

percent used satellite parental controls, whereas only 5 percent used the V-chip.<sup>192</sup>

58. The November 2005 Russell Research Survey commissioned by TV Watch also concluded that 66 percent of parents surveyed found cable blocking technology useful and 57 percent found satellite blocking technology useful.<sup>193</sup> Cox states that a survey it conducted in 2004 showed that 60 percent of the parents surveyed found that parental controls on cable boxes were the most valuable monitoring tool for television.<sup>194</sup>

59. Some commenters contend that the parental control devices that MVPDs provide to their subscribers are both more user-friendly than the V-chip and offer a greater variety of options in terms of monitoring children's television viewing.<sup>195</sup> Both analog and digital cable boxes allow parents to block channels and lock the settings with passwords.<sup>196</sup> Newer digital boxes offer more extensive filtering capabilities that allow programs to be blocked by rating, channel, or program title.<sup>197</sup> The current generation of digital cable set-top boxes also permits parents to set up their controls so that children are unaware that a particular channel or program is available on a particular television set.<sup>198</sup> Channels and programs on the skip channel list will not be displayed on the TV screen and in some cases can be omitted from display in the program guide.<sup>199</sup> Some boxes also allow customers to block access to an entire service, such as VOD, and allow customers to block content based on time and day.<sup>200</sup> NCTA states that cable operators are working to make these blocking capabilities easier for customers to use.<sup>201</sup>

---

<sup>192</sup> See *id.* A March 2007 Zogby poll of 1000 adults nationwide commissioned by PTC found that 11 percent of those surveyed used the V-chip or cable box parental controls. See *PTC Declares the Industry's V-Chip Education Campaign a Failure*, March 15, 2007, <http://parentstv.org/PTC/news/release/2007/0315.asp>. The study does not distinguish between the percentage of those surveyed who used the V-chip and the percentage of those surveyed who used cable box parental controls.

<sup>193</sup> See *Survey: Parents Combine Old-Fashioned TV Rules and Latest Blocking Technologies to Manage Kids' TV*, November 28, 2005, <http://www.televisionwatch.org/NewsPolls/PressReleases/PR008.html>.

<sup>194</sup> See Cox Comments at 3.

<sup>195</sup> See, e.g., DISH Network Comments at 5; CEA Comments at 7, 10; Funai Comments at 3.

<sup>196</sup> See PFF Comments at 21; DISH Network Comments at 6 (discussing password protection for satellite set-top boxes). Parents can also purchase aftermarket devices that block specific cable channels. See <http://www.familysafemedia.com/index.html>. According to NCTA, operators of cable systems serving more than 90 percent of cable customers offer free channel blocking to customers who do not otherwise have the means to block unwanted channels. See NCTA Supplemental Comments at 8. Comcast states that it will block any channel upon request and for no charge. See Comcast Comments at 3. Depending on the technology used, a channel or channels can be blocked indefinitely within the entire household or on a particular television within the household. In addition, the Communications Act mandates that cable operators block certain channels. See also 47 U.S.C. § 560(a) ("Upon request by a cable service subscriber, a cable operator shall, without charge, fully scramble or otherwise fully block the audio and video programming of each channel carrying such programming so that one not a subscriber does not receive it.").

<sup>197</sup> See PFF Comments at 21. See also Comcast Comments at 3-4; NCTA Supplemental Comments at 8-9.

<sup>198</sup> See NCTA Supplemental Comments at 10. See also PFF Comments at 21; DirectTV Comments at 7; DISH Network Comments at 6; AT&T Comments at 6.

<sup>199</sup> See, e.g., Comcast Comments at 4; Cox Comments at Appendix B at iv.

<sup>200</sup> See NCTA Supplemental Comments at 10-11; Cox Comments at Appendix B, p. iii.

<sup>201</sup> See NCTA Supplemental Comments at 11. See also CEA Comments at 10 (regarding the tru2way platform which CEA states enables cable operators to deploy advanced program guides with innovative blocking features).

60. Digital set-top boxes offer a variety of different menu options from which to gain information about a show's rating and to activate parental controls.<sup>202</sup> Programs can be blocked according to the TV Parental Guidelines' age-based ratings or content descriptors, or by a combination of the two.<sup>203</sup> Movies can be blocked according to MPAA ratings.<sup>204</sup> A customer can view MPAA ratings for movies and block particular movies based on those ratings, thereby enabling the customer to select movies appropriate for family viewing.<sup>205</sup> In addition, many digital cable boxes provide access to information about the TV Parental Guidelines, including descriptions of the content labels in the information bar (e.g., TV-PG, V/ V=moderate violence), as well as full ratings information, including content labels in the description of a highlighted program that appears in the TV listings grid.<sup>206</sup> In addition, several cable operators offer links on their websites to the websites of third-party rating services. For example, Time Warner Cable, Cox, and Comcast provide links to the Common Sense Media programming reviews.<sup>207</sup>

61. The cable industry has voluntarily undertaken specific actions to promote the availability of parental control tools in cable technology.<sup>208</sup> In 2004, the cable industry commenced a new education effort, "Control Your TV," which produced additional PSAs as well as websites, in both English and Spanish, promoting the availability of cable's blocking technology as well as resources devoted to media literacy and education.<sup>209</sup> In addition, cable companies provide other assistance to help parents with parental controls, including telephone hotlines, websites, and instructional short programs and videos.<sup>210</sup>

62. Local telephone companies that offer video service also provide customers with the ability to control their children's television viewing.<sup>211</sup> Verizon, for example, uses the same set-top boxes as other cable companies.<sup>212</sup> AT&T notes that its U-verse Television service allows parents to, among other things, block channels, record programs, set limits on ordering and watching on-demand

---

<sup>202</sup> See NCTA Supplemental Comments at 9-10.

<sup>203</sup> *Id.* at 9.

<sup>204</sup> See *id.* at 10.

<sup>205</sup> See *id.*

<sup>206</sup> See *id.*

<sup>207</sup> *Id.* at 12. See also Comcast Comments at 6-7; Cox Comments at 8-9.

<sup>208</sup> NCTA and MPAA, along with NAB, assert that the First Amendment and the Communications Act limit the Commission's authority to establish new mandates concerning alternative ratings systems. See NAB/NCTA/MPAA Joint Comments at 19-20; NAB/NCTA/MPAA Reply at 14-15.

<sup>209</sup> See NCTA Supplemental Comments at 5. The NCTA "Control Your TV" website provides a description of the parental controls offered by cable television providers. See <http://controlyourtv.org>.

<sup>210</sup> See Comcast Comments at 5-6 (brochure, telephone hotline, website, video); Cox Comments at 4 (Take Charge instruction sheets and website). See also DIRECTV Comments at 3-4 (describing its website and its "Basics Show" which runs continuously on one of the DIRECTV channels).

<sup>211</sup> See AT&T Comments at 6 (regarding U-verse Television); Verizon Comments at 4-6 (regarding FiOS TV). See also USTelecom Comments at 6 (noting that smaller companies are also offering state of the art video networks that provide parental controls).

<sup>212</sup> See PFF Comments at 23. See also Verizon Comments at 4-6. For FiOS TV customers, a variety of parental control options are available through the DVR offered to Verizon's FiOS customers. See *id.* at 5

videos, and prevent a channel or VOD from appearing in the EPG listing.<sup>213</sup>

63. Satellite providers also offer parental control capabilities through their set-top boxes.<sup>214</sup> Satellite providers state that, without any government mandate, the industry has developed tools that are more effective and user-friendly than the V-chip and that these tools have proven to be a key marketing and subscriber retention tool for video providers.<sup>215</sup> Both DISH Network and DIRECTV have established a relationship with a third-party ratings service, Common Sense Media, and state that they anticipate that in the future the Common Sense Media ratings will be available on information screens accessible through their on-screen programming guides.<sup>216</sup>

64. In its Reply Comments, Motorola, Inc. (“Motorola”) provides information about its advanced server technology called TV Firewall which it expects to be ready for deployment in cable headends in 2010.<sup>217</sup> Motorola states that TVFirewall will offer the same kind of capabilities available now to many cable subscribers but will also permit parents to make affirmative viewing choices, create a pre-selected library of programming for their children to view, customize parental control configurations for each set-top box in the home, specify the time periods during each day when a child is allowed to view programming, and log the viewing activity of each set-top box.<sup>218</sup> TVFirewall will be configured via a graphical user interface (“GUI”) that is available online and can be accessed from any device that can access the Internet, including web-enabled mobile devices.<sup>219</sup> The GUI will allow parental control configurations to be customized for each set-top box in the home.<sup>220</sup> TV Firewall will utilize switched digital video (“SDV”) technology to control access to cable content.<sup>221</sup> The parental control settings for each set-top box in the home will be maintained in servers at the cable headend.<sup>222</sup> When a child tunes to a particular channel, the set-top box will send an inquiry to the server to confirm whether the set-top box is authorized to tune to that channel.<sup>223</sup>

65. TVFirewall will allow for white listing of content selected by parents.<sup>224</sup> Specifically, Motorola explains that the playlist support feature of TVFirewall will allow parents to use the GUI to select programs that they want their children to view.<sup>225</sup> The programs selected will create a playlist for

---

<sup>213</sup> See AT&T Comments at 6.

<sup>214</sup> See DISH Network Comments at 4-6; DIRECTV Comments at 3-11.

<sup>215</sup> See DISH Network Comments at 4-6.

<sup>216</sup> See *id.* at 6; DIRECTV Comments at 11.

<sup>217</sup> See Motorola Reply at 4-8.

<sup>218</sup> See *id.* at 4-8.

<sup>219</sup> See *id.* at 4-5.

<sup>220</sup> See *id.* at 4.

<sup>221</sup> In contrast to the traditional cable architecture, in which all channels are typically delivered to all customers at all times regardless of whether anyone is watching, SDV enables operators to allocate bandwidth based on usage levels, thereby enabling more effective bandwidth utilization. SDV must be enabled on the network, but a particular channel does not have to be switched, in order for TV Firewall to work. See *id.* at 7-8 n.11.

<sup>222</sup> See *id.* at 7.

<sup>223</sup> See *id.*

<sup>224</sup> See *id.* at 7.

