⁶⁰⁰

157. *Flags and Tags.* An alternative strategy that commenters discuss is to have the community that interacts with the content flag or tag the content.⁶⁰¹ The amount of video content being uploaded to the Internet is more than any hosting service or filtering service can manually review for compliance with its acceptable use policy. By “crowdsourcing”⁶⁰² the review of content to the community that interacts with the content, services can have many people looking at large amounts of content, increasing the effectiveness of the acceptable use policy.⁶⁰³ When problematic content is encountered, anyone viewing the content can click on the flag and identify how the content in question violates the site’s acceptable use policy. When a video receives a certain number of flags, it may come to the attention of the hosting service, which may then review the video and decide whether it comports with the guidelines and whether it should be taken down. A number of video hosting sites follow this approach.⁶⁰⁴

158. Another strategy is for the interacting community to tag content. Tagging is not directed so much at identifying *objectionable* content, as it is directed at simply identifying content. Individuals

⁵⁹⁷ The terms “tags,” “labels,” and “flags” are used differently by different sites, and are somewhat interchangeable.

⁵⁹⁸ See W3C Semantic Web Activity, <http://www.w3.org/2001/sw/> (W3C is the standards body for the World Wide Web).

⁵⁹⁹ See, e.g., PFF Comments at 95 (The Family Online Safety Institute is developing the Internet Content Rating Association (ICRA) which “is helping to develop improved Internet filtering systems through comprehensive website labeling and metadata tagging.”); See also Website Reviews Kids Websites, <http://www.common sense media.org/website-reviews>. The COPA Report described labeling as “[v]oluntary action by content sources to indicate that a site or particular content meets a particular standard or fits a particular category. The ‘label’ can take the form of a metatag, or entry into a database listing, or display of a seal. The use of a label may be audited.” COPA Report, Sec. II.C.6. At the time, the COPA Commission noted that “labeling” had not been widely adopted by publishers. *Id.*

⁶⁰⁰ See Promoting Videos: Tags definitions, YouTube, <http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=55769>; YouTube Glossary: Category, <http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=94328>. One method of labeling content could be through digital watermarks. Digimarc Corporation Comments at 5-6; Digimarc Corporation at 5-6. Digital watermarking is discussed above.

⁶⁰¹ See PFF Comments at 98; Google Comments at 6.

⁶⁰² See Jeff Howe, *The Rise of Crowdsourcing*, WIRED (June 2006), <http://www.wired.com/wired/archive/14.06/crowds.html>.

⁶⁰³ See PFF Comments at 95.

⁶⁰⁴ See Google Comments at 6; PFF Comments at 98 (noting efforts of YouTube, Flickr, and MySpace). YouTube’s efforts will be discussed in greater detail below. See, e.g., Flickr: Help: Content Filters, <http://www.flickr.com/help/filters/#258>; Facebook Facebook Safety, <http://www.facebook.com/help/search.php?hq=report#/safety/> (“You can help Facebook by notifying us of any nudity or pornography, or harassment or unwelcome contact by clicking on the “Report” link located on pages throughout the site.”); Vimeo FAQ, How Do I Report Abuse, <http://www.vimeo.com/help/faq>; Google Webpage Removal Request Tool, <https://www.google.com/webmasters/tools/removals?pli=1> (offering the option to identify “inappropriate webpage or image that appears in our SafeSearch filtered results.”).

interacting with content can tag that content as worthy of reading and identify what type of content it is.⁶⁰⁵ They can tag the content with keywords that, like labels, help to identify the content. For example, someone may tag a photo with the names of the individuals in the photo and where the photo was taken. Or one might tag a news article with keywords that identify the topics of the article. Like labels, tags can be used to help find (or avoid) the type of content for which individuals are looking.⁶⁰⁶

159. *Safe Search.* Several search engines provide settings that enable individuals to set the search engine to a restrictive setting that filters the responses returned. Many services such as Google, Flickr, and AOL provide safesearch features.⁶⁰⁷ According to Google, “[m]any users prefer not to have adult sites included in search results (especially if children use the computer). Google’s SafeSearch screens for sites that contain explicit sexual content and deletes them from your search results. No filter is 100 percent accurate, but SafeSearch should eliminate most inappropriate material.”⁶⁰⁸

