Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of Schools and Libraries Universal Service Support Mechanism
CC Docket No. 02-6

Comments Submitted by:
Nancy Willard, M.S., J.D. Director Center for Safe and Responsible Internet Use
Web site: <http://csriu.org>.
E-mail: <nwillard@csriu.org

Submitted: 11/26/09

Regulations Addressing Internet Safety Education Requirements

Control of Content

The proposed regulations addressing Internet safety education could benefit from the addition of language similar to that which you have proposed under the section addressing "harmful to minors" regarding local control of control. Local school officials should have the authority to make the determination of what the content of such education should be, including when subjects should be introduced in light of developmental and Internet use patterns.

The language of the statute implies that school districts must teach kindergartners about safety on social networking websites and in chat rooms, as well as cyberbullying. As these young students are just learning their alphabet, it is highly unlikely that they are engaged in social networking, chatting, or cyberbullying. In fact, the most commonly used social networking sites do not allow registration until age 13. Popular children's sites such as WebKinz and Club Penguin could be called "chat rooms" but most people do not think of them as chat rooms.

The following language is suggested: "A determination of the content of education to be provided regarding appropriate online behavior shall be made by the school board, local educational agency, library, or other authority responsible for making the determination . No agency or instrumentality of the United States Government may establish criteria for making such determination; review the determination made by the certifying school, school board, local educational agency, library, or other authority; or consider the criteria employed by the certifying school, school board, local educational agency, library, or other authority in the administration of the schools and libraries universal service support mechanism."

Data Reporting

One major provider of Internet safety education, I-Safe, is advising districts that an advantage of using their Internet safety instructional materials is data reporting. Their site advertises < http://isafe.org/channels/sub.php?ch=ed&sub_id=erate> that their product provides:

> Documentation. Independent third party records from i-SAFE indicate which teachers at each district school are teaching i-SAFE's E-Rate lessons. Each school receives an E-Rate Internet Safety Education Certificate for their files. See sample below.
> End of year audit report. A comprehensive verifiable report backing up the E-Rate Certificate with i-SAFE's E-Rate Audit Report, which details school, teacher, Internet safety topic and date.

I-Safe has engaged in a significantly aggressive email messaging campaign to create the misperception that such data collection and verifiable reports are necessary to ensure the continued receipt of E-Rate funds and that if districts are not able to verify that every students has received the necessary instruction, districts could lose their E-Rate funds. .

In the prior FCC CIPA regulations, you stated: “Because we concur that these data collection and reporting requirements fall outside the requirements of CIPA, we decline to impose such requirements on recipients. As we have stated previously, we are confident that local authorities will take the appropriate steps to ensure that they have complied with CIPA's requirements.”

Given the extent to which misinformation has been disseminated, it would be helpful for school districts if the FCC were to reiterate this statement in the context of this new requirement to provide Internet safety education.

Public Notice and Hearing Requirements
Section 254(h)(5)(A)(iii) of CIPA establishes that a school, school board, local educational agency, or other authority with responsibility for administration of the school, shall provide reasonable public notice and hold at least one public hearing or meeting to address a proposed Internet safety policy.

You have failed to clarify whether a notice and hearing is necessary to amend the Internet safety policy to incorporate the new provision for Internet safety education. Presumably, it is. However, information to this effect would likely be advisable, for example: “Public notice; hearing. A school or library shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy, *or amendment thereto*.”

Additional Comments on Local Control and Disabling

Your request for comments under paragraph 14 and paragraphs 10 - 12, appear to reflect concerns about how CIPA is actually implemented in the schools. Such concerns are very legitimate. In the vast majority of schools, the “technology protection measure” required under CIPA have been implemented in a manner that is preventing teachers and students from accessing relevant Internet resources and is preventing schools across the country from establishing 21st century learning environments that are so necessary to prepare our students for success in their future, as well as preventing the U.S. from ensuring its future effectiveness and competitiveness in the global marketplace and society.