<sup>225</sup> See *id.*

the set-top box.<sup>226</sup>

66. In addition to the parental control tools available through set-top boxes and programming guides, many MVPDs offer subscribers the option of purchasing a bundle of “family friendly” channels.<sup>227</sup> For example, DISH Network offers “DishFAMILY”<sup>228</sup> and DIRECTV offers a “Family Choice” bundle of channels.<sup>229</sup> Major cable operators, including Comcast, Time Warner, Cox, Insight Communications, Mid-Continent, and Bright House, also offer family packages.<sup>230</sup> In addition, a satellite service called Sky Angel offers over 70 channels of Christian and family friendly programs.<sup>231</sup>

67. While the record reflects that MVPD parental control technologies exist, the record is lacking data in a number of areas regarding MVPD parental control technologies, as explained further below, which the Commission intends to explore in a forthcoming *NOI*.<sup>232</sup>

### C. Other Parental Control Devices for Television

68. The Commission invited comment in the *NOI* on advanced blocking technologies for television, other than the V-chip and other than those provided by MVPDs, that either currently exist or are under development.<sup>233</sup> Pursuant to the directive of the Child Safe Viewing Act, the Commission invited comment specifically on technologies that operate based on ratings established by an entity other than the creator of the programming<sup>234</sup> and on technologies that can filter language based upon information in closed captioning.<sup>235</sup> As discussed below, while the record reflects that “other parental control devices” for television (*i.e.*, parental control devices and technologies other than the V-chip and those provided by MVPDs) exist, the record is lacking data in a number of areas regarding these devices,

---

<sup>226</sup> See *id.*

<sup>227</sup> See CEA Comments at 10. We note that the Commission adopted a *Notice of Proposed Rulemaking* in September 2007 in which it sought comment on concerns raised by MVPDs regarding certain wholesale programming practices. See *Program Access Rules and Examination of Programming Tying Arrangements*, MB Docket No. 07-198, Notice of Proposed Rulemaking, 22 FCC Rcd 17791, 17862, ¶ 119 and 17867, ¶ 133 (2007). In response to the *NPRM*, a number of MVPDs alleged that programmers often demand tier or minimum penetration requirements, pursuant to which the programmer will make its content available only if the MVPD carries it on one of the MVPD’s most highly penetrated tiers and will specifically preclude the MVPD from placing the station or network on anything other than one of the most highly penetrated tiers. See, e.g., American Cable Association Comments (MB Docket No. 07-198) at 14-16, 18, 27-43; Broadband Service Providers Association Comments (MB Docket No. 07-198) at 19-24; DISH Network Comments (MB Docket No. 07-198) at 2-3, 14-16. Some MVPDs have claimed that these alleged tier or minimum penetration requirements limit their ability to offer themed tiers, including “family friendly” tiers. See ACA Comments (MB Docket No. 07-198) at 43; BSPA Comments (MB Docket No. 07-198) at 19; DISH Network Comments (MB Docket No. 07-198) at 2.

<sup>228</sup> See DISH Network Comments at 7.

<sup>229</sup> See PFF Comments at 23.

<sup>230</sup> *Id.*

<sup>231</sup> See [www.skyangel.com](http://www.skyangel.com). See also PFF Comments at 23-24.

<sup>232</sup> See *infra* section XI.

<sup>233</sup> See *NOI*, 24 FCC Rcd at 3349, ¶ 23.

<sup>234</sup> *Id.* at 3348, ¶ 20. See also Child Safe Viewing Act at Section 2(b)(4).

<sup>235</sup> See *NOI*, 24 FCC Rcd at 3349, ¶ 24. See also Child Safe Viewing Act at Section 2(b)(3).

as discussed below, which the Commission intends to explore in a forthcoming *NOI*.<sup>236</sup>

### 1. TiVo's KidZone

69. As noted in the *NOI*, TiVo offers a service to its subscribers called KidZone that permits parents to block, select, and/or record programming for their children based on a list of recommended programs developed by independent organizations including PTC, KIDS FIRST!, and Common Sense Media.<sup>237</sup> TiVo states that it developed KidZone after its research showed that parents found the V-chip "confusing and difficult to configure."<sup>238</sup> Using KidZone, parents turn on program blocking for live and recorded television by selecting an appropriate age range: 6 and under; 9 and under; or 12 and under. Pursuant to the default settings for each age range, KidZone blocks shows with ratings above a certain level (e.g., for ages 9 and under, shows with a rating of TV-PG, TV-14 and TV-MA are blocked) and shows with certain content labels (e.g., for ages 9 and under, D, S, L, V and FV are all blocked).<sup>239</sup> Parents have the option of changing these default settings for the indicated age range.<sup>240</sup> KidZone will also block entire channels so that the children are permitted to tune into only those channels that parents likely would approve for children in that age range (e.g., PBS, ABC Family, Nickelodeon, Disney and Animal Planet, among others, are permitted by default for ages 9 and under).<sup>241</sup> KidZone allows parents to override the TV Parental Guideline ratings and default settings and permit viewing of particular programs and channels based on their own assessment of the appropriateness of the content for their children.<sup>242</sup>

70. TiVo explains that KidZone allows for both white listing and black listing of particular shows.<sup>243</sup> Specifically, KidZone provides parents with the option to indicate that particular shows are or are not permitted for live or recorded viewing.<sup>244</sup> TiVo states that when the parents see the title of a show that they do or do not want their children to view, the parents have the option to affirmatively allow or prevent recording of the program.<sup>245</sup>

71. In addition, KidZone provides parents with access to KidZone Guides, which lists programs recommended by independent ratings organizations, as well as programs identified by

---

<sup>236</sup> See *infra* section XI.

<sup>237</sup> See TiVo Comments at 3. Approximately 3.3 million customers, both within and outside of the United States, subscribe to the TiVo service. See TiVo, Inc., SEC Form 10-K (April 3, 2009), at 41.

<sup>238</sup> See TiVo Comments at 2.

<sup>239</sup> See *id.* at 3.

<sup>240</sup> See *id.*

<sup>241</sup> See *id.*

<sup>242</sup> See *id.* Comcast set-top boxes with TiVo functionality do not currently support the KidZone feature, but they do support other parental control features. See Letter from Ryan G. Wallach, Counsel for Comcast, to Ms. Marlene H. Dortch, Secretary, FCC, MB Docket No. 09-26 (July 24, 2009), at 2. TiVo and DIRECTV announced that they are working to introduce a DIRECTV DVR featuring the TiVo Service that includes KidZone in the second half of 2009. See DIRECTV and TiVo to Launch New HD DIRECTV DVR with TiVo Service, available at <http://www.directv.com/DTVAPP/global/contentPage.jsp?assetId=P4900010>.

<sup>243</sup> See TiVo Comments at 3.

<sup>244</sup> See *id.*

<sup>245</sup> See *id.*

broadcasters as E/I.<sup>246</sup> Parents can review the recommended programs and select any individual programs for recording or choose to record all of the recommendations.<sup>247</sup> The KidZone Now Playing List provides a list of the shows recorded by the parents for viewing by their children.<sup>248</sup> When parents want to watch their own programs, they enter a password to exit KidZone.<sup>249</sup> The TiVo DVR can be set to automatically re-enter KidZone after a period of time, or the parents may choose to re-enter KidZone at any time.<sup>250</sup>

72. According to TiVo, the KidZone usage rate is about equivalent to the V-chip usage rate.<sup>251</sup> As discussed above, the Kaiser Family Foundation conducted two studies, one of which found that 15 percent of parents have used the V-chip<sup>252</sup> and the other of which found that 16 percent of parents have used the V-chip.<sup>253</sup> TiVo estimates that 30-35 percent of households with a TiVo DVR have children and, among those households, KidZone usage has never exceeded the 15 percent to 16 percent V-chip usage rate found in the 2004 and 2007 Kaiser Family Foundation Studies.<sup>254</sup> In addition, TiVo states that parents it surveyed who use KidZone report that they value the feature highly, similar to the findings regarding the V-chip in the studies conducted by the Kaiser Family Foundation.<sup>255</sup>

73. TiVo states that it surveyed recent purchasers of TiVo DVRs.<sup>256</sup> Among recent purchasers in households with children 13 years of age and younger, only 29 percent were aware of KidZone prior to purchase.<sup>257</sup> Among these households that were aware of KidZone, 61 percent said that it was important or very important in increasing their purchase interest.<sup>258</sup> Among recent purchasers of TiVo DVRs in households with children that were aware of KidZone prior to purchase, 49 percent reported that KidZone was important or very important in increasing their purchase interest.<sup>259</sup> TiVo also states that the research it conducted during the development of KidZone showed that parents were using the TiVo DVR to record shows for their children rather than using the V-chip to block programming.<sup>260</sup>

---

<sup>246</sup> See *id.* at 3-4.

<sup>247</sup> See *id.* at 4.

<sup>248</sup> See *id.*

<sup>249</sup> See *id.*

<sup>250</sup> See *id.*

<sup>251</sup> See *id.*

<sup>252</sup> See *Parents, Children & Media: A Kaiser Family Foundation Survey* (Fall 2004).

<sup>253</sup> See *2007 Kaiser Family Foundation Study*.

<sup>254</sup> See TiVo Comments at 4. See also *supra* ¶ 17.

<sup>255</sup> See TiVo Comments at 4. We note that TiVo did not provide statistics to substantiate this claim. By comparison, the 2007 Kaiser Family Foundation Study found that “nearly three out of four parents (71%) who have tried the V-Chip say they find it ‘very’ useful, a higher proportion than for any of the media ratings or advisory systems.” See *2007 Kaiser Family Foundation Study* at 10.

<sup>256</sup> See TiVo Comments at 4.

<sup>257</sup> See *id.* at 4-5.

<sup>258</sup> See *id.*

<sup>259</sup> See *id.* at 5.

<sup>260</sup> See *id.*

## 2. TVGuardian

74. Section 2(b)(3) of the Act specifically requires the Commission to consider technologies that filter language based on closed captioning information.<sup>261</sup> In the *NOI*, the Commission noted that TVGuardian is a currently available technology that uses closed captions to identify inappropriate content in television programs.<sup>262</sup> According to TVGuardian, its technology is an “Advanced Foul Language Filtering Technology” (“AFLFT”) that reads the closed captioning that is embedded and required in most forms of television programming.<sup>263</sup> When the technology encounters a word that the viewer has deemed objectionable, the captioned phrase is muted and a non-offensive version of the phrase appears on the screen.<sup>264</sup> TVGuardian argues that, unlike the V-chip which blocks objectionable programs, AFLFT offers families the best of both worlds – they can watch the shows they enjoy without the objectionable language.<sup>265</sup> Parents can choose between multiple filter levels, ranging from very strict to tolerant, and can select specific kinds of offensive speech to filter, such as racial/hate slurs, offensive religious references, and sexual terms.<sup>266</sup>

75. In the *NOI*, the Commission noted that closed captions are not always synchronized perfectly with the audio, and thus the captions may appear slightly before or after the time words are spoken as part of the on-screen program.<sup>267</sup> The *NOI* invited comment on whether this lack of synchronization affects the use of captions to block inappropriate comment.<sup>268</sup> TVGuardian states that, while errors within the closed captions may reduce the accuracy rate of its technology slightly, its accuracy level is only slightly less than 100 percent.<sup>269</sup> In contrast, TVGuardian asserts that the V-chip ratings often do not contain appropriate content descriptors, such as an “L” warning on a program containing numerous offensive words.<sup>270</sup>

76. TVGuardian states that a survey it commissioned in 2007 shows that 70 percent of families with children, and 62 percent of all viewers surveyed, are uncomfortable with the language on TV, and 38 percent of viewers without pay TV service would be more likely to choose pay TV if language filtering were available.<sup>271</sup> TVGuardian reports that its technology was first sold as an add-on hardware solution – a \$99 box that could be connected between the TV and cable or satellite box or a

---

<sup>261</sup> Child Safe Viewing Act at Section 2(b)(3) (requiring the Commission to consider advanced blocking technologies that “can filter language based upon information in closed captioning”).

<sup>262</sup> See *NOI*, 24 FCC Rcd at 3349, ¶ 24. TVGuardian can operate with both networked and non-networked technologies. Accordingly, we also discuss TVGuardian in Section VI below pertaining to non-networked devices.