160. *Age Verification.* The NOI also asked about age verification solutions.⁶⁰⁹ Age verification solutions require the user to verify his or her age, sometimes by using a credit card number or an independently issued identification.⁶¹⁰ Commenters note that it is generally not effective as a tool in online environments where minors are likely to participate.⁶¹¹

161. *Tools Used by Specific Online Video Services.* As noted above, the diversity of sources for online video and audio is almost infinite. There are, however, certain notable large players. According to Nielsen Online,⁶¹² in April 2009 the top five online video sites as measured by streams were YouTube (58.1 percent), Hulu (3.9 percent), Yahoo! (2.2 percent), Fox Interactive (2.1 percent), and Nickelodeon (1.9 percent). YouTube stands out as one of the most popular sites on the web (all websites included),⁶¹³ most popular video site, and most popular site among children.⁶¹⁴ The second

⁶⁰⁵ See PFF Comments at 95.

⁶⁰⁶ There are many popular tagging services that inform participants in a community regarding what other members of the community have found interesting and worth reading. See, e.g., Delicious, <http://delicious.com/>; reddit.com: what’s new online, <http://www.reddit.com/>; Digg, <http://digg.com/>. See also *Social Networks and Bookmarking*, Pew Internet & American Life Project (Jan. 24, 2005), <http://www.pewinternet.org/PPF/p/1035/pipcomments.asp>.

⁶⁰⁷ See FOSI Comments at 8. See also Google SafeSearch, <http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=35892>; Flickr: Help: Content Filters: What is Safesearch, <http://www.flickr.com/help/filters/#249>; AOL SafeSearch, <http://about-search.aol.com/>.

⁶⁰⁸ See <http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=35892>.

⁶⁰⁹ See NOI, 24 FCC Rcd at 3360, ¶ 41.

⁶¹⁰ See COPA Report at II.D.

⁶¹¹ See CDT Comments at 13; PFF Comments at 90. See also *Mukasey*, 534 F.3d at 195; *Gonzales*, 478 F. Supp. 2d at 800 (finding that “there is no evidence of age verification service or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users” and “nor is there evidence of such service or products that can effectively prevent access to Web pages by a minor”); COPA Report, Sec. II.D.8.

⁶¹² See *YouTube Maintains Top Rankings by Total Streams and Hulu Grows 490% Year-Over-Year, According to Nielsen Online*, (May 14, 2009), http://www.nielsen-online.com/pr/090514_2.pdf.

⁶¹³ See *comScore Media Metrix Ranks Top 50 US Web Properties for May 2009*, (Jun. 23, 2009), <http://www.comscore.com/content/download/2589/27981/file/comScore%20Media%20Metrix%20Ranks%20Top%2050%20U.S.%20Web%20Properties%20for%20May%202009.pdf>

⁶¹⁴ See Mariam Merritt, *YouTube is Top Kid Destination; Hot to Enjoy it Safely*, (Jun. 24, 2009), <http://community.norton.com/t5/Ask-Marian/YouTube-Is-Top-Kid-Destination-How-To-Enjoy-It-Safely/ba-p/111256>

most popular video site has only 4 percent market share, demonstrating how profuse the offering of video sites is.⁶¹⁵ The top audio download services include iTunes, Amazon, Napster, and others.⁶¹⁶ The amount of online video and audio content continues to grow.⁶¹⁷ We review below some of the solutions online video services have employed in order to promote online safety.

162. *YouTube*. YouTube is a video hosting site where anyone anywhere can upload short videos to his account and share them with the world.⁶¹⁸ YouTube has enabled a number of safety features, leveraging community review and input.⁶¹⁹ YouTube uses flags and Community Guidelines.⁶²⁰ Each video page has a button under the video called “flag.” To use the flags, an individual must sign into the YouTube service, click on “Flag”, and choose among six categories: (1) sexual content, (2) violent or repulsive content, (3) hateful or abusive content, (4) harmful dangerous acts, (5) spam, and (6) infringes my rights.⁶²¹ In addition, YouTube has Community Guidelines that prohibit pornography or sexually explicit content, animal abuse, drug abuse, under-age drinking and smoking, bomb making, graphic or gratuitous violence, shock or gross out material, copyright violations, hate speech, predatory behavior, stalking, threats, and spam. YouTube states that content uploaders who are found to have violated the YouTube Community Standards once will be given a warning, and a strike will be placed on the account that lasts six months. If in that six months the uploader receives a second strike, the account will be temporarily disabled. If no further strikes are received during the period, the account will be restored. If a third strike is received, the account will be terminated.⁶²²