National Research Council (NRC) released its report entitled Youth Pornography and the Internet in 2002 <http://bob.nap.edu/html/youth_internet/>. Many of its findings describe concerns that remain present today:

> All filters-those of today and for the foreseeable future-suffer (and will suffer) from some degree of overblocking (blocking content that should be allowed through) and some degree of underblocking (passing content that should not be allowed through). While the extent of overblocking and underblocking will vary with the product (and may improve over time), underblocking and overblocking result from numerous sources, including the variability in the perspectives that humans bring to the task of judging content.
>
> (F)ilters can be highly effective in reducing the exposure of minors to inappropriate content if the inability to access large amounts of appropriate material is acceptable.

> In an educational setting, the restrictions on information flow associated with filters may lead to substantial problems with teachers and librarians who are trying to develop useful and relevant educational activities, assignments, projects, and so on. Indeed, some teachers reported to the committee during site visits that sometimes their lesson preparations were hampered by the fact that their Internet access was filtered at school In other cases, when they prepared a lesson plan at home (with unfiltered access), they were unable to present it at school because a site they found at home was inaccessible using school computers.

The following statement was recently posted by Julie Evans, director of the Speak Up Project on a discussion group hosted by the National Computer Security Alliance:

> Many of you are already familiar with our Speak Up Project (http://www.tomorrow.org/speakup/index.html) where we collect and report on the authentic, unfiltered views of K-12 students, teachers, parents and administrators about 21st century education and the use of technology, in school and out of school. Since 2003, Speak Up has received over 1.5 million surveys from education stakeholders from all 50 states and also from schools worldwide. ... We ask K-12 students on the Speak Up surveys each year what are the major obstacles that prevent you from using technology at your school. The top response each year since 2003 has been the same – filters and firewalls that block website that I need for learning (56% of high school students for example chose this response – Speak Up 2008 data). [Message sent to group 11/11/2009]

Thus, while CIPA was enacted for laudable reasons, close to 60% of U.S. students think that the implementation of filtering, as required under CIPA with obvious concerns predicted by the NRC, is THE MAJOR obstacle to using technology at school for their learning!

What appears to have happening in schools across the country is that the Internet came into schools "holding the hand" of CIPA. School officials presumed that filtering was an effective tool for Internet use management, so in addition to blocking the material required to be blocked under CIPA, filters are being used in an attempt to manage all student and staff internet use. Further, under fear of the potential of losing E-Rate funding, schools are aggressively blocking all categories of material if their is a faint possibility that some sites included in that category could have adults material (see discussion on blogs below) and they are closely controlling the ability to override the filter to provide access to material that is perfectly appropriate.

As a result of this, too often teachers have had the experience of working hard on a lesson while at home only to come to class to find the sites blocked. Several experiences of this nature have led many teachers to simply go back to their textbooks and avoid any instruction that would involve Internet resources. Students, likewise, often find the Internet resources necessary to write a research paper blocked when they try to write the paper in the library computer lab. So they wait until they are at home with unfettered Internet access for these activities. While at school, then, Internet use has become "Internet recess - entertainment or socializing use. It is during Internet recess, that misuse occurs.

Essentially, because of how CIP{A has been implemented in schools, the billions of dollars in E-Rate funds for technology in schools is not having anywhere near the positive impact it could have on student learning and the improvement of instruction..

Constitutional Ramifications

Students in the public schools do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate." [*Tinker v. Des Moines Independent Community School Dist.*, 393 U.S. 503

(1969)]. However, the courts have recognized that the First Amendment rights of students in the public schools are not the same as the rights of adults in other settings and must be "applied in light of the special characteristics of the school environment." [*Bethel School District No. 403 v. Fraser*, 478 U.S. 675 (1986)].

Supreme Court standards related to the importance of student access to information were set forth in the case of Board of Education, Island Trees Union Free School District No. 26 v Pico [457 US 853 (1982)]:

> In our system, students may not be regarded as closed-circuit recipients of only that which the State chooses to communicate. ...[School] officials cannot suppress 'expressions of feeling with which they do not wish to contend. ... In brief, we hold that local school boards may not remove books from school library shelves simply because they dislike the ideas contained in those books and seek by their removal to ‘prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion.’ Such purposes stand inescapably condemned by our precedents.

Clearly, at this point in our society, the access to the Internet in school serves a similar, but more expansive, role of that of a school library in providing students with access to information that is vital to education and preparation for adulthood.