<sup>263</sup> See TVGuardian Reply at iii.

<sup>264</sup> See *id.*

<sup>265</sup> See *id.* Most of the approximately 9,900 brief comments the Commission received in response to the *NOI* express support for foul language filtering technology in general, and many of these commenters mention TVGuardian specifically.

<sup>266</sup> See *id.* at 4.

<sup>267</sup> See *NOI*, 24 FCC Rcd at 3349, ¶ 24.

<sup>268</sup> See *id.*

<sup>269</sup> See TVGuardian Comments at 21.

<sup>270</sup> See *id.*

<sup>271</sup> See *id.* at 29-30.

VCR tuner – and subsequently was built into some DVD players and VCRs.<sup>272</sup> TVGuardian states that over 12 million DVD players with TVGuardian technology have been sold to date.<sup>273</sup> According to TVGuardian, however, hardware containing TVGuardian technology is no longer being manufactured and fewer and fewer DVD players are being built with the TVGuardian feature.<sup>274</sup>

77. TVGuardian states that, for foul language filtering to work in the digital world, the filtering must be either built into the pay-TV receiver for viewers that subscribe to pay-TV service or into the TV for viewers without pay-TV.<sup>275</sup> According to TVGuardian, it has repeatedly offered its technology to major cable and satellite companies and has been repeatedly turned down.<sup>276</sup> TVGuardian explains that it offered this technology to various MVPDs for free, subject only to the condition that TVGuardian would receive half of any fee an MVPD charges its subscribers for the service.<sup>277</sup> TVGuardian urges the Commission to include in this report a “strong recommendation that Congress ensure that providers enable consumers to have access to AFLFT.”<sup>278</sup>

78. According to NAB, NCTA, and MPAA, MVPDs have met with TVGuardian and elected not to use its technology.<sup>279</sup> These commenters contend that the Commission should not pick technology winners and losers.<sup>280</sup> Comcast states that incorporation of TVGuardian technology into set top boxes would be neither easy nor inexpensive and urges the Commission to decline to recommend such a mandate to Congress.<sup>281</sup> Comcast also points out that TVGuardian acknowledges that its technology has been incorporated into consumer electronics devices that consumers interested in the technology can purchase.<sup>282</sup> Comcast states that it conducted research on TVGuardian and concluded that the technology would be of limited use to its customers, that there were potential legal and technical concerns related to its deployment, and that incorporation of the technology into set-top boxes would not be a good business decision.<sup>283</sup> TiVo and Comcast state that they have doubts that the TVGuardian technology would work well nationwide across a wide variety of close captioned video programs.<sup>284</sup> These commenters also oppose “mandates of particular technology implementations without a thorough

---

<sup>272</sup> See *id.* at 26.

<sup>273</sup> See *id.*

<sup>274</sup> See *id.* at 5. As discussed in Section VI below, TVGuardian explains that, in the past few years, DVDs have been increasingly distributed with the Subtitles for the Deaf and Hard-of-Hearing (SDH) format rather than closed-captions, which limits the usefulness of TVGuardian technology in DVD players. See *id.* at Appendix C at 3.

<sup>275</sup> See *id.* at 40.

<sup>276</sup> See *id.* at 5-9.

<sup>277</sup> See *id.* at 8.

<sup>278</sup> See TVGuardian Reply at iv. See also *id.* at 12 (the “government should require that cable, satellite and IPTV providers permit families to have access to AFLFT so that the public interest can be served.”).

<sup>279</sup> See NAB/NCTA/MPAA Reply at 15-16.

<sup>280</sup> See *id.*

<sup>281</sup> See Comcast Reply at 3.

<sup>282</sup> See *id.* at 3.

<sup>283</sup> See *id.* at 4.

<sup>284</sup> See TiVo Comments at 9 n.4; Comcast Reply at 3-4.

cost/benefit analysis and an understanding of all intellectual property issues.”<sup>285</sup>

### 3. CC+

79. Caption TV Inc.’s CC+ is another example of a technology that filters language based on closed captioning information, but it also has the capability of filtering objectionable video content.<sup>286</sup> According to Caption TV, CC+ permits viewers to selectively block images, soundtrack, and captioning text in television programming.<sup>287</sup> Depending upon the level of sensitivity selected by the viewer, the CC+ technology mutes specific words, partially or totally blocks nudity and sex, and partially or totally blocks violence.<sup>288</sup> Caption TV explains that it has developed a software development kit for inserting filter codes that allows specific and precise blocking of portions of the audio and video.<sup>289</sup> The filter codes, inserted in Line 21 by the captioner, provide cues to the hardware that allow it to perform the filtering.<sup>290</sup> Caption TV says that the CC+ technology can be implemented into any closed captioning encoding software program, such as that used in many personal computers and digital cable and satellite set top boxes.<sup>291</sup> TVGuardian maintains that technologies such as CC+, as well as ClearPlay and CustomPlay,<sup>292</sup> are not ready for use in television programming.<sup>293</sup> TVGuardian contends that, unlike technologies like TVGuardian that rely on existing closed captioning data, technologies such as CC+ require every frame of every scene of each program to be manually screened and coded in advance for objectionable content.<sup>294</sup> By analogy, TVGuardian notes that it took twelve years to add closed captioning to the majority of television programming.<sup>295</sup> TVGuardian argues that the incorporation of CC+ into the wide range of devices and platforms mentioned in the Child Safe Viewing Act would represent an overwhelming burden for the media industry.<sup>296</sup> According to TVGuardian, another challenge for these technologies is that they filter on the basis of subjective judgment calls rather than foul language that is relatively easier to define.<sup>297</sup>

80. Caption TV states that parents can customize the list of words to be muted from the audio and/or replaced in the closed caption readout, can filter portions of a scene containing the selected level of nudity, and can filter portions of a scene containing the selected level of violence.<sup>298</sup> Unlike the V-

<sup>285</sup> TiVo Comments at 9 n.4. *See also* Comcast Reply at 3-4.

<sup>286</sup> *See* Caption TV Comments at 1.

<sup>287</sup> *See id.* at 3.

<sup>288</sup> *See id.* at 2.

<sup>289</sup> *See id.*

<sup>290</sup> *See id.*

<sup>291</sup> *See id.* at 4.

<sup>292</sup> *See infra* ¶¶ 119-120 for discussion of the ClearPlay and CustomPlay technologies for non-networked devices.

<sup>293</sup> *See* TVGuardian Comments at 15.

<sup>294</sup> *See id.* at 16.

<sup>295</sup> *See id.*

<sup>296</sup> *See id.* at 15-16.

<sup>297</sup> TVGuardian notes that even the Commission has concluded that violence is difficult to define. *See id.* at 16 (citing *In the Matter of Violent Television Programming And Its Impact on Children*, Report, 22 FCC Rcd 7929, 7931 (2007)).

<sup>298</sup> *See* Caption TV Comments at 2.

chip, which blocks entire programs, CC+ permits filtering to be performed on portions of a program, blocking the objectionable material and allowing the unobjectionable material to pass through the filter.<sup>299</sup> Caption TV states that the CC+ technology is compatible with the V-chip and that a prototype “Set Top Box Decoder” has been developed together with Tri-Vision, the original V-chip patent holder.<sup>300</sup> According to Caption TV, CC+ can be developed into the V-chip menu so parents can choose to activate CC+ or the V-chip from the same screen and with the same access code.<sup>301</sup>

#### 4. Digital Watermarking

81. Two commenters, Digimarc Coproration (“Digimarc”) and the Digital Watermarking Alliance (“DWA”), propose that the Commission consider digital watermarking technology as a possible alternative to the V-chip.<sup>302</sup> As these commenters point out, the V-chip was developed only for television distribution.<sup>303</sup> In contrast, Digimarc and DWA assert that digital watermarking could permit advanced content blocking across numerous delivery platforms.<sup>304</sup>

82. Digital watermarking is a technology whereby a digital code that is imperceptible to humans but detectable by computers, networks, and other electronic devices is embedded in media or other content.<sup>305</sup> When a device reads a digital watermark, it can allow the content to be viewed or not viewed.<sup>306</sup> Because watermarks remain embedded in the content through subsequent manipulations, copying, and format conversions, they permit this technology to be used across a variety of media delivery platforms including television, cable, satellite, wireless devices, non-networked devices, and the Internet.<sup>307</sup> According to Digimarc and DWA, digital watermarking is currently in use in many applications.<sup>308</sup> For example, it is used in preventing unauthorized access to copyrighted work and in deterring counterfeiting of currency.<sup>309</sup> In addition, the Nielsen Company uses digital watermarking in television broadcasts to track viewership among families participating in audience measurement.<sup>310</sup> Digimarc and DWA assert that, because watermarking is content-specific rather than hardware, software, device, or distribution-specific, this technology is one of the very few, if not the only, technology capable of operating across multiple content types and platforms.<sup>311</sup> Digimarc and DWA request in their comments that the Commission consider how digital watermarking technology might provide content

---

<sup>299</sup> *See id.*

<sup>300</sup> *See id.* at 1.

<sup>301</sup> *See id.* at 4.

<sup>302</sup> *See* Digimarc Comments at 2; DWA Comments at 5. Digital watermarking can operate with both networked and non-networked technologies. Accordingly, we also discuss digital watermarking in Section V regarding wireless devices and Section VI pertaining to non-networked devices.

<sup>303</sup> *See* Digimarc Comments at 9; DWA Comments at 3.

<sup>304</sup> *See* Digimarc Comments at 4; DWA Comments at 5.

<sup>305</sup> *See* Digimarc Comments at 2.

<sup>306</sup> *See id.* at 3.

<sup>307</sup> *See id.* at 4-6.

<sup>308</sup> *See* Digimarc Comments at 8 and Appendices A-C; DWA Comments at 4.

<sup>309</sup> *See* Digimarc Comments at 3. *See also* DWA Comments at 4.

<sup>310</sup> *See* Digimarc Comments at 3.

<sup>311</sup> *See id.* at 4. *See also* DWA Comments at 5.

identification for purposes of parental control of media content.<sup>312</sup> In addition, Digimarc suggests that the Commission should recommend to Congress the deployment of other technologies, such as digital watermarking, as an alternative to the V-chip.<sup>313</sup>

83. CEA contends that digital watermarking is not a viable replacement for the V-chip.<sup>314</sup> According to CEA, proponents of digital watermarking have sought legislation for years to incorporate this technology in televisions to control the conditions under which consumers can access content that may be subject to copyright protection.<sup>315</sup> CEA contends that, by advocating watermarking in this proceeding, the proponents are seeking another avenue to accomplish the goal of requiring televisions to incorporate Digital Rights Management (“DRM”) functionality.<sup>316</sup> CEA states that fair use proponents, including many consumer electronics manufacturers and public interest groups, have opposed these attempts as inconsistent with the Supreme Court’s *Sony Betamax* decision.<sup>317</sup> In addition, CEA explains that the ownership and licensing terms of any necessary intellectual property rights would have to be examined before mandating digital watermarking or similar technologies.<sup>318</sup>

### 5. Other Technologies

84. In addition to the technologies discussed above, there are a variety of other kinds of parental control tools available by which to monitor television use. These include after-market television time management tools that allow parents to restrict the time of day or aggregate number of hours that children watch programming,<sup>319</sup> as well as remote controls made for children (*e.g.*, the Weemote) that have just a few large buttons that permit a child to select only certain television channels pre-selected by

---

<sup>312</sup> See Digimarc Comments at 10; DWA Comments at 7. Digimarc advocates a joint industry and government effort to promote the development of parental controls. See Digimarc Comments at 6 n.2 (“Fostering broad adoption of advanced blocking technologies will require government and industry leadership, orchestration of all the stakeholders, and an underlying recognition that consumer value is paramount. Where there is consumer value, there is incentive within industry to innovate and offer solutions. Since the market for parental control to date has not been of sufficient size to stimulate broad-based innovation or deployment, government and industry should pursue orchestrated industry approaches wherein parental controls are a component of a full set of features that offer commercial value.”).