163. YouTube promises to enforce its Community Guidelines:

YouTube staff review flagged videos 24 hours a day, seven days a week to determine whether they violate our Community Guidelines. When they do, we remove them. Sometimes a video

⁶¹⁵ See Chris Anderson, *The Long Tail*, Wired Magazine (Oct. 2004), <http://www.wired.com/wired/archive/12.10/tail.html>.

⁶¹⁶ See Eliot Van Buskirk, *Zune Eats Creative's Lunch, Grapping 4 Percent of MP3 Player Market*, WIRED (May 12, 2008), http://www.wired.com/listening_post/2008/05/ipod-loses-mark/ (as of Q108 listing Apples market share of MP3 players as 71%, SanDisk 11%, Creative 2%, and Microsoft 4%); Sam Costello, *Top 4 Music Download Services*, About.com, http://ipod.about.com/od/downloadservicereviews/tp/top_download_services.htm.

⁶¹⁷ See *Online TV Grows in Popularity*, (Sept. 4, 2008), <http://www.tnsglobal.com/news/news-CA47962D13C744DD9A4BEDCAA07AF42E.aspx>; Greg Sandoval, *Study: Web-video viewers to top 1 billion by 2013*, CNET (May 27, 2008), http://news.cnet.com/8301-10784_3-9952659-7.html?part=rss&subj=news&tag=2547-1_3-0-20; Ben Worthen, *Cisco Says Internet Video to Explode*, Wall Street Journal (Jun. 9, 2009), <http://blogs.wsj.com/digits/2009/06/09/cisco-says-internet-video-to-explode/>.

⁶¹⁸ See YouTube Company History, <http://www.youtube.com/t/about>.

⁶¹⁹ See *Safety, education, and empowerment on YouTube*, The Official Google Blog (Dec. 11, 2008), <http://googleblog.blogspot.com/2008/12/safety-education-and-empowerment-on.html>.

⁶²⁰ See http://www.youtube.com/t/community_guidelines.

⁶²¹ Each of those categories has several subcategories. For instance, sexual content is broken down into (a) graphic sexual activity, (b) nudity, (c) suggestive, but without nudity, and (d) other sexual content. See http://www.youtube.com/t/community_guidelines.

⁶²² See *Accounts and Policies: General Policy Enforcement Information*, <http://help.youtube.com/support/youtube/bin/answer.py?hl=en&answer=92486>; *Flagging on YouTube: The Basics*, <http://www.youtube.com/watch?v=ZA22WSVICZA/>. See Marian Merritt, *YouTube is Top Kid Destination; How to Enjoy it Safely*, (June 24, 2009), <http://community.norton.com/t5/Ask-Marian/YouTube-Is-Top-Kid-Destination-How-To-Enjoy-It-Safely/ba-p/111256>.

doesn't violate our Community Guidelines, but may not be appropriate for everyone. These videos may be age-restricted. Accounts are penalized for Community Guidelines violations and serious or repeated violations can lead to account termination. If your account is terminated, you won't be allowed to create any new accounts.⁶²³

164. Each video posted to YouTube can have comments posted by the community, discussing the video. Individuals who uploaded videos to their accounts can moderate the comments posted at their videos, requiring pre-approval before any comments are posted⁶²⁴ or deleting offensive comments,⁶²⁵ block users whose comments they consider inappropriate,⁶²⁶ or permit only friends to post comments to their videos.⁶²⁷

165. Online safety organizations encourage parents to go to YouTube and become familiar with the content that their children are accessing.⁶²⁸ Parents can also use monitoring software, discussed above, to receive reports about which YouTube videos a child has watched.