The Supreme Court addressed the importance of local school control in *Pico* as follows.

> The Court has long recognized that local school boards have broad discretion in the management of school affairs. ... (B)y and large, "public education in our Nation is committed to the control of state and local authorities," and that federal courts should not ordinarily intervene in the resolution of conflicts which arise in the daily operation of school systems. ... (W)e have repeatedly emphasized . . . the comprehensive authority of the States and of school officials . . . to prescribe and control conduct in the schools.

The primary reason offered by the justices who dissented from the decision in *Pico* was deference to local school authorities. Chief Justice Burger stated:

> We can all agree that as a matter of educational policy students should have wide access to information and ideas. But the people elect school boards, who in turn select administrators, who select the teachers, and these are the individuals best able to determine the substance of that policy. ... A school board is not a giant bureaucracy far removed from accountability for its actions; it is truly "of the people and by the people."

The issue of the inappropriate delegation of decision-making authority to filtering companies was addressed in the case of *Mainstream Loudoun v. Board of Trustees of the Loudoun County* [2 F. Supp. 2d 783 (ED Va. 1998)]. This case also found the use of filtering software in a public library to be unconstitutional.

> The degree to which the (library's filtering) Policy is completely lacking in standards is demonstrated by the defendant's willingness to entrust all preliminary blocking decisions -- and, by default, the overwhelming majority of final decisions -- to a private vendor,... . Although the defendant argues that (the filtering product) is the best available filter, a defendant cannot avoid its constitutional obligation by contracting out its decision making to a private entity. Such abdication of its obligation is made even worse by the undisputed facts here. Specifically, defendant concedes that it does not know the criteria by which (filtering company) makes its

> blocking decisions. (See statement in deposition) stating that (the filtering company) has refused to provide defendant with the criteria it uses to block sites). It is also undisputed that (the filtering company) does not base its blocking decisions on any legal definition of obscenity or even on the parameters of (the library's) Policy.

While the U.S. Supreme Court upheld the constitutionality of CIPA, [[*United States v. ALA*, 539 U.S. 194 (2003] despite despite documented concerns of overblocking, because of the ease by which the filter could be overridden.

Issues of Concern
The issues that must be considered include:

- The lack of any real local control over blocking decision-making or accountability for such decision-making on the part of filtering companies.

- The rapid expansion of Web 2.0 sites where users are easily able to post material. While most large sites that host blogs or allow people to post videos and the like have restrictions against posting of adult material, some of the material that could be posted could fall within the definition of “harmful to minors.”

- The recognition that blocking isn’t working because students (generally not adult staff) are easily able to bypass the filter using bypass technologies developed with funding by the US Government to support Internet access by dissidents in Asia and the Middle East, which is resulting in even more aggressive blocking in a vain attempt to address the unauthorized bypass concerns.

- Substantial confusion over issues over overriding the filter to provide access to inappropriately blocked sites.

Illusory Local Control - No Public Accountability
Schools are not making the decisions about what students can or cannot access. By default, these decisions are being made by private sector filtering companies that protect what and how they block as proprietary information and are not held publicly accountable. In the overwhelming majority of schools, there is no local control of content other than the selection of categories to be blocked.

In its proposed regulations, the FCC appears to desire to perpetuate the myth that the school board or local educational agency, other authority has any control over what material is deemed inappropriate or harmful for minors. Such control is illusory. The only control local officials have is in selecting what categories to be blocked. Such selection is made under the following conditions:

- The category lists maintained by the filtering companies are considered to be proprietary information, and hence are unavailable to school officials or the general public for review. When school officials select categories they do so not really know what they are blocking. Some examples from the M86 categories:

  Terrorist/Militant/Extremist
  Sites that contain information regarding militias, anti-government groups, terrorism, anarchy, etc.

Does this category include all documents related to the Declaration of Independence made by our Founding Fathers? Does it include sites that have been established by dissidents in Iran and China? On what basis is this company making these decisions?

Lifestyle
Sites that contain material relative to an individual's personal life choices. This includes sexual preference, cultural identity, or organization/club affiliations.

Does “sexual preference” include multiple partner relationships? Does “individual’s personal life choices” and “organizations” include nudist organizations? Will this category block sites such as the Gay Lesbian Straight Educational Network or information and support sites for LGBTQ teens?

