Legal Issues Concerning Children

The Internet is constantly changing and evolving. The vast amount of information available to teachers and students has schools looking toward the Internet and away from the traditional textbook. The textbook is generally a resource that is chosen by educators and is limited in the information it provides. The Internet is a doorway to the rest of the world and every person that lives within it. The school is a home away from home for our children and they are given over to teachers and administrators to guide, teach, and protect while they are in our schools. When the doorway to the schools are thrown wide open, the students need to be protected and it is the job of the teachers and administrators to stand guard at the door to make sure that only those with useful information are allowed in. (Filtering Software: The Educators Speak Out)

Most school districts are governed by federal laws that guide Internet use. In order to receive federal funds, the school districts must have several policy pieces in place. In the early days of the E-rate program a district technology plan was required in order to receive those funds. The technology plan included specifics on the planned usage of technology and how the district would protect students from material on the Internet. The technology plan has fallen away in importance as technology has evolved, and as the E-rate program has changed focus. At this time, it is in limbo as to what its future will be but has not been completely removed as a requirement. (Is the Five Year Technology Plan Dead?)

Policies that are still required in school districts include the Internet Safety Policy and the Acceptable Use Policy. The Acceptable Use Policy is adopted by the local schools' governing body that incorporates the rules students must abide by in order to access the technology in their schools. The Acceptable Use Policy is something that is used in businesses as well. The purpose takes on a different meaning in schools. Most Acceptable Use Policies in the business world are simply fair use policies that govern the use of a network, website, or technology service. In a school, the Acceptable Use Policy also adds language meant to protect students from dangers that exist on the Internet, Web, and communication via electronic mail. Most schools have adopted "Acceptable Use Policies"(AUPs) defining student and employee use of the Internet. Such policies are intended to define Internet services, guide educational activities, inform parents/guardians about Internet access, and direct supervision of a school's Internet access. (Green, B. 2014)

Internet Safety Policies

The laws that were updated in 2011 to include more specific language which led to school districts adopting updated Internet Safety Policies into their Acceptable Use Policy. The FCC change Order 11-125 specifically addressed the monitoring of student activity and the education of students concerning online interactions, social media, and cyber bullying awareness. The Internet Safety Policy contains the same information that was previously contained in the schools Acceptable Use Policy but many schools were not actively educating children about Internet safety in the classroom. The updates in 2011 specifically require that Internet safety be included in the curriculum. (Children's Internet Protection Act, 2011)

Children's Internet Protection Act

CIPA is the acronym for the Children's Internet Protection Act, enacted by Congress in 2000 along with NCIPA (Neighborhood Children's Internet Protection Act) and went into effect on April 20, 2001. CIPA governs filtering and Internet safety in schools and NCIPA governs its use in public libraries. The two acts require Internet safety policies and filtering technology for schools and libraries to receive funds from the Universal Service Fund. USF provides telecommunications discounts for schools and libraries depending upon the poverty level in their area and the rurality. CIPA and NCIPA compliance is not required for those schools and libraries that choose to not receive reimbursements from the USF.

Schools and libraries receiving funds from the USF must specifically incorporate protection measures to block or filter Internet access to any content that is (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). (Children's Internet Protection Act, 2011) Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal. (National Education Technology Plan - Office of Educational Technology.)

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy that addresses five different points. First is the issue of minors accessing inappropriate content. Most schools address this by utilizing a filter to block the content. The second issue is keeping minors safe while utilizing different direct communication tools. This can be addressed by a web filter, but generally the system must be expanded to filter e-mail, as well, and to capture and log certain keywords. The third becomes even more difficult since it requires schools to police any unlawful activities by minors on the Internet. A filter can catch some of these things, but generally this must be addressed in a policy, and hooked to a discipline measure. Once students have broken the law, they are much more difficult to catch because they are hiding all of their actions. Schools are also required to keep student information from being disclosed. This is probably the Achilles' heel of most schools. Everyone seems to need access to the student data, and the database has so much information that it is difficult to lock down exactly who needs what information. Schools should always err on the side of caution and not give permission. If the user needs permission to student data, they will request access and it can be determined, at that point, if access is truly warranted.

The final piece is the most subjective. The school should restrict access to any material that would be considered harmful to minors. This is usually a decision made within the community, and the community should be the last word, but unfortunately it is not. Outside forces will invade a school district to make an example of it. This could be organizations with a specific agenda, or federal agencies that have been called in by those with a specific agenda to stop the district from whatever horrible offense they have wrought against the children. This interference makes it difficult to make a policy decision on what is harmful, and stand behind it. The potential threat from the federal government or outside organizations generally causes a weak and watered down policy on what is harmful to minors, and that is usually limited to violence and pornography.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding. CIPA would not apply to entities applying only for telecommunication services. If a person needs to do legitimate research, or access sites that are normally blocked, an authorized

person may disable the filtering to allow for research or other lawful usage. CIPA does require monitoring, but not the tracking of Internet usage for minors or adults. The difference is that monitoring is in the here and now, while tracking is keeping a history on the individual of all their steps, or in this case, the different sites they have accessed over a period of time. (Willard, N. 1998).

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. (Libraries and the Internet Toolkit)

Internet Filtering

One of the major issues that school districts have brought forward concerning CIPA is that the USF will not pay for internet filtering. It seems counter-productive to require a poor school to filter its Internet service in order to receive discounts on the circuit itself but not give a discount on any kind of filtering service as a separate service or even as a bundle service provided by the internet service provider. It is logical to conclude that the subsequent filtering and other requirements set forth by CIPA will be less robust and lacking in quality because the poorer school districts must tap their local budgets in order to afford the filtering and the materials to include Internet safety in their curriculum. It seems to be another case of the federal government mandating certain requirements of the state and local government while not providing needed funds in order to fulfill those requirements. The filtering options for small school districts are generally weak and just simply not as robust as the paid versions. A firewall to protect from hackers and good quality filtering is a must for any school district since one mistake can lead to a hugely expensive lawsuit.