166. *Other Video Services.* Other online video and audio services also include safety features. Yahoo! Video, which permits individuals to upload their own videos, follows a strategy similar to YouTube's, with guidelines and the ability of the community to flag offensive content.⁶²⁹ Hulu streams TV shows and movies and offers parental controls that will block minors' access to mature content.⁶³⁰ iTunes, which enables individuals to download music and shows on demand to be enjoyed on a computer, TV, or handheld device, offers a feature whereby parents can block the downloading of songs or videos with explicit language and sends a receipt to the email on the account whenever content is purchased.⁶³¹

167. As commenters note, there are also a number of video and audio sites that are walled gardens, providing only family friendly content.⁶³² Examples of child safe zones include Yahoo! Kids

⁶²³ YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines.

⁶²⁴ See Getting Started: Comments on my videos, <http://www.google.com/support/youtube/bin/answer.py?answer=58123>.

⁶²⁵ See Learn More: Removing comments on my videos, <http://www.google.com/support/youtube/bin/answer.py?answer=56112>.

⁶²⁶ See Abusive Users: Blocking users, <http://help.youtube.com/support/youtube/bin/answer.py?answer=56113>.

⁶²⁷ See Learn More: "Friends-only" messages, <http://www.google.com/support/youtube/bin/answer.py?answer=67057>.

⁶²⁸ See Marian Merritt, *YouTube is Top Kid Destination; How to Enjoy it Safely*, (Jun. 24, 2009), <http://community.norton.com/t5/Ask-Marian/YouTube-Is-Top-Kid-Destination-How-To-Enjoy-It-Safely/ba-p/111256>; *YouTube and Your Teen*, <http://www.common sense media.org/youtube-and-your-teen>.

⁶²⁹ See Guidelines, <http://video.yahoo.com/guidelines>.

⁶³⁰ See CDT Comments at 10. Hulu Support, <http://www.hulu.com/support/account> ("Parental Controls Users are required to be logged into an account and over the age of 18 in order to view mature content (films rated R, TV-MA shows) on Hulu. Unfortunately, we do not have a setting that allows for more customized parental controls at this time. The best suggestion we can offer is to log out of your Hulu account while watching with younger children; this will block mature content.").

⁶³¹ See CDT Comments at 10; PFF Comments at 45; *iTunes: Using Parental Controls*, <http://support.apple.com/kb/HT1904>.

⁶³² See, e.g., PFF Comments at 88. See also COPA Report, Sec. II.F.14.

(kids.yahoo.com), PBS Kids (pbskids.org), Nickelodeon (nick.com), Cartoon Network (cartoonnetwork.com), TV Disney.com (home.disney.go.com), and .Kids.US.⁶³³

4. Parent and Care Giver Driven Solutions

168. Outside of any technical solution, the record in this proceeding suggests that there are a series of best practices that parents and all adult care givers can follow in order to promote children's safety.⁶³⁴ These generally include education, acceptable use policies, and supervision.

169. *Education.* The *NOI* asked what role education should play in protecting children from objectionable content, especially given the ways in which blocking technology may be circumvented.⁶³⁵ Commenters,⁶³⁶ previous reports,⁶³⁷ experts, case law, and government officials agree that the key to online safety is education. Children need to be educated regarding Internet safety and media literacy. The National Academy of Sciences states that “[w]hile both technology and public policy have important roles to play, social and educational strategies to develop in minors an ethic of responsible choice and the skills to effectuate these choices and to cope with exposure are foundational to protecting children.”⁶³⁸

170. Education is also needed for parents, teachers, and care givers.⁶³⁹ As the National Academies of Sciences stated, “[a]dults must be taught to teach children how to make good choices on the Internet. They must be willing to engage in sometimes-difficult conversations.”⁶⁴⁰ Educational materials and resources are increasingly available online,⁶⁴¹ including educational materials dealing with video and audio.⁶⁴² Internet Service Providers are also aggregating and making available to their subscribers educational materials.⁶⁴³

⁶³³ See .Kids.US – Play, Learn, Surf, <http://www.kids.us/>. See also COPA Report, Sec. II.E.10 & 11. Some parties noted that .kids.us has had limited success. CDT Comments at 12.

⁶³⁴ See, e.g., AT&T Comments at 6, FOSI Comments at 10.

⁶³⁵ See *NOI*, 24 FCC Rcd at 3361, ¶ 43.

⁶³⁶ See CDT Comments at 14; FOSI Comments at 12.