<sup>313</sup> See Digimarc Reply at 1.

<sup>314</sup> See CEA Reply at 10.

<sup>315</sup> See *id.*

<sup>316</sup> See *id.*

<sup>317</sup> See *id.* See also *Sony Corp. of America v. Universal City Studios*, 464 U.S. 417 (1984) (“*Sony Betamax*”) (establishing that recording programs for later viewing in the privacy of the user’s home is a noncommercial use permitted under the fair use doctrine).

<sup>318</sup> See CEA Reply at 10-11. See also TiVo Reply at 3.

<sup>319</sup> See PFF Comments at 24. PFF explains that the Family Safe Media website sells TV time management tools that allow parents to restrict the time of day or aggregate number of hours that children watch programming. See *id.* (citing [www.familysafemedia.com/tv\\_time\\_management\\_tools\\_-\\_par.html](http://www.familysafemedia.com/tv_time_management_tools_-_par.html)). PFF explains further that devices such as the Bob TV Timer by Hopscotch Technology and the TV Allowance television time manager feature PIN-activated security methods and tamper-proof lock boxes that make it impossible for children to unplug or reset the device. See *id.* (citing [www.hopscotchtechnology.com](http://www.hopscotchtechnology.com), [www.tvallowance.com](http://www.tvallowance.com)). PFF states that “credit-based” devices such as the Play Limit box require children to place time tokens in a metallic lockbox to determine how much TV or game time is allowed. See *id.* (citing [www.playlimit.com](http://www.playlimit.com)).

parents.<sup>320</sup> In addition, as noted by PFF, devices such as VCRs, DVD players, DVRs, and VOD services permit parents to accumulate libraries of selected programming for their children and control when it will be viewed.<sup>321</sup>

### III. VIDEO GAMES

85. The *NOI* sought comment on whether to examine blocking technology for video game players and video games.<sup>322</sup> As noted in the *NOI*, video game players are not included among the devices specifically identified in Section 2(b)(2) of the Act, and video games are not mentioned in the Senate Report and were not discussed in the Senate hearing on the Act.<sup>323</sup> In light of the popularity of video games among children and concerns expressed regarding their content, however, the Commission sought comment on whether to examine methods of controlling access to video games in this proceeding.<sup>324</sup>

86. The majority of commenters that address this issue take the position that video games should not be reviewed in this proceeding.<sup>325</sup> In general, these commenters contend that the Act is silent with respect to video games and, in any event, the video game industry already provides one of the most robust voluntary rating systems available.<sup>326</sup> Although we conclude that video game players and video games are not the focus of the Child Safe Viewing Act, we did receive some comments on parental controls used in the video game industry, and report on those here. Moreover, we intend to explore issues pertaining to parental controls for video game players and video games in a forthcoming *NOI*.<sup>327</sup>

87. According to PFF, the video game industry rating system is “in many ways the most sophisticated, descriptive, and effective ratings system devised by any major media sector in America.”<sup>328</sup> Virtually all games sold at retail in the U.S. are rated by the Entertainment Software Rating Board (“ESRB”) pursuant to a system of six age-based ratings and more than 30 content descriptors.<sup>329</sup> Common Sense Media also provides independent video game ratings.<sup>330</sup> In addition to appearing on the video game packaging, the ESRB ratings are also available digitally in the game metadata thereby

---

<sup>320</sup> See *id.* at 25.

<sup>321</sup> See *id.* at 26.

<sup>322</sup> See *NOI*, 24 FCC Rcd at 3345, ¶ 11.

<sup>323</sup> See *id.* at 3345, ¶ 11.

<sup>324</sup> See *id.*

<sup>325</sup> See, e.g., CDT Comments at 6; Digital Media Association (“DMA”) Comments at 2; Microsoft Comments at 4. See also Entertainment Software Association (“ESA”) Comments at 3-8 (arguing that the Commission has neither direct nor ancillary jurisdiction to regulate video games, including video game content or video game rating systems).

<sup>326</sup> See CDT Comments at 6; DMA Comments at 2; Microsoft Comments at 4; ESA Comments at 3-8. A description of the Entertainment Software Rating Board (“ESRB”) ratings is contained at Exhibit 1 of the ESA Comments.

<sup>327</sup> See *infra* section XI.

<sup>328</sup> PFF Comments at 48.

<sup>329</sup> See ESA Comments at 9. According to ESA, at least three specially-trained raters review all game content against a wide range of criteria, and the ESRB assigns the rating after an “extensive deliberative process.” *Id.*

<sup>330</sup> See Common Sense Media Comments at 2.

enabling video game platforms to screen content based on the ratings.<sup>331</sup> Virtually all current generation video game platforms contain tools that block by ESRB rating, including Microsoft Xbox 360, Nintendo's Wii, Sony PlayStation 3, and Windows Vista operating system.<sup>332</sup> Some devices also allow parents to control with whom their children play video games online and how and when they play, as well as to restrict or track the amount of time the children spend playing the games.<sup>333</sup> According to ESA, surveys show that, because of the usefulness of the video game ratings and outreach programs sponsored by the industry, 86 percent of parents who purchase video games are aware of the ESRB ratings and 78 percent regularly check the rating before making a video game purchase.<sup>334</sup> According to the 2007 Kaiser Family Foundation Study, 58 percent of parents who have used the video game ratings found them useful.<sup>335</sup> Moreover, the Federal Trade Commission ("FTC") examines the marketing and advertising practices of major media sectors, including video games.<sup>336</sup> The FTC recently found that, whereas 42 percent of children were able to purchase an M-rated video game in 2006, that percentage fell to 20 percent in 2008.<sup>337</sup>

88. Common Sense Media maintains that the rating assigned by ESRB no longer applies if a user downloads a modification or utilizes the game's online functions to play other networked users.<sup>338</sup> In response, ESA says that ESRB does rate authorized game downloads and online content created by the video game publisher.<sup>339</sup> According to ESA, an issue arises only with user-created content or user chats – which is not an issue unique to video games.<sup>340</sup> ESA contends that no rating system or control device can anticipate the extemporaneous world of the Internet. Moreover, ESA states that ESRB-rated games contain a warning notifying parents that online interactions are possible in connection with game play and that such interactions are not rated.<sup>341</sup>

---

<sup>331</sup> See ESA Comments at 10.

<sup>332</sup> See *id.* See also CEA Comments at 12, Nintendo Reply at 2.

<sup>333</sup> See ESA Comments at 10.

<sup>334</sup> See *id.* at 11 and Exhibit 2.

<sup>335</sup> See 2007 Kaiser Family Foundation Study at 9. According to a survey of 8-18 year-olds, 21 percent say that their parents have rules about which video games they can play. See *Generation M: Media in the Lives of 8-18 Year-olds* at 17 and Appendix 3.4.

<sup>336</sup> See *id.* at 12-13; PFF Comments at 55-56. See, e.g., FTC, *Marketing Violent Entertainment to Children: A Fifth Follow-up Review of Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries* (April 2007), available at <http://www.ftc.gov/reports/violence/070412MarketingViolentEChildren.pdf>.

<sup>337</sup> See FTC, *Press Release, Undercover Shoppers Find It Increasingly Difficult for Children To Buy M-Rated Games* (May 8, 2008), available at <http://www.ftc.gov/opa/2008/05/secretshop.shtml>. But see Patrick M. Garry & Candice J. Spurlin, *The Effectiveness of Media Rating Systems in Preventing Children's Exposure to Violent and Sexually Explicit Media Content: An Empirical Study*, 32 OKLA. CITY U. L. REV. 215, 233-5 (2007) (reporting results of a survey that showed that 58 percent of children between the ages of 9 and 15 had played a game rated Mature (M) or Adults Only (AO); 47 percent of children between the ages of 9 and 15 owned an M or AO-rated game; and that of the children who purchased the games themselves, 90 percent were not asked for their age).

<sup>338</sup> See Common Sense Media Comments at 2.

<sup>339</sup> See ESA Reply at 3-5.

<sup>340</sup> See *id.*

<sup>341</sup> See *id.*

#### IV. AUDIO-ONLY PROGRAMMING

89. The *NOI* also sought comment on whether to examine blocking technology designed for content that is audio only (e.g., music), or technologies designed for content that combines audio and video (e.g., television programs), or both.<sup>342</sup> Section 2(b)(2) of the Act requires the Commission to consider “advanced blocking technologies” that may be appropriate across a wide variety of “devices capable of transmitting or receiving video *or* audio programming.”<sup>343</sup> Moreover, Section 2(d) of the Act defines “advanced blocking technologies” as technologies that can improve or enhance the ability of a parent to protect children from any indecent or objectionable “video *or* audio” programming.<sup>344</sup> Although the Commission explained in the *NOI* that the legislative history indicates that Congress was focused primarily on television content,<sup>345</sup> the text of the Act directs the Commission to consider blocking technologies for audio-only programming. Accordingly, we discuss here the few comments the Commission received on the issue of parental controls used for audio-only programming. In addition, the Commission intends to explore issues pertaining to parental controls for audio-only programming in a forthcoming *NOI*.<sup>346</sup>

90. Most commenters addressing the issue contend that we should not examine audio-only programming in this proceeding.<sup>347</sup> In general, these commenters agree that Congress did not intend for the Commission to inquire into music or radio.<sup>348</sup> Commenters also note that, since the 1980’s, the music industry has administered a voluntary parental advisory labeling program to warn parents if an album contains explicit lyrics concerning sex, violence, or drug use.<sup>349</sup> The program is run by the Recording Industry Association of America on behalf of record companies and producers who decide which songs and products receive the ratings. According to the 2007 Kaiser Family Foundation Study, 56 percent of parents who have used the music ratings found them very useful.<sup>350</sup> In addition to ratings provided by the music industry, there are a number of independent websites that provide music reviews for parents, including Common Sense Media and Plugged In Online, as well as user-generated music reviews and sites that permit parents to examine music lyrics.<sup>351</sup>

91. PFF explains that not every portable music player on the market today offers embedded parental control capabilities, but Apple and Microsoft offer some controls on their devices and are

---

<sup>342</sup> See *NOI*, 24 FCC Rcd at 3344, ¶ 7.

<sup>343</sup> Child Safe Viewing Act at Section 2(b)(2) (emphasis added).

<sup>344</sup> Child Safe Viewing Act at Section 2(d) (emphasis added).