- The category definitions and categorization decisions are made without reference to any local community standards and it is not possible to modify the filtering product to meet local standards.

- The actual URLs or IP addresses of the Web sites or pages contained in the category lists are considered to be proprietary information and are unavailable for review by school officials or the general public.

- Compiling and categorizing URLs to form the category lists is a complex process that is impossible to conduct with any high degree of accuracy. The specific methods that filtering companies use to compile and categorize lists are, like the lists themselves, proprietary information.

- The private filtering companies are not subject to any laws to ensure public accountability including factors which raise concerns about the potential for biased-based blocking.

  For example, it appears that the popular 8e6 Technologies company, now called M86 Technologies as the result of a merger [http://www.m86security.com/i/Marshal8e6-Becomes-M86-Security,news.1059~.asp], whose filter is used in many public schools and libraries, has a close corporate connection with the American Family Association, a highly conservative religious organization. Here is the evidence trail:

  Go to: http://www.afa.net and scan down the left hand side to AFA Filter. This goes to http://bsafeonline.com. Note here: http://www.charismamag.com/articles/index.php?id=4674 “Florida officials announced last week that state and local funds will be given to Bsafe Online.com, a subsidiary of American Family Association.” BSafeOnline is operated by a company called BSecure Technologies. Now go here: http://www.8e6.com/internet-filtering/sl_soho.htm. Scan down and click the “ Click here to learn more or to purchase the 8e6Home product.” This goes to http://bsafehome.com/?72141. Note the press release on the bsafeonline site: http://secure2.bsafeonline.com/News/8e6Home.aspx “Florida-based Bsecure Technologies and California-based 8e6 Technologies today announce the beginning of a powerful collaboration aimed at expanding upon the companies’ best-of-breed technologies by providing the first, truly integrated client/server Internet Security solution.” Also here: http://www.8e6.com/partners/technology-partners/bsafe-online-inc.html. “A vertical service provider (VSP), Bsafe Online distributes and supports new and growing lines of Internet filtering and security applications. Using the 8e6 Database, Bsafe currently markets a client software version entitled 8e6Home.”

While it may be the desire of the FCC to approve language that would create the illusion that local school boards have control of the the determination of what material is considered “harmful to minors,” clearly local control is not the reality. The reality is that the U.S. Government has required schools to turn over authority for these decisions to private companies with absolutely no public accountability. It would be disingenuous for the FCC regulations to suggest otherwise.

Given the current state of affairs, it would be helpful if the FCC would set forth language that recognizes the reality that the only control that school officials have is the selection of categories - under conditions which do not allow the local officials to accurately determine what is being blocked. Given the limitations of filtering technology, districts may decide not to block some categories that possibly could have sites adult content when the selection of that category would result in blocking sites that provide high quality instructional or professional development resources.

It should be presumed that other actions the districts could take, including technologies that can allow for “white-listing” of appropriate sites for elementary students, setting search engines to filter search results and more extensive reliance on monitoring , including the use of monitoring technologies, are vehicles that would hold the potential of being more effective in preventing inappropriate access of objectionable material.

It would be helpful for the FCC to state that the FCC will assume that local authorities will select the filtering categories that best match the kinds of material sought to be blocked under CIPA - the categories that specifically describe pornographic materials or other materials designated as “for adults only” - and that the U.S. Government will not establish criteria or review decisions made by local officials on any blocking decisions.

Further, that given the challenges in making such selection and the ineffectiveness of filtering in general, it would be helpful if the FCC would indicate that it would only entertain a review of district compliance of CIPA in cases where there is evidence of a flagrant disregard for the requirements of the law - the intentional failure to block categories that clearly describe the presence of pornographic and adult-only material. This would help to remove the “fear of loss of E-Rate funds for violation of CIPA” mind-set that is currently causing districts to block every category where there might possibly be materials that fall under CIPA prohibitions, the selection of which is significantly impeding the use of the Internet for high quality instructional purposes.