⁶³⁷ See, e.g., COPA Report, Sec. II.A.2 (“As families are the first line of defense in raising and protecting children, education programs can be highly effective in giving caregivers needed information about online risks and protection methods, and access to technologies and ways to get help.”).

⁶³⁸ NAS Report at 12. See also Byron Review at 2-4; NAS Report at 9.

⁶³⁹ See ISSTF Report at 6; CIPA Study at Sec. IV.A (recommending parent and school staff education).

⁶⁴⁰ NAS Report at 10.

⁶⁴¹ See NCTA Comments at 13-14; Verizon Comments at 10; Google Comments at 6. See also CIPA Study at Sec. IV.A (recommending Child Media Literacy education); COPA Report, Sec. II.A.2. See, e.g., *Become a Common Sense School*, <http://www.common sense media.org/schools>.

⁶⁴² See, e.g., *Top 10 Safety Tips for Video-Sharing* (Sept. 3, 2007), <http://www.connectsafely.org/Safety-Tips/top-10-safety-tips-for-video-sharing.html> (“Many kids today are video-literate – able to communicate in a medium once reserved for highly trained professionals with expensive equipment.”).

⁶⁴³ See Verizon Comments at 10; Cox Comments at 7; NCTA Comments at 13-14. See also COPA Report, Sec. II.A.1. Online Information Resources (“Internet companies have made substantial efforts to make these online information resources available.”) The COPA Report states, “While not directly preventing access to harmful to minors materials, online information resources are essential to protecting children, as they can effectively provide access to technologies, information for families online, and hotlines to reach and report to authorities. Easily (continued....)

171. AT&T observes that the government has an important role in providing educational opportunities and resources.⁶⁴⁴ The FTC has operated, in partnership with several government agencies, the educational project OnGuard Online.⁶⁴⁵ In 2008, the Broadband Data Improvement Act directed the FTC to engage in a public awareness campaign “to promote the safe use of the Internet by children.”⁶⁴⁶ Individual agencies also have their own separate educational programs.⁶⁴⁷

172. Internet safety courses are increasingly being taught in schools,⁶⁴⁸ and several states have online safety as a part of their required school curriculum.⁶⁴⁹ The Broadband Data Improvement Act also amended the Children’s Internet Protection Act (“CIPA”) requirements for schools receiving funding from the Commission’s universal service fund program known as the E-rate program. Section 215 of the Broadband Data Improvement Act now requires participating schools to educate “minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.”⁶⁵⁰

173. *Acceptable Use Policies.* Acceptable use policies, in which expectations regarding Internet use are established in the home, can be a part of the educational experience between children and parents or caregivers. According to a study of children aged 8-18 with a computer in their home, 28 percent reported that they have rules about how much time they spend on the computer, 32 percent said there are explicit rules about what they can do on the computer, and 30 percent said their parents usually know what Web sites they access.⁶⁵¹ These acceptable use policies can help educate children regarding the limits of safe and appropriate behavior, and when they might stray into risky areas. More formal, institutional acceptable use policies, such as the acceptable use policies drafted by educational institutions and posted near computers, serve a similar purpose. Model acceptable use policies are available online.⁶⁵²

(Continued from previous page) _____
 accessible online, the “one-click-away” approach is well-designed to make sure that notice of available technologies is provided at common points of entry to the Internet.” COPA Report, Sec. II.A.1.

⁶⁴⁴ See AT&T Comments at 5-6 (contending that federal, state and local governments “should allocate resources to better educate parents and children regarding the risks children face online and the tools available to protect them”). See also Byron Review at 8 (recommending “a properly funded public information and awareness campaign”).

⁶⁴⁵ See OnGuard Online, <http://www.onguardonline.gov/>.

⁶⁴⁶ Broadband Data Improvement Act, § 212, codified at 15 U.S.C. § 6552.

⁶⁴⁷ See, e.g., ED Technology Internet Safety, <http://www.ed.gov/about/offices/list/os/technology/safety.html>; Project Safe Childhood, US Dept. of Justice, <http://www.projectsafefchildhood.gov/>; A Parent’s Guide to the Internet, <http://www.fbi.gov/publications/pguide/pguidee.htm>. See also FOSI Comments at 14 (“what is lacking [is] a high level of coordination and leadership” for the different agencies.); Byron Review at 8 (recommending “an authoritative ‘one stop shop’ for child internet safety” information).