<sup>345</sup> See *NOI*, 24 FCC Rcd at 3344, ¶ 7.

<sup>346</sup> See *infra* section XI.

<sup>347</sup> See CDT Comments at 4; DMA Comments at 2; Google Comments at 10; National Association of Recording Merchandisers (“NARM”) Comments at 1.

<sup>348</sup> See CDT Comments at 4; DMA Comments at 2; Google Comments at 10; NARM Comments at 1.

<sup>349</sup> See PFF Comments at 43. The labeling of explicit lyrics does not include age-based categories because the music industry contends that music is not amenable to such classification. See NARM Comments at 2.

<sup>350</sup> See 2007 Kaiser Family Foundation Study at 9. In addition, a study of children aged 8-18 showed that 16 percent say their parents have rules about what kind of music they can listen to and 14 percent say their parents check parental warnings or ratings on music. See *Generation M: Media in the Lives of 8-18 Year-olds* at Appendix 3.4.

<sup>351</sup> See PFF Comments at 48.

committed to improving these capabilities.<sup>352</sup> The iTunes software contains parental controls that enable parents to disable all podcasts, online radio, music sharing, or access to the iTunes Store.<sup>353</sup> On the iTunes store, music containing explicit lyrics is labeled “Explicit,” and movies are labeled with MPAA movie ratings and other content descriptors.<sup>354</sup> Parents can restrict downloading of music that contains the “Explicit” label.<sup>355</sup> Parents can also designate the movie and TV ratings that are appropriate for their children, thereby restricting a child’s access to anything rated above that level.<sup>356</sup>

92. With respect to terrestrial radio, the Center for Democracy and Technology (“CDT”) claims that there does not appear to be any significant perception of a problem with inappropriate content.<sup>357</sup> The National Hispanic Media Coalition, however, counters that many Latinos are particularly concerned about inappropriate sexual content on Spanish language radio and requests that the Commission inquire into blocking technology for such content.<sup>358</sup> We note, however, that we are unaware of any current blocking technology that would allow parents to protect their children from indecent or objectionable audio programming on terrestrial radio.<sup>359</sup> Moreover, CDT’s assertion that there is not a perception of a problem with regard to terrestrial radio is inconsistent with the history of the Commission’s indecency enforcement, which has focused predominantly on broadcast radio,<sup>360</sup> and the fact that the Commission continues to receive numerous radio broadcast indecency complaints.

93. With respect to satellite radio, CDT notes that satellite radio offers subscribers the option to block channels that frequently use explicit language.<sup>361</sup> PFF explains that satellite radio subscribers can choose from a variety of plans, or purchase channels a la carte, to exclude any channels that might include programming with explicit language or lyrics.<sup>362</sup>

## V. WIRELESS DEVICES

94. In the *NOI*, the Commission sought comment on blocking and filtering technologies for wireless devices, recognizing that wireless devices present additional challenges due to technical aspects and because mobile phones are typically operated by children away from the purview of their parents.<sup>363</sup>

---

<sup>352</sup> See PFF Comments at 44.

<sup>353</sup> See *id.* at 45.

<sup>354</sup> See *id.*

<sup>355</sup> See *id.*

<sup>356</sup> See *id.*

<sup>357</sup> See CDT Comments at 4.

<sup>358</sup> See National Hispanic Media Coalition Comments at 3.

<sup>359</sup> Moreover, the record has no data indicating whether HD Radio™ receivers have channel blocking capabilities. See CDT Comments at 4 (noting that satellite radio allows subscribers to block channels).

<sup>360</sup> While the Commission’s most recent indecency enforcement actions have involved television, the Commission over the course of its history enforcing the indecency regulations has focused predominantly on broadcast radio. See, e.g., *Industry Guidance on the Commission’s Case Law Interpreting 18 U.S.C. § 1464 and Enforcement Policies Regarding Broadcast Radio*, 16 FCC Rcd 7999 (2001).

<sup>361</sup> See CDT Comments at 4. See also <http://www.xmradio.com/help/index.xmc>.

<sup>362</sup> See PFF Comments at 44.

<sup>363</sup> See *NOI*, 24 FCC Rcd at 3353, ¶ 27.

With respect to wireless issues, the Commission received comments primarily from wireless providers; therefore, the discussion below largely does not reflect input from consumers and non-carrier entities. We intend to explore the issues discussed in Section XI below pertaining to parental controls for wireless devices, in particular seeking comments from consumers and non-carrier entities, in a forthcoming *NOI*.

95. In the *NOI*, the Commission asked what role the Government should play in ensuring that blocking and filtering tools are made available to parents so that children can be shielded from inappropriate content.<sup>364</sup> Industry commenters assert that, even in the absence of regulation, the industry has developed a wide range of blocking technologies and parental control features; therefore, government regulation is unnecessary at this time.<sup>365</sup> They further contend that the competitive market has responded to consumer demands for parental controls and predict that more advanced filters and access controls are in development.<sup>366</sup> On the other hand, some consumers support a government requirement that filtering technologies be embedded across all platforms of consumer devices that support video applications, including wireless devices.<sup>367</sup> Specifically, for example, some consumers express support for making TVGuardian (or similar products) available on all devices that support video content.<sup>368</sup>

96. The record was limited with respect to wireless solutions (both in terms of number and type of commenters discussing wireless issues and the specific issues addressed). Below we provide a factual overview of the marketplace and the wireless industry's efforts to educate parents on the options available to them to block unwanted mobile content. We discuss below child protection measures for content offered directly by wireless providers and content available over the Internet that is accessed via wireless devices. We also address non-content-based blocking and filtering technologies and other empowerment tools available to parents. Finally, we discuss the impact of wireless open platforms on these technologies, future developments, and educational efforts. We will address remaining questions regarding wireless solutions in a forthcoming *NOI*.<sup>369</sup>

#### A. Wireless Industry Guidelines and Content Controls

97. As described in the *NOI*, CTIA and participating wireless carriers have voluntarily adopted child protection measures, both for content offered by wireless providers as well as content available over the Internet and accessed via wireless devices.<sup>370</sup> Beginning in 2004, CTIA and

---

<sup>364</sup> See *id.* at 3355, ¶ 33.

<sup>365</sup> See, e.g., CTIA Comments at 2-3; Sprint Comments at 1-2; Verizon Comments at 11-12; T-Mobile Reply at 1, 3.

<sup>366</sup> See CTIA Comments at 12. CTIA believes that companies and content providers who are not under the Commission's jurisdiction would be more likely to participate and follow CTIA-sponsored best practices, which can be adjusted in response to changing consumer expectations and new technologies and applications "in contrast to government mandated regulations that require years of lengthy administrative proceedings to review and revise." *Id.*

<sup>367</sup> See, e.g., Comments of Jennifer White at 1; Tracie Hall at 1; Bill Buhl at 1.

<sup>368</sup> See, e.g., Comments of Mike Coker at 1; Art Gillespie at 1; Johna Oldfield.

<sup>369</sup> See *infra* section XI.

<sup>370</sup> See *NOI*, 24 FCC Rcd at 3353-54, ¶ 29; CTIA Comments at 4. CTIA notes that filters and blocking technologies for carrier-provided content do not include filters for "any end-user generated content (for example, on message boards, chat rooms, or blogs)." CTIA Comments at 4. We also note that the International Telecommunications Union (ITU) has issued draft industry guidelines as part of its Child Online Protection (COP) Initiative, which recognizes CTIA's Guidelines as an approach to protecting children from inappropriate mobile content. The draft (continued....)

participating wireless carriers began developing Carrier Content Classification and Internet Access Control Guidelines.<sup>371</sup> Under these guidelines, participating carriers agree to develop content classification standards and educate consumers about these standards and ratings.<sup>372</sup> With respect to Carrier Content (*i.e.*, content that is available through a carrier's managed content portal and third-party content for which customers may be billed directly by their wireless carrier), carriers generally divide these materials into "Generally Accessible Carrier Content," which is available to all consumers, and "Restricted Carrier Content," which is available to wireless users 18 years of age or older or younger users only with specific parental authorization.<sup>373</sup>

98. Further, CTIA's voluntary Internet Access Control Guidelines require participating carriers to provide consumers with parental control tools for wireless handsets that are designed to restrict access to content available via the public Internet or other public data networks.<sup>374</sup> With respect to this third-party content, the nationwide wireless carriers currently provide consumers with the ability to block all Internet access on their devices and are either providing or researching solutions to provide controls with the ability to limit specific Internet content or sites on consumers' devices (to be implemented on a carrier-by-carrier basis).<sup>375</sup> Although CTIA has developed both the Carrier Content Classification and Internet Access Control Guidelines, it emphasizes that implementation of these guidelines is left to the individual wireless carriers or third-party vendors.<sup>376</sup> Further, many of these tools cannot block or filter inappropriate user-generated content, such as "sexting."<sup>377</sup>

99. With respect to content controls provided directly by wireless carriers, CTIA explains that wireless carriers currently provide parents with many parental control tools that allow parents to control directly the content their child can access.<sup>378</sup> For example, Sprint provides a free content blocking control service that permits parents to restrict Internet access to only designated websites

(Continued from previous page) \_\_\_\_\_  
industry guidelines are available at: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>. Final Guidelines on COP are expected in October 2009.

<sup>371</sup> See CTIA Comments at 3-4.

<sup>372</sup> See *id.* at 4.

<sup>373</sup> See *id.* According to CTIA, "Restricted Carrier Content" consists of material that is generally recognized as appropriate only for adults 18 years of age or older, such as material that may contain strong violence or may be sexually explicit, or material that is legally restricted to persons at least 18 years of age, such as lotteries and gambling. *Id.*

<sup>374</sup> See *id.* at 5-6.

<sup>375</sup> See *NOI*, 24 FCC Rcd at 3354, ¶ 30. See also CTIA Comments at 6.

<sup>376</sup> See CTIA Comments at 5. Each of the four nationwide wireless carriers generally follows these guidelines in implementing their individual filtering and blocking technologies. See *id.* at 7-9.

<sup>377</sup> "Sexting" is used to describe texting of sexual images via mobile devices. Once the images are more widely distributed, there are unintended legal consequences to such distribution. Thierer, A., "Parental Controls & Online Protection: A Survey of Tools and Methods," PFF *Special Report*, Ver. 4, Summer 2009 (Thierer Report), at 111-112, available at <http://www.pff.org/parentalcontrols/>. As Thierer notes, neither laws nor parental controls are likely to be "of much help" in this area. "Legal responses are difficult to craft...[a]nd the only technological solution to this problem is for parents to simply not purchase a phone for their teen that has a camera," which is difficult given the proliferation of wireless handsets that include cameras. See *id.* at 112.