Web 2.0 User Content Sites

The rapid embrace by society of what are sometimes called Web 2.0 technologies, essentially interactive technologies that allow users to easily upload and display self-generated content, has also caused significant problems in schools. On sites where it is possible to upload such content range in the kinds of material that is allowed to be posted. The guidelines for the kinds of materials that can be posted on such sites varies:

- The relevant language from YouTube Community Guidelines <http://www.youtube.com/t/community_guidelines.> : “YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation.”

- The guidelines for a popular blogging site, Blogger <http://www.blogger.com/content.g> are more expansive: “Adult Content: We do allow adult content on Blogger, including images or videos that contain nudity or sexual activity. But, please mark your blog as 'adult' in your Blogger settings.

Otherwise, we may put it behind a 'mature content' interstitial. (Blogger is a site owned by Google. The same guidelines are present for Google Groups.)"

- The Terms of Use for another popular blog site WordPress are more restrictive <http://en.wordpress.com/tos/>: "By making Content available, you represent and warrant that: ...the Content is not pornographic,..."

- An example of the terms of use of the Ning site, which allows users to establish their own social networking is <http://help.ning.com/cgi-bin/ning.cfg/php/enduser/std_adp.php?p_faqid=3450>: "We believe in freedom of expression and Ning, as a broad-based service, is designed to respect many different perspectives and enable them to co-exist seamlessly and effortlessly. That said, Ning does not support social networks of an adult nature, subject or theme. As it relates to the Ning Platform, adult social networks include, but aren't limited to pornography and depictions of sexual acts. ...

Many teachers are now participating fully in the blogging community as a vehicle for ongoing professional development. The Online Education Database indicated that there are over 30,000 educator blogs hosted at Edublogs.org alone. Their list of the top 100 blogs is here: <http://oedb.org/library/features/top-100-education-blogs> An example of a high quality social network for teachers is Classroom 2.0 <http://www.classroom20.com/> a social network for those interested in Web 2.0 and collaborative technologies in education, which has been established on Ning.

In many, if not most, districts, sites with valuable instructional resources are likely blocked in the "blog" or "social networking" categories. Thus, because of the fear of being found to be in violation of CIPA, educators throughout the country are prevented from accessing valuable instructional and professional development resources. What districts do not realize is that blogs that are set up with "adult content" would be blocked not only in the "blog" category, but also in the "adult content" or "pornography," thus it is not necessary to block "blogs" or "social networking" to be in compliance with CIPA.

The recommendations set forth in the prior section will also help to address this concern.

Bypass Technologies

It would be advisable for FCC staff to conduct a simple search on the following search terms: "bypass Internet filter." A search conducted on 11/25/09 returned 4,280,000 links, including some helpful YouTube videos that provide instructions. Some highlights from the initial returns: "Today more and more employers and schools block websites like myspace.com. You can learn how to get around the filter from this article." "How to bypass the internet filter in your office, university, school, library, and cyber cafe? How to be invisible while surfing the net ..." "Easily Bypass Internet Filter At Work Or School: If some websites get blocked in your company or school, how to access those websites at work or school?"

An interesting editorial discussing bypass technologies appeared on 11/20/09 in the *Washington Post*. "Twitter this: The means exist to rupture Internet censorship in China and Iran -- if the State Department will cooperate." <http://www.washingtonpost.com/wp-dyn/content/article/2009/11/20/AR2009112004152.html> This editorial addresses the desire of members of Congress that the State Department provide more funding for organizations that develop and provide bypass technologies. Based on the insight presented, it is unclear the degree to which the US Government is currently funding such bypassing initiatives.

However, in a column written by Sen. Specter, 7/7/09, entitled "Attack the Cyberwalls!: The Internet is the Pathway to Democracy in Places Like Iran." <http://www.huffingtonpost.com/sen-arlen-specter/

attack-the-cyberwalls-the_b_227114.html> clearly calls for federal funding for the expansion of development of such technologies.

The situation that exists in most high schools and many middle schools today is that the adult staff are blocked by the filters, but the majority of the students can easily bypass the filter to get where they want online. Unfortunately when students are engaged in such misuse, it is less likely that they want to access relevant instructional material. They more likely want to access sites that allow them to socialize and because of the false security in schools that filters are effective technologies to manage student Internet use, much of this misuse goes undetected.