⁶⁴⁸ See NCTA Comments at 13-14; see also Byron Review at 8 (noting important role of schools in equipping children to stay safe online); ISTTF Report at 6 (recommending greater resources be allocated to schools and libraries to assist them in providing education about online safety).

⁶⁴⁹ See, e.g., VA. CODE ANN. § 22.1-70.2 (Michie 2003) (acceptable Internet use policies for public and private schools); CAL. EDUC. CODE § 51871.5 (West 2008); 105 ILL. COMP. STAT. 5/27-13.3 (2009).

⁶⁵⁰ Broadband Data Improvement Act, Sec. 215, codified as 47 U.S.C. § 254(h)(5)(B)(iii).

⁶⁵¹ See *Generation M: Media in the Lives of 8-18 Year-olds* at 17 and Appendix 3.4.

⁶⁵² See CIPA Study Sec. IV (“Most of the commenters expressed a great deal of satisfaction with the evolution and use of safety policies...”); NAS Report at 9, 235; COPA Report, Sec. II.F.16 (“Involvement of parents and institutions in expressly establishing guidelines through an acceptable use policy or family contract can have a (continued....)”).

174. *Supervision.* As FOSI observed, supervision of children is crucial.⁶⁵³ Supervision may vary. It may initially include sitting side-by-side while teaching a child online literacy,⁶⁵⁴ placing a family computer where it can be viewed by parents, occasionally reviewing social network accounts, or using software tools to monitor online usage.⁶⁵⁵ Common Sense Media offers simple supervision recommendations. For example, if you give permission to your children to upload videos, they suggest that you ask to see the videos before they are uploaded.⁶⁵⁶

VIII. UNIVERSAL STANDARDS

175. The Child Safe Viewing Act directed the Commission to consider advanced blocking technologies that “may be appropriate across a wide variety of distribution platforms” and “may be appropriate across a wide variety of devices capable of receiving video or audio programming.”⁶⁵⁷ Today, there is no single universal rating technology or system that applies across all media sectors.⁶⁵⁸ As discussed above, however, voluntary content ratings systems currently exist within each media sector – television, movies, music, video games, and the Internet – and much of the content within each sector is rated.⁶⁵⁹ In addition, a wide variety of organizations provide independent ratings for television programming, movies, music, video games, and Internet content.⁶⁶⁰

176. Some commenters argue that imposing either a mandatory advanced blocking technology or ratings standard to apply across all media platforms would be impractical and unworkable.⁶⁶¹ With respect to a technical standard, commenters note that wired, wireless, and Internet platforms differ widely in terms of their technical capabilities.⁶⁶² They assert that a single technology designed to work across platforms would by necessity have to be reduced to a lowest common denominator in terms of

(Continued from previous page) _____

significant positive impact on awareness and behavior, although they do not themselves directly reduce access by minors to harmful to minors material.”). See also Family Contract for Online Safety, <http://www.safekids.com/contract.htm>; *Using Family Contracts to Help Protect Your Kids Online*, (Oct. 21, 2006), <http://www.microsoft.com/protect/family/guidelines/contract.mspix>; *Internet Safety Plan*, <http://www.webwisekids.org/internet-safety-plan.pdf>.

⁶⁵³ See FOSI Comment at 9.

⁶⁵⁴ See also Marian Merritt, *YouTube is Top Kid Destination; How to Enjoy it Safely*, (Jun. 24, 2009), <http://community.norton.com/t5/Ask-Marian/YouTube-Is-Top-Kid-Destination-How-To-Enjoy-It-Safely/ba-p/111256> (discussing how to the YouTube features to improve the safety of your child’s experience).

⁶⁵⁵ See CIPA Study Sec. IV.A; NAS Report at 9.

⁶⁵⁶ See *YouTube and Your Teen*, <http://www.common sense media.org/youtube-and-your-teen>.

⁶⁵⁷ Child Safe Viewing Act at Section 2(b).

⁶⁵⁸ See PFF Comments at vi, 112.

⁶⁵⁹ See *id.* at 112.