<sup>378</sup> See CTIA Comments at 6.

deemed appropriate for children 17 and under.<sup>379</sup> According to Sprint's Parental Controls web site, parents may manage this service either online or on the wireless handset itself.<sup>380</sup> T-Mobile offers Web Guard: a free service that restricts access to adult-oriented content.<sup>381</sup> According to T-Mobile's web site, Web Guard is an optional service available on specific rate plans only (targeting Web access data plans).<sup>382</sup> It blocks adult-oriented content (but not user-generated content), such as content featuring alcohol, drugs, gambling, pornography, mature content, violence, and weapons.<sup>383</sup> AT&T's MEdia™ Net Parental Control service allows parents to restrict access to inappropriate content.<sup>384</sup> Specifically, AT&T's service (which has no recurring charge to its customers) filters inappropriate Internet content to wireless devices, provided the user has a compatible handset.<sup>385</sup> Verizon Wireless offers a free service called Content Filters, which allows parents to set customized limits based on specific age levels: (1) "C7+" for content recommended for children ages seven and older (similar to TV-G); (2) "T13+" for children ages 13 and older (similar to TV-PG/TV 14 or PG 13 rated movies); and (3) "YA17+" for children ages 17 and older (similar to TV-MA or R-rated movies and explicit rated songs).<sup>386</sup> This service allows parents to ensure that their children receive only age-appropriate content over their Verizon Wireless device, including content accessible through the Internet (over Verizon Wireless' Mobile Web 2.0 Browser), V CAST Music and Video, and short code message campaigns.<sup>387</sup>

---

<sup>379</sup> See Sprint Comments at 2.

<sup>380</sup> See [http://nextelonline.nextel.com/en/services/safety\\_security/parental\\_control.shtml](http://nextelonline.nextel.com/en/services/safety_security/parental_control.shtml). On its web site, Sprint notes that access to certain parental control features varies, depending on the type of wireless handset used, and recommends that parents consult their phone's User Guide for further details.

<sup>381</sup> See T-Mobile Reply Comments at 2. See also CTIA Comments at 8.

<sup>382</sup> For more information on T-Mobile's Web Guard, see [http://www.t-mobile.com/shop/addons/services/information.aspx?PAsset=FamilyWireless&tp=Svc\\_Tab\\_FW101ProtectYourKids](http://www.t-mobile.com/shop/addons/services/information.aspx?PAsset=FamilyWireless&tp=Svc_Tab_FW101ProtectYourKids)

<sup>383</sup> See T-Mobile's Web Guard FAQs at: <https://support.t-mobile.com/doc/tm23350.xml?related=y&Referring%20Related%20DocID%20List%20Index=5&navtypeid=6&pagetypeid=7&prevPageIndex=9>.

<sup>384</sup> See CTIA Comments at 7; AT&T Comments at 7.

<sup>385</sup> See CTIA Comments at 7. See also AT&T's FAQ's on MEdiaNet at: [http://www.wireless.att.com/learn/messaging-internet/media-entertainment/faq.jsp#parental\\_controls\\_decide](http://www.wireless.att.com/learn/messaging-internet/media-entertainment/faq.jsp#parental_controls_decide). On its web site, AT&T states that it does not offer content that is obscene or pornographic in nature, but there is some MEdia Net content that may not be appropriate for those under age 18—like chat and dating sites—that the Content Filter will block when turned "on."

<sup>386</sup> See Verizon Comments at 7. According to Verizon Wireless's web site, the following content can be filtered: (1) "Explicit" labeled music on V CAST Music; (2) Content on V CAST Video; (3) Websites accessible via wireless device; and (4) Short code-based messaging campaigns (4 to 6 digit phone numbers that subscribers use to obtain content or participate in various programs. Standard messaging rates apply to short codes. Premium charges may apply for certain short codes). Verizon Wireless states: "Content from other sources, including Get It Now, is not consistently filtered by the service at this time. The service does not filter calls or messages sent by customers to other customers (this includes any content created by customers and sent directly by them to other customers) or content previously available on phones before the service was enabled." [http://support.vzw.com/faqs/Features%20and%20Optional%20Services/content\\_filtering.html#item1](http://support.vzw.com/faqs/Features%20and%20Optional%20Services/content_filtering.html#item1). See also [https://wbillpay.verizonwireless.com/vzw/nos/uc/uc\\_content\\_filter.jsp](https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_content_filter.jsp); PFF Comments at 65; CTIA Comments at 9.

<sup>387</sup> See Verizon Comments at 7. See also CTIA Comments at 9. On its web site, Verizon indicates that Content Filtering works on most mobile phones, most PDAs, and most PC cards, but will not work on BlackBerry® devices, any device with a static IP address or on search results provided through the Get It Now or Song ID search (continued...)

100. With respect to content controls created by third parties, a number of applications have been developed to filter Internet content accessed via wireless devices. Ace\*Comm's Content Patrol offers a third-party network-based solution that allows filtering of wireless web and Wireless Application Protocol ("WAP")-based content.<sup>388</sup> Further, several parental control applications have been developed for the iPhone platform,<sup>389</sup> which, in the United States, operates only on the AT&T network. One of these applications, the Mobicip browser (available to parents for a monthly fee), provides real-time content filtering at three pre-defined, age-based levels.<sup>390</sup> Further, Microsoft recently announced the Windows Marketplace for Mobile, which will allow parents to prohibit applications containing adult content, including applications featuring excessive violence, consumption of alcohol, sexual content, and excessive profanity.<sup>391</sup>

### 1. Using Content Controls

101. The *NOI* also requested comment on whether content controls were effective and easy to understand and activate by parents, and sought information on the extent to which parents use them.<sup>392</sup> According to PFF, the Yankee Group reports that 72 percent of teens between ages 13 and 17 already have a mobile phone.<sup>393</sup> The Commission did not receive any data on parental use of content controls for wireless devices. While we do not have precise data on parental use of content controls, according to a recent survey, among those teens whose parents are aware they go online through a cell phone, only one in five have parents that limit or control that online time and just over half have parents who have talked to them about Internet safety on their cell phone.<sup>394</sup> Wireless providers comment regarding the

(Continued from previous page)

capabilities. Additionally, the music filtering capabilities of the service do not work on devices with certain V CAST Music software (Music v01.0 or v01.01); and the Internet filtering capabilities will not work with devices utilizing Mobile Web 1.0, or on devices that use the Venturi data compression software, including phones tethered to PCs or PC cards, unless the compression software is turned off. Verizon Wireless notes that Content Filtering may not work outside the National Enhanced Services Rate and Coverage Area. See [http://support.vzw.com/faqs/Features%20and%20Optional%20Services/content\\_filtering.html#item1](http://support.vzw.com/faqs/Features%20and%20Optional%20Services/content_filtering.html#item1).

<sup>388</sup> See CTIA Comments at 10.

<sup>389</sup> See PFF Comments at 68; CTIA Comments at 11. These applications – Mobicip, Safe Eyes Mobile, and iWonder – consist generally of a browser that replaces the installed Apple browser on the device. See PFF Comments at 68. While PFF notes that these filtering tools currently work only with Apple's iPhone, it asserts that this "will likely change in coming months." See *id.* at 68-69.

<sup>390</sup> See CTIA Comments at 11; PFF Comments at 68 (noting that Mobicip costs \$9.99 for the premium version of its software). Another iPhone application, the Safe Eyes Mobile browser (which has a retail price of \$19.95), allows parents to choose from 35 categories to determine the specific types of content that will be allowed or blocked, and allows parents to change settings remotely through a web-based interface. See PFF Comments at 68. A third iPhone application, iWonder, works in a similar fashion to Safe Eyes Mobile, allowing parents to disable wireless web browsing or block access to certain web sites (and costs \$14.99). See CTIA Comments at 11; PFF Comments at 68.

<sup>391</sup> See Microsoft Comments at 11. Windows Marketplace for Mobile allows consumers to download applications for wireless phones running Microsoft's upcoming Windows Mobile 6.5 software.

<sup>392</sup> See *NOI*, 24 FCC Rcd at 3354, ¶ 31.

<sup>393</sup> See PFF Comments at 63.

<sup>394</sup> Cox Communications Teen Online & Wireless Safety Survey: Cyberbullying, Sexting, and Parental Controls (May 2009) at 49. The survey was conducted by Harris Interactive for Cox Communications, in Partnership with the National Center for Missing & Exploited Children® (NCMEC) and John Walsh, regarding teen (ages 13-18) use of the Internet and wireless devices. The survey found that about one in five teens go online via their wireless phone, and among those, one in five say that their parents are not aware that they do. *Id.* at 48. According to a (continued....)

ease with which parents can activate, use, and learn about carriers' content controls. Sprint and Verizon assert that their controls are easy to use and activate through the customer's wireless handset, the carrier's website, or by calling customer care.<sup>395</sup> AT&T notes that its content control service, "AT&T Smart Limits™," includes a suite of wireless parental controls and an online portal that explains all of the parental control features available for its services, including directions on how to use the controls for wireless, Internet, video and home phone services.<sup>396</sup>

102. The Commission also sought comment on how the content rating systems operate.<sup>397</sup> In response, the Commission received extremely limited information. As discussed above, a number of wireless carriers offer certain blocking or filtering technologies.<sup>398</sup> They do not, however, provide in their comments further specifics regarding the mechanisms used to filter inappropriate content.<sup>399</sup> CTIA notes that the Safe Eyes Browser system uses "a blacklisted website address categorization and filtering approach to prevent viewing of and visits to certain sites."<sup>400</sup> With respect to how content is rated, the nationwide wireless carriers appear generally to follow CTIA's guidelines. Specifically, Verizon states that its content classification levels are similar to TV Parental Guidelines and MPAA rating systems.<sup>401</sup> According to AT&T's web site, AT&T uses an internal content review process to determine whether content is appropriate for minors.<sup>402</sup> T-Mobile uses a third party vendor to assist in reviewing and blocking content for its Web Guard feature, which maintains the list of blocked URL's.<sup>403</sup> Microsoft also notes that the ESRB, which provides video games rating information, recently has begun rating games that are playable on mobile phone handsets.<sup>404</sup>

(Continued from previous page) \_\_\_\_\_

Nielsen survey, 62 percent of teens using mobile devices say that parents have "placed at least one restriction on their mobile use." See Nielsen, *How Teens Use Media*, June 2009, at 8-9. In both of these surveys, however, it is unclear whether parents are limiting their child's mobile phone/mobile Internet use via an advanced blocking technology, or through a parental rule (e.g., prohibiting mobile phone/Internet use at the dinner table).

<sup>395</sup> See Sprint Comments at 2-3; Verizon Comments at 7-8.

<sup>396</sup> See AT&T Comments at 6. See also [www.att.com/smartialimits](http://www.att.com/smartialimits).

<sup>397</sup> See *NOI*, 24 FCC Rcd at 3354, ¶ 31.

<sup>398</sup> See *supra* ¶¶ 98-100.

<sup>399</sup> Although the carriers do not describe in their comments how precisely the content is filtered, they do provide some specific information on their web sites regarding what type of content is filtered. For additional information on specific content controls, see the following web sites: AT&T (<http://www.wireless.att.com/learn/messaging-internet/media-entertainment/faq.jsp#controls>); Sprint ([http://nextelonline.nextel.com/en/services/safety\\_security/parental\\_control.shtml](http://nextelonline.nextel.com/en/services/safety_security/parental_control.shtml)); T-Mobile ([http://www.t-mobile.com/shop/addons/services/information.aspx?tp=Svc\\_Tab\\_IncludedServices&tsp=Svc\\_Sub\\_ContentControl](http://www.t-mobile.com/shop/addons/services/information.aspx?tp=Svc_Tab_IncludedServices&tsp=Svc_Sub_ContentControl)); and Verizon ([https://wbillpay.verizonwireless.com/vzw/nos/uc/uc\\_content\\_filter.jsp](https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_content_filter.jsp)).