Thus while school districts are spending millions of dollars for technology protection measures to be in compliance with CIPA, it is presumed that the effectiveness of such technologies will be even further undermined, by increased federal funding to support bypass technologies.

There is not much the FCC can do about this situation other than to discontinue making any false representations that the technology protection measures required under CIPA are at all effective in preventing access to objectionable material.

Disabling and Overriding

Lastly, we come to the topic that provides a solution to the the concerns that have been presented. It is necessary that the FCC understand that there is some confusion about the concept of disabling and overriding. The key question must be: disabling or overriding to access what? Note the following language:

> (c)(1)(i). The Internet safety policy adopted and enforced pursuant to 47 U.S.C. 254(h) must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors. The technology protection measure must be enforced during use of computers with Internet access, although an administrator, supervisor, or other person authorized by the certifying authority under subparagraph (c)(1) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

To interpret this language, recognize that in schools, the technology protection measure is only required to be configured to block access to visual depictions that are obscene, child pornography, or harmful to minors - nothing more. Under the terms of the statute, the technology protection measure may be disabled during use by an adult to provide access to visual depictions that are obscene, child pornography, or harmful to minors, for bona fide research or other lawful purpose.

According to the Supreme Court, which assessed the situation only in libraries, a library can either disable the filter when requested to do so by an adult - or unblock a site in response to a patron request to access an inappropriately blocked site. Justice Rehnquist stated:

> Like the District Court, the dissents fault the tendency of filtering software to "overblock"--that is, to erroneously block access to constitutionally protected speech that falls outside the categories that software users intend to block. See post, at 1-3 (opinion of Stevens, J.); post, at 3-4 (opinion of Souter, J.). Due to the software's limitations, "[m]any erroneously blocked [Web] pages contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions, such as 'pornography' or 'sex.' "

> 201 F. Supp. 2d, at 449. Assuming that such erroneous blocking presents constitutional difficulties, any such concerns are dispelled by the ease with which patrons may have the filtering software disabled. When a patron encounters a blocked site, he need only ask a librarian to unblock it or (at least in the case of adults) disable the filter. As the District Court found, libraries have the capacity to permanently unblock any erroneously blocked site, id., at 429, and the Solicitor General stated at oral argument that a "library may ... eliminate the filtering with respect to specific sites ... at the request of a patron." Tr. of Oral Arg. 4. With respect to adults, CIPA also expressly authorizes library officials to "disable" a filter altogether "to enable access for bona fide research or other lawful purposes." 20 U. S. C. §9134(f)(3) (disabling permitted for both adults and minors); 47 U. S. C. §254(h)(6)(D) (disabling permitted for adults). The Solicitor General confirmed that a "librarian can, in response to a request from a patron, unblock the filtering mechanism altogether," Tr. of Oral Arg. 11, and further explained that a patron would not "have to explain ... why he was asking a site to be unblocked or the filtering to be disabled," id., at 4.

Note the distinctions. Any patron may request that a site be unblocked if the site has been erroneously blocked. An adult patron may request that the filter be disabled entirely. “Erroneous blocking” refers to blocking of material that is not required to be blocked under CIPA.

It would be very helpful if the FCC would address what is a very significant concern of many districts that is leading to ineffective processes to accomplish an override. Unfortunately in seeking to be in compliance with CIPA and to use the filter for management purposes (a job for which it is ill- suited), large amounts of appropriate material is also being blocked. This is significantly interfering with the use of the Internet for effective instructional purposes.

To ensure effective instructional use, districts must have a process by which teachers and students can easily and rapidly have the filter overridden to allow access to appropriate material. In an overwhelming number of districts, the process to accomplish such an override is overburdensome and cumbersome. Frequently, arguments against providing broad authority to override the filter are grounded in the concern that if a teacher made a mistake, a complaint for violation of CIPA could be filed with the FCC against the district and the district could lose E-Rate funds.

It would be exceptionally helpful if the FCC could note that given the strict boundaries of CIPA with respect to the kinds of material that must be blocked, any issues or questions related to overriding to provide access to material in categories other than “pornography” and “adult context” are entirely outside of the consideration of the FCC. A statement to this effect would be very helpful for those of us who are seeking to address the major challenges in schools that are grounded in a misunderstanding of the CIPA requirements.