⁶⁶⁰ See, e.g., CEA Comments at 7, 10; Common Sense Media Comments at 7; CMPC Comments at 8; Comcast Comments at 9; DISH Network Comments at 6; PFF Comments at 138-142; Smart Television Alliance Comments at 2.

⁶⁶¹ See, e.g., CDT Comments at 14; Industry and Public Interest Groups Joint Comments at 8-12; NAB/NCTA/MPAA Comments at 21-22.

⁶⁶² See Industry and Public Interest Groups Joint Comments at 8 (noting that there is a significant difference in capability between, for example, an in-home computing device and a small portable device). See also NAB/NCTA/MPAA Comments at 21 (noting that the interfaces and protocols used in various consumer electronics devices for accessing content on platforms vary and are not designed to handle a single blocking technology).

technical capabilities, thereby losing the greater flexibility and control currently provided by individual media platforms.⁶⁶³ Commenters also point out that a move to a single technology, whether voluntary or mandated, would stifle the drive to innovate within each platform, thus hindering the cause of empowering parents.⁶⁶⁴ While commenters generally oppose a mandated cross-platform technology, one commenter notes that particular companies or interest groups could pursue the development of such a technology and could create a niche market for a cross-platform solution.⁶⁶⁵ Several commenters urge the government to take steps to encourage industry and trade associations to work together to develop a universal parental control technology.⁶⁶⁶ As discussed above, digital watermarking is one possible technology that might provide a means of creating standards that work across multiple media platforms.⁶⁶⁷

177. With respect to a universal media rating system, some commenters argue that mandating such a rating system would require re-educating the public, which would be expensive and could result in consumer confusion.⁶⁶⁸ In addition, NAB, NCTA, and MPAA contend that media providers and consumer electronics companies would be required to install new filtering technology to accommodate the new rating standard, which would be expensive and would likely pose an issue with respect to legacy content and devices.⁶⁶⁹ Some commenters also assert that a universal ratings standard would destroy innovation by requiring a government-approved, “one-size-fits-all” approach that would result in less useful and effective ratings than those currently in use.⁶⁷⁰ Finally, commenters question how a universal rating system would be selected, pointing out that media ratings and content-labels are inherently subjective and inevitably reflect the perspectives and values of the person evaluating the content.⁶⁷¹ In addition, some commenters contend that imposition of mandatory government ratings poses significant First Amendment concerns.⁶⁷²

178. Although industry commenters in general oppose the notion of mandating universal ratings, other commenters argue that individual groups could offer a cross-platform rating scheme.⁶⁷³

⁶⁶³ See AT&T Comments at 11; NAB/NCTA/MPAA Comments at 22; Verizon Comments at 12.

⁶⁶⁴ See Industry and Public Interest Groups Joint Comments at 9; AT&T Comments at 4; CEA Comments at 2. See also DMA Comments at 12-13 (noting that the effort to develop DRM solutions across media platforms was unsuccessful, and suggesting that parental controls developed to suit specific applications would be more likely to succeed). Some commenters argue that government adoption of the V-chip led to less innovation in content blocking for broadcast television than for other media platforms. See, e.g., Industry and Public Interest Groups Joint Comments at 9; AT&T Comments at 12.

⁶⁶⁵ See Industry and Public Interest Groups Joint Comments at 10.

⁶⁶⁶ See, e.g., Common Sense Media Comments at 5; TiVo Comments at 6; CFIRS Comments at 7-8; DISH Network Comments at 8.

⁶⁶⁷ See, *supra*, section II.B.4. But see CEA Comments at 10-11 (expressing concern that digital watermarking could also be used for DRM functionality and that intellectual property licensing terms for this technology are unknown). See also TiVo Reply at 3.

⁶⁶⁸ See, e.g., NAB/NCTA/MPAA Comments at 20. See also ALEC Comments at 7.

⁶⁶⁹ See NAB/NCTA/MPAA Comments at 20.

⁶⁷⁰ See PFF Comments at vi. See also ESA Comments at 7-8.

⁶⁷¹ See NAB/NCTA/MPAA Comments at 19. See also Industry and Public Interest Groups Joint Comments at 11.

⁶⁷² See PFF Comments at 114-117; Industry and Public Interest Groups Joint Comments at 12.

⁶⁷³ See Industry and Public Interest Groups Joint Comments at 12. See also CFIRS Comments at 7.