<sup>400</sup> CTIA Comments at 11.

<sup>401</sup> See Verizon Comments at 7.

<sup>402</sup> See [http://www.wireless.att.com/learn/messaging-internet/media-entertainment/faq.jsp#parental\\_controls\\_decide](http://www.wireless.att.com/learn/messaging-internet/media-entertainment/faq.jsp#parental_controls_decide). AT&T notes it is also participating in CTIA's industry efforts to develop content ratings, which, according to AT&T, "may be used in conjunction with Parental Controls in the future."

<sup>403</sup> See T-Mobile's Web Guard FAQs at: <https://support.t-mobile.com/doc/tm23350.xml?related=y&Referring%20Related%20DocID%20List%20Index=5&navtypeid=6&pagetypeid=7&prevPageIndex=9>.

<sup>404</sup> See Microsoft Comments at 11.

## 2. Filtering Content Using Digital Watermarking

103. Digimarc and DWA suggest that digital watermarking would be an effective way to enable parents to filter inappropriate content accessible across various distribution platforms, including wireless devices.<sup>405</sup> Digital watermarking enables the use of any rating system, allowing parents to block or allow content based on a set of labels parents can select. Rating systems and their associated labels can be provided either by content owners, content distributors (such as satellite, cable, or the Internet), or vendors of devices, and digital watermarks from one vendor can work and coexist with other digital watermarks from other vendors.<sup>406</sup> Some consumers express support for a uniform rating system across all platforms.<sup>407</sup> Because digital watermarking allows ratings-related information to be embedded into the content itself,<sup>408</sup> it might allow parents more precise Internet blocking technologies than those technologies implementing CTIA's Internet Content Access Control guidelines, which enable parents to block access to specific web sites. As discussed above, however, some commenters express concern that digital watermarking could also be used for DRM functionality and that intellectual property licensing terms for this technology are unknown.<sup>409</sup>

### B. Non-Content-Based Blocking and Filtering Technologies

104. In addition to the content-based blocking technologies described above, the *NOI* also sought information on any other types of technologies currently available to consumers for use on wireless devices.<sup>410</sup> Commenters mention several technologies that allow parents to view the information children receive over their wireless devices.<sup>411</sup> For example, the "iWonder" browser, for use on Apple's iPhone, allows parents to view remotely from their own computer or wireless device the web sites that the child visits and also allows parents to disable wireless web browsing or block access to certain web sites.<sup>412</sup> As referenced in the *NOI*, eAgency's "Radar - My Mobile Watchdog" parental monitoring system is a handset-based solution that sends parents an alert when a child receives calls and messages from unauthorized or unapproved sources and also allows parents to view and archive remotely all of the text, e-mail, and instant messages that their child sends and receives.<sup>413</sup> Ace\*Comm's "Content Patrol™" service also offers a range of services that allow parents to restrict usage of wireless devices, such as restricting use to certain times of day or limiting the specific phone numbers a child can

<sup>405</sup> See, e.g., Digimarc Comments at 2, 4-5, 10; DWA Comments at 6. Digital watermarking is discussed in greater detail in Section II.C.4 above.

<sup>406</sup> See Digimarc Comments at 5; Digimarc Reply at 2, 4. Digital watermarks can carry both semantic information and a reference number and can block based on ratings. See Digimarc Comments 5-6. For example, when a mobile device is enabled to read the watermark, it can allow parents to set parameters of content accessibility, such as: Block all "Mature Audience" content and/or "look up sub-rating of designated 'Mature Audience' and block 'TV-14' and higher designations." See *id.* at 5.

<sup>407</sup> See, e.g., Comments of Nancy Brennan at 1; Robert Matthews at 1.

<sup>408</sup> See DWA Comments at 6.

<sup>409</sup> See *supra* ¶ 83. See also CEA Reply at 10-11; TiVo Reply at 3.

<sup>410</sup> See *NOI*, 24 FCC Rcd at 3354-55, ¶ 32.

<sup>411</sup> See, e.g., CTIA Comments at 10-11; PFF Comments at 66.

<sup>412</sup> See CTIA Comments at 11.

<sup>413</sup> See *id.* at 10; PFF Comments at 66. According to PFF, this service costs \$10 per month for one user or \$15 per month for an entire family. See PFF Comments at 66.

call.<sup>414</sup>

105. In addition to restricting access to inappropriate content or monitoring messages, wireless carriers themselves also provide tools to help parents set customized limits for each child. Although specific parameters – including cost of the service – vary by provider, these services allow parents to manage how and when children use their phones, including limitations on time, dollar amount, and number of messages or downloads a child receives.<sup>415</sup> Many wireless carrier plans also allow parents to place restrictions on the specific individuals that their children are permitted to contact on their mobile phones.<sup>416</sup> Below, we provide brief descriptions of the parental control limits offered by the nationwide wireless carriers, as well as a survey of location-based services and other technologies that have been developed to aid parents in monitoring and limiting their child's mobile phone usage.

### 1. General Limits on Wireless Phone Use

106. *AT&T*. With AT&T's Smart Limits for Wireless™, parents can set monthly limits on the number of text and instant messages their children send and receive; the amount of web-browsing allowed per billing cycle; the dollar amount of downloadable purchases (e.g., ringtones, games); and the times of day when the phone can be used for texting, browsing, or outbound calling.<sup>417</sup> Through this program, parents can also block messages or calls to certain numbers.<sup>418</sup>

107. *Sprint*. Sprint's free parental controls give parents the ability to (1) restrict premium content purchases; (2) disable data usage and access to the Internet; (3) disable text messaging entirely or block incoming text messages from specific numbers; and (4) limit incoming and outgoing voice calls to phone numbers specified in the handset's phone book.<sup>419</sup> Parents can also lock device features, such as the handset's camera, on particular wireless devices.<sup>420</sup>

108. *T-Mobile*. One of T-Mobile's services, Family Allowances<sup>SM</sup>, allows parents to manage their child's account activity to reduce overage charges and control their child's phone usage.<sup>421</sup> For a monthly fee, the Family Allowances<sup>SM</sup> service allows parents to assign allowances for minutes, messages, and downloads to multiple lines on the account.<sup>422</sup> In addition, parents can set up to ten "Always Allowed"<sup>SM</sup> and ten "Never Allowed"<sup>SM</sup> numbers, and block usage during certain times of the

---

<sup>414</sup> See CTIA Comments at 10.

<sup>415</sup> See PFF Comments at 65.

<sup>416</sup> See *id.* at 65-66.

<sup>417</sup> See AT&T Comments at 6; see [www.att.com/smartlimits](http://www.att.com/smartlimits). See also CTIA Comments at 7; PFF Comments at 65.

<sup>418</sup> See AT&T Comments at 6; see also CTIA Comments at 7; PFF Comments at 65.

<sup>419</sup> See Sprint Comments at 2. See also [http://nextelonline.nextel.com/en/services/safety\\_security/parental\\_control.shtml](http://nextelonline.nextel.com/en/services/safety_security/parental_control.shtml); CTIA Comments at 8.

<sup>420</sup> See Sprint Comments at 2; CTIA Comments at 8.

<sup>421</sup> See T-Mobile Reply at 1; see [http://www.t-mobile.com/shop/addons/services/information.aspx?PAsset=FamilyWireless&tp=Svc\\_Tab\\_FW101FamilyAllowances](http://www.t-mobile.com/shop/addons/services/information.aspx?PAsset=FamilyWireless&tp=Svc_Tab_FW101FamilyAllowances).

<sup>422</sup> See T-Mobile Reply at 1-2.

day (in most cases).<sup>423</sup> T-Mobile also offers – free of charge – its Message Blocking Service, which allows parents to block incoming and outgoing text messages (SMS), picture messages (MMS), instant messages (IM), and e-mail.<sup>424</sup>

109. *Verizon Wireless.* Verizon Wireless provides “Usage Controls,” which, for a monthly fee per line, allow parents to: (1) limit the times of day during which their child can use messaging or wireless data services; (2) block calls or messages to or from certain phone numbers; (3) set monthly voice minute and messaging allowances and receive free alerts when a child approaches or reaches the allowance; and (4) designate trusted numbers from which a child can always be reached, even outside of the designated time of use and regardless of usage allowances.<sup>425</sup>

## 2. Location-Based Services and Other Technologies

110. CTIA has developed a set of Consumer Best Practices guidelines to protect user privacy for Location-Based Services.<sup>426</sup> Many wireless carriers offer global positioning system (“GPS”) tracking technology in their mobile handsets, which allows parents to locate their children and monitor their whereabouts.<sup>427</sup> Sprint’s Family Locator service allows parents to monitor a child’s location by using the GPS chip in the mobile phone.<sup>428</sup> Verizon Wireless offers the Chaperone<sup>SM</sup> Family Locator service, a tool that helps parents monitor the location of a child’s wireless phone at all times using either the Chaperone<sup>SM</sup> Website or the Chaperone<sup>SM</sup> Parent application on parents’ own mobile phones.<sup>429</sup> The Chaperone<sup>SM</sup> service also includes Child Zone capabilities, which allow parents to establish geographical boundaries around specific locations, such as school, home, or soccer practice.<sup>430</sup> In addition to carrier-provided services that assist parents in tracking their child’s location, a number of third parties offer location-based services. The Wherify “Wherifone” offers GPS location tracking via the Internet, and

<sup>423</sup> See *id.* at 1-2; CTIA Comments at 8-9. “Always Allowed”<sup>SM</sup> numbers are reachable even when a user has exceeded a set maximum, and 911 calls do not count against the allowed numbers and minutes. See CTIA Comments at 8-9.

<sup>424</sup> See T-Mobile Reply at 2-3. See also CTIA Comments at 8.

<sup>425</sup> See Verizon Comments at 8; CTIA Comments at 9. See also [https://wbillpay.verizonwireless.com/vzw/nos/uc/uc\\_home.jsp](https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_home.jsp). Parents can customize these settings for each line on the account. Designated trusted numbers are limited to other lines on the same account.

<sup>426</sup> See CTIA Comments at 18. According to CTIA, under these guidelines, Location-Based Services providers must give notice to users about how location information will be used, disclosed, etc., and must give users the opportunity to give their consent prior to certain uses (such as disclosing information to third parties). See CTIA Comments at 18-19. These guidelines assist parents by ensuring that social mapping and networking services do not allow unauthorized individuals to monitor their children’s whereabouts. See PFF Comments at 69-70.

<sup>427</sup> See PFF Comments at 65-66.

<sup>428</sup> Sprint’s service costs 5 dollars monthly per family. See Sprint Comments at 2. See also [http://www.nextel.com/en/services/gps/familv\\_locator.shtml](http://www.nextel.com/en/services/gps/familv_locator.shtml).

