Comments in Answer to FCC NPR WC Docket No. 13-184

Modernizing the E-rate Program for Schools and Libraries

Specifically regarding CIPA in Section VI. *Other Outstanding Issues* ¶270-275

Introduction

I am a parent who led a successful campaign against my local school district's* policy of providing 5th-8th grade students with portable computers that provided no protection measures from harmful content when used away from school grounds. For nearly a full school year (2011-12) parents' complaints with the school district administration, BOE, Colorado Department of Education and USAC (see cases 22-269647 and 22-269661) failed to stop our district from continuing to provide minors with completely unrestricted portable computers. The Colorado legislature, however, responded to our request for intervention and passed an amendment to Colorado's own CCIPA law that made such reckless technology deployments illegal—creating new law explicitly requiring all Colorado schools to provide protection measures on portable technology devices whenever minors access the internet *"…from any location*" (An Act; House Bill 12-1240, Concerning Statutory Changes to K-12 Education)
*Manitou Springs, Colorado D-14

For a more detailed account of this event and citations of other districts' sordid experiences with minors accessing harmful content on school issued portable computers please see
http://safelibraries.blogspot.com/2012/12/SchoolsMustFilter.html

Please also see the legal arguments made against D-14's "no protection" policy in a memorandum written by *Morality in Media* General Counsel Robert Peters at
http://safelibraries.blogspot.com/2012/04/school-issued-apple-ipads-allow-porn-in.html

Comments Regarding Section VI. ¶ 275

¶ 275 states in part:

> *Should the CIPA requirements only apply when the computer is used on campus, because the school is not seeking E-rate support for the off-campus portion of the cost of the data plan? We also seek comment on whether our existing CIPA-related rules need to be amended to cover these off-campus use situations.*

Existing CIPA language repeatedly stipulates that all computers have protections without exception for portables away from campus:

> *…includes the operation of a technology protection measure with respect to any of its computers with Internet access…*
> *…enforcing the operation of such technology protection measure during any use of such computers…*

CIPA clearly requires schools to provide minors with computers that afford those minors certain safety measures on *any computer* and *any use of such computer* in order for those schools to qualify for E-rate funding—with no provision for exception for portable computers. CIPA does not specify that the connectivity or networks subsidized by E-rate must include protection measures, but rather, in more robust fashion, that the computers used by minors be made appropriately safe—without exception.

It is not unusual for the federal government to impose requirements upon recipients of federal funding that are not entirely related to the use of such funding. The federal government, for example, requires that states adopt and enforce law specifying a .08 blood alcohol content level as the standard for criminal drunk driving as a requirement to receive federal transportation appropriations. While the U.S. Congress might have limited the scope of the .08 BAC mandate to federally subsidized or owned highways, it did not. The Congress required that states establish the .08 BAC standard for driving on any public roadway—without exception.

CIPA-related rules must be amended to clear any ambiguity in the law; the rules must explicitly require CIPA compliance on any school-supplied computer in *"these off-campus use situations."*

Comments Regarding Section VI. ¶ 273

¶ 273 states in part:

> *For example, should we consider as a limiting principle the language in CIPA that requires the operation of a technology protection measure that provides protection against access to "visual depictions" that are obscene, child pornography, or harmful to minors?*

CIPA only requires filtering of "*harmful*" "*pictures...or other visual depictions*", and furthermore provides a limiting definition of *"harmful to minors"* as only relating to sexual content.

Without amendment to CIPA, or FCC rules, even the youngest elementary students will continue to be provided devices by their schools upon which they find music replete with explicit sex, violence and drug use, or visit with predatory pedophiles in chat rooms, or view demonstrations of the "choking game" and persons being stoned to death or burned alive.

The FCC and Congress should amend rules and law to stipulate that any technology device used by minors, that is in any way supplied or subsidized by a school or library receiving E-rate subsidies (or for that matter receiving federal money of any kind) must meet the following requirements for policy addressing internet content protections:

--Content blocking/filtering measures must function during a minor's internet use at any location on any network accessible to the technology device.

--A description of the protection measures employed by the school or library must be published and available for public review to include description of what settings are being used on devices used by minors of various age and grade level.

--Protection measures must include the means to block/filter content that is age inappropriate or harmful to minors including but not limited to audio, video, images or text containing, offering or portraying age inappropriate violence, sexual material, gaming, drug use, social networking, products or services.

Conclusion

Parents have limited ability to protect their children from harmful experiences online, particularly when their local school district issues portable computers that lack any form of content protection measure —as our district once did. Despite the petitioning efforts of parents, attorneys' memoranda, and complaints filed with State and federal agencies, our children had to use unsafe, unrestricted computers in order to perform their work away from school as part of a "24/7" technology program. It literally took an act of Colorado's Congress to finally force our district to adopt policy requiring protections on portable computers that work *"from any location."*

Parents across this nation should not have to suffer the same divisive ordeal that we did in gaining reasonable protections on portable computers, and children need not continue to suffer the harm caused by the unrestricted computers provided by schools. The existing language of CIPA already provides cause for explicit rules asserting the applicability of CIPA to school issued portable computers used away from school grounds. Additionally, FCC rule makers and federal lawmakers alike must broaden the scope of CIPA to address changing technology and expand the definition of what constitutes *"harmful to children."*

Not so long ago parents could walk the isles of the school library or request a list from the school librarian and gain a functional understanding of the materials available to their children at school. The internet offers children the equivalent of a nearly infinite library, but parents and schools must yet maintain some understanding and control of the content available to their children; some minimum requirement for protections against harmful content, beyond just that of sexual images, must apply to all school issued computers including portable ones. The internet can be a tremendously beneficial educational tool for our children, and with appropriate law and technology a child's time online can be made a much more secure and enriching experience.

Attached Exhibit A is the *Web Content Filtering* control panel and content categories currently offered by a free content control service called OpenDNS that exemplifies the range and flexibility of content control technology readily and affordably available--in this case at no cost to the user whatsoever.

Regards,

Joe Morin
Joe@i1u1.com
719-684-2596 ph

Exhibit A

OpenDNS Web Content Filtering Control Dashboard

Choose your filtering level

High	Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. **26** categories in this group - View - Customize
Moderate	Protects against all adult-related sites and illegal activity. **13** categories in this group - View - Customize
Low	Protects against pornography. **4** categories in this group - View - Customize
None	Nothing blocked.
Custom	Choose the categories you want to block.

Academic Fraud	Government	Religious
Adult Themes	Hate/Discrimination	Research/Reference
Adware	Health and Fitness	Search Engines
Alcohol	Humor	Sexuality
Anime/Manga/Webcomic	Instant Messaging	Social Networking
Auctions	Jobs/Employment	Software/Technology
Automotive	Lingerie/Bikini	Sports
Blogs	Movies	Tasteless
Business Services	Music	Television
Chat	News/Media	Tobacco
Classifieds	Non-Profits	Travel
Dating	Nudity	Typo Squatting
Drugs	P2P/File sharing	Video Sharing
Ecommerce/Shopping	Parked Domains	Visual Search Engines
Educational Institutions	Photo Sharing	Weapons
File Storage	Podcasts	Web Spam
Financial Institutions	Politics	Webmail
Forums/Message boards	Pornography	
Gambling	Portals	
Games	Proxy/Anonymizer	
German Youth Protection	Radio	