<sup>429</sup> See Verizon Comments at 8

<sup>430</sup> See *id.* See also [http://products.vzw.com/index.aspx?id=fnd\\_chaperone](http://products.vzw.com/index.aspx?id=fnd_chaperone); CTIA Comments at 9; PFF Comments at 68. When a child carrying a registered Chaperone service mobile phone arrives at or leaves the Child Zone, the parent receives a notification via text message. See Verizon Comments at 8. Parents can elect to receive text message alerts notifying them of the location of the child’s phone at a specific date/time, similar to a curfew check. See *id.*

includes an SOS panic button for emergencies.<sup>431</sup> Guardian Angel Technology produces a GPS mobile phone that also allows parents to monitor their children's movements via the Internet.<sup>432</sup> In addition to using Location-Based wireless services to monitor one's child, another application is "social mapping." Social mapping allows subscribers to find others on a digital map and then instantly network with those individuals through social networking utilities.<sup>433</sup> CTIA and the industry are currently working to create safeguards to ensure that information over social mapping networks is not shared inappropriately.<sup>434</sup>

111. In addition to usage controls available for wireless services and location-based services, specific mobile devices have been designed for younger users. For example, Firefly Mobile has created a voice-only phone for very young children that allows them to call their parents and emergency services via pre-programmed numbers that are represented by icons on the mobile phone.<sup>435</sup> Verizon Wireless's "Migo," like the Firefly Mobile phone, also has a limited number of buttons for parents to program.<sup>436</sup> Enfora's TicTalk phone (in partnership with the educational toy maker LeapFrog Enterprises) allows parents to restrict numbers that can be called only during certain times of the day and determine at what times during the day the phone can ring.<sup>437</sup>

### C. Open Platform Issues

112. The *NOI* also sought comment on how blocking and filtering will be affected as wireless carriers move toward open platforms.<sup>438</sup> CTIA asserts that wireless consumers have unprecedented access to "open" third-party devices, content, and applications.<sup>439</sup> Although not commenting in this

<sup>431</sup> See PFF Comments at 67. The "Wherifone" also allows parents to program phone numbers and can restrict the downloading of games and text messages. See *id.*

<sup>432</sup> See *id.* The Guardian Angel GPS phone allows parents to keep a record of their child's precise movements for a 30-day period. See *id.* For instance, when a child is traveling in a car, the phone can monitor how fast the car is going and the direction in which it is heading. See *id.*

<sup>433</sup> See PFF Comments at 69; Thierer Report at 110-111.

<sup>434</sup> For example, Google, Loopt, and Helio have already established user privacy safeguards. See CTIA Best Practices and Guidelines for Location-Based Services, [www.ctia.org/business\\_resources/wic/index.cfm/AID/11300](http://www.ctia.org/business_resources/wic/index.cfm/AID/11300). See, e.g., Loopt's safety and privacy guide, <https://loopt.com/loopt/beSafe.aspx>.

<sup>435</sup> See PFF Comments at 67 (the Firefly Mobile phone contains only five buttons, two of which "have small icons symbolizing Mom and Dad...[and] comes in several colors and contains a variety of accessories geared toward kids").

<sup>436</sup> See *id.* at 68.

<sup>437</sup> See *id.* at 67. Parents can also enter phone numbers that children can call at any time of day. See *id.*

<sup>438</sup> See *NOI*, 24 FCC Rcd at 3354-55, ¶ 32. In the *700 MHz Second Report and Order*, 22 FCC Rcd 15289 (2007), the Commission adopted an "open platform" rule that requires licensees of the Upper 700 MHz Band C Block to allow consumers to use the handset of their choice and download and use the applications of their choice, subject to certain reasonable network management conditions that allow the licensee to protect the network from harm. Following adoption of this rule, some wireless carriers have announced that they will voluntarily make their networks more open to devices and/or applications.

<sup>439</sup> See CTIA Comments at 16. Further, CTIA notes that "As open device and application initiatives take hold in the marketplace, CTIA expects both carriers and third party vendors will continue to focus on the task of introducing groundbreaking technologies that not only provide additional open platforms and applications, but also on providing a new generation of parental controls that are as effective in an open environment as they are within a carrier's walled garden." *Id.* at 17.

proceeding, other entities have recently criticized the claims of “openness” of wireless networks in related Commission proceedings.<sup>440</sup> CTIA notes that wireless carriers have made great strides in ensuring that third-party content filtering applications and access controls can be compatible with wireless devices and services.<sup>441</sup> CTIA also asserts that parents can independently download third-party parental control solutions to their wireless devices through various sources, including wireless “app stores,” web sites, and other outlets.<sup>442</sup>

#### D. Future Developments

113. The *NOI* also sought information on blocking or filtering technologies for wireless devices that are currently in development.<sup>443</sup> Although the record on this issue was scant, commenters briefly addressing the issue predict that more advanced filters and access controls for wireless devices will be developed.<sup>444</sup> Given the competition within the wireless industry, however, carriers report that they cannot disclose their specific competitive offerings prior to launch.<sup>445</sup> Some individual commenters support extending filtering technology, such as TVGuardian, to mobile devices.<sup>446</sup> Further, some individuals indicate they are willing to pay a modest fee for this service – less than \$5 for 6 months, for example.<sup>447</sup>

#### E. Educational Efforts

114. In the *NOI*, the Commission requested information on how wireless providers educate consumers on existing filtering technologies, as well as how consumer and trade organizations should publicize the development, deployment, and use of filtering technologies.<sup>448</sup> CTIA reports that wireless carriers such as Sprint have worked with the National Center for Missing & Exploited Children (“NCMEC”) and the National Education Association (“NEA”) to develop educational tools and initiatives aimed to improve wireless and Internet safety awareness.<sup>449</sup> Specifically, Sprint’s

---

<sup>440</sup> See, e.g., Letter from Christopher Libertelli, Skype S.A.R.L., to Julius Genachowski, Chairman, FCC, RM-11361, WT Docket No. 09-66 (Jun. 29, 2009); Letter from Ben Scott and Chris Riley, Free Press, to Michael Copps, Acting Chairman, FCC, WC Docket No. 07-52 (Apr. 3, 2009).

<sup>441</sup> See CTIA Comments at 9-10.

<sup>442</sup> See *id.*

<sup>443</sup> See *NOI*, 24 FCC Rcd at 3354-55, ¶ 32.

<sup>444</sup> See, e.g., CTIA Comments at 12 (“more advanced filters and access controls are most certainly on the way”); T-Mobile Reply at 3 (“T-Mobile continues to enhance [its parental control] offerings, as well as explore other initiatives that would be useful for parents in managing their children’s online experiences”); PFF Comments at 70.

<sup>445</sup> See Sprint Comments at 3 (“Sprint does have additional parental control features under development that it intends to offer parents in the future. But as the Commission will appreciate, given the intense competition within the wireless industry, Sprint cannot disclose its competitive offerings prior to launch.”).

<sup>446</sup> See, e.g., Comments of Brenda Prosser at 1; Diane Finnan at 1; William Bauza at 1; Art Gillespie at 1.

<sup>447</sup> See, e.g., Comments of Curtiss Wilson at 1; Barbara Jenkins at 1; James Sammons at 1.

<sup>448</sup> See *NOI*, 24 FCC Rcd at 3355, ¶ 33.

<sup>449</sup> See CTIA Comments at 8. In addition to ways to make a child’s wireless experience safer, in 2005 the wireless industry and The Wireless Foundation partnered with the United States Department of Justice and NCMEC to create the Wireless AMBER Alerts™ Program, a “key example of the wireless industry’s commitment to harnessing the convenience and ubiquity of wireless technology to safeguard children.” *Id.* at 13. The Wireless AMBER Alerts™ (continued....)

4NetSafety<sup>SM</sup> program provides individuals with the tools and information they need to teach minors how to use the Internet more safely.<sup>450</sup> Through this program, individuals can also access (for free) the bNetS@vy, an online resource created by the NEA Health Information Network (“HIN”) that offers adults information to help teach children – and pre-teens in particular – how to navigate the Internet safely.<sup>451</sup> Verizon Wireless notes that on its website it has posted a set of recommendations about steps parents can take to control their children’s access to certain materials – regardless of the technology platform used.<sup>452</sup>

115. Similarly, Cox’s “Take Charge” program includes a web site to educate parents, which includes a list of chat acronyms that children use on cell phone text messages and instant messages.<sup>453</sup> Cox states that in 2009, its Take Charge program will emphasize safety on wireless phones and will focus on smartphones’ Internet access and the importance of using parental controls with mobile devices.<sup>454</sup> In its comments, Cox notes that it will conduct new research on teen behavior patterns on the Internet using mobile devices.<sup>455</sup> In May 2009, Cox released a report summarizing its findings.<sup>456</sup>

116. In addition, the Wireless Foundation, a non-profit organization established by CTIA’s member companies in 1991, educates children, parents, teachers, and policymakers about the tools the wireless industry provides to ensure that children are safe while using wireless technology.<sup>457</sup> For example, it maintains a “Wireless Online Safety” section on its website, which contains information for

(Continued from previous page) \_\_\_\_\_

Program provides free text messages available to wireless subscribers who have signed up to receive such messages when a child has been abducted, thereby allowing alert recipients to serve as the extra “eyes and ears that public safety officials vitally need” in such situations. *See id.*

<sup>450</sup> *See* CTIA Comments at 8; Sprint Comments at 3-4.

<sup>451</sup> *See* Sprint Comments at 4.

<sup>452</sup> *See* Verizon Comments at 10-11 (“These include: talking to children to create an environment that allows honest and open dialog with children about their media activities and experiences; using all available parental control software to filter out potentially harmful, inappropriate, or offensive content; surfing the Internet, watching TV, and enjoying wireless content together with their children to help them learn to recognize and anticipate the risks associated with certain online content; using usage controls and parental controls software to monitor television, personal computer, phone, and wireless use and setting limits where appropriate; moving the TV and personal computer to open areas of the home, with the screens facing out and visible at all times, to better monitor children; and joining their children’s online social networks so that parents can make sure they know who their children’s online and wireless friends are”). *See* <http://parentalcenter.verizon.radialpoint.net/>.

<sup>453</sup> *See* Cox Comments at 5. Cox notes a 2005 survey that showed that only five percent of the surveyed parents knew that “POS” was an alert to others in the chat that there was a “Parent Over their Shoulder” and that only four percent knew that “P911” was an alert that a parent was nearby. *See id.*

<sup>454</sup> *See id.* (Cox “continues to examine and evaluate emerging content filtering technologies, such as editable video-on-demand content and technologies using customizable rating systems”).

<sup>455</sup> *See id.* at 11.

<sup>456</sup> *See* Cox Communications Teen Online & Wireless Safety Survey: Cyberbullying, Sexting, and Parental Controls (May 2009), available at [http://www.cox.com/takeCharge/includes/docs/2009\\_teen\\_survey\\_internet\\_and\\_wireless\\_safety.pdf](http://www.cox.com/takeCharge/includes/docs/2009_teen_survey_internet_and_wireless_safety.pdf).

<sup>457</sup> *See* CTIA Comments at 13. Further, in 2008, CTIA created the Wireless Child Safety Task Force, which aims to further deter child pornography on wireless networks while safeguarding consumer privacy. *See id.* at 15. This Task Force also plans to develop an educational initiative to inform parents and children about best practices for safe wireless Internet behavior. *See id.* CTIA has submitted the Wireless Child Safety Task Force for inclusion in the International Telecommunications Union’s “Child Online Protection Initiatives Around the World” program. *See id.*