The federal government has not been proactive in protecting children from the dangers that exist online. It seems more intent upon stopping file sharing and pirating for the big Hollywood movie companies instead of efforts to keep children from having easy access to pornography. In the early years of CIPA, I e-mailed my legislators with a proposal to create an .xxx domain and require all sites that contain pornography to utilize that domain. School districts would be able to implement a simple DNS block of all domains ending in .xxx and allow them to focus on other efforts such as combating hate speech, bullying, and stopping pedophiles. Years later, laws were passed that allowed producers of pornography to “voluntarily” register and utilize an .xxx domain. I feel that our children are being sold simply because the filtering business is such as huge part of the economy now. Simply requiring those domains that have nudity to register as an .xxx domain would save the taxpayers millions of dollars per year. The filtering companies would still be in business since corporations would still want to filter eBay, Facebook and shopping sites.

It certainly doesn’t help things when corporations such as Google make it more difficult to filter the information on the Internet. It’s understandable that they would like to switch all of their sites from the http protocol to https. Https is a secure protocol that encrypts the traffic between the host and client computers, but it breaks most filters to the point that a school district must take

more extreme measures to be able to continue to monitor their students, per CIPA. The recent move of Youtube and other popular Google sites to https caused many school districts to scramble to get a solution in place. The cost to schools has been a huge source of consternation for IT departments, as they have had to change while Google tried out Youtube.edu, Google for Schools, and other failed solutions. In the end many schools spent a lot of money upgrading their filtering in order to stay compliant and still allow teachers to access the millions of instructional videos on Youtube.

Those who feel that the Internet should be free of any censorship purposefully make it difficult for schools and libraries to do the job that they have been given by both the federal government and their local community. Many corporations have large numbers of people working for them that do not believe in any type of censorship. There are those trying to circumvent filtering on behalf of our children for their beliefs, and there are those that are doing it for the almighty dollar. It's in the best interest of pornographers and pedophiles to bypass filtering in order to get children hooked on their material at an early age. Those companies and individuals that are "Paid per click" are also eager to bypass filtering to get our children off of their schoolwork, and onto a website where ads and games pay the owner depending upon how much time the children spend on their sites viewing ads. Parents should never make the assumption that anyone on the Internet views their child the way they do. Many of the people on the other side of the keyboard view children as something to be used, either to make a dollar or for some even more sinister purpose. An unfiltered computer sitting somewhere that the mother and father cannot help monitor is an invitation for the worst people on the Internet to come right into your home. (The Internet Censorship Controversy.)

Freedom of Speech

Districts must carefully balance a student's right to free speech and the protection of children from objectionable material. School districts have the responsibility of protecting a large amount of data. Schools must be cognizant of the potential loss of data due to security breaches from the outside as well as from the inside. Students can be a potential security risk if they are able to access sensitive data and post it to the Internet. Student information should be protected from access from other students. Schools should constantly train on "netiquette" for not only their teachers, but their regular staff. In his book "Guidebook for developing an effecting Instructional Technology Plan" Dr. Larry Anderson advocates for the training of those who secure software and equipment as well. (Anderson, 1996)

FERPA

In much the same way that HIPAA governs patient data when it comes to the healthcare field, FERPA governs access to student data and records. Most Acceptable Use Policies do not specifically address FERPA, but more are addressing it now that school districts realize the potential issues that surround student data being shared with other organizations, such as software companies, over the internet. FERPA stands for Family Educational Rights and Privacy Act. The biggest security risk in schools at this time is the loss of student data. The credit report for a student is pristine, and a whole database of student social security numbers would be a windfall of money for any hacker on the Internet. There have been several cases in Mississippi where employee information was lost, but none that involved student data, yet.

Litigation

The dangers to schools exist on both sides. In *Hunter v. City of Salem* the local library has been sued for allegedly blocking sites that should be protected as free speech. In another case, *PFLAG, Inc. v. Camdenton R-III School District,* the school district is being sued for blocking websites that dealt with "sexuality", claiming that the filter blocked access to sites that were positive toward LGBT issues, while allowing through websites that contained negative speech towards the LGBT community. The district subsequently was found guilty of violating the students first amendment rights. At any moment a school district could be sued by a student for anything that may seem like a double standard. The pendulum could easily swing the other way if a Christian student finds all religious sites blocked, while sites about atheism are completely unfiltered. (How to Sue a School District)

Community Involvement

The issue becomes the fact that local communities are not allowed to police according to their standards. The standards set forth by the federal government on what is deemed to be obscene or harmful to children may not coincide with the values of the local community. The local community and schools have lost all rights to police behavior based upon the local community's morals and values. Many times, outsiders that are willing to participate in a lawsuit are moved in to an area to challenge the local authorities. Activism on the part of special interest groups, whether they are to the right or the left of the political spectrum, should not be allowed to act out their cause in the courts by dragging school districts into positions that waste tax dollars that should be utilized for the benefit of the children. (Na, E., & Kim, E., 2014)

School Focus

School districts should be concerned about the education of their students. The decisions made on behalf of their students are, and should be, made by a duly elected board made up of local citizens from their community. No student should be able to sue a school district based on decisions made by the local community. The schools are an extension of the local community and as such should be free from any threat of litigation so that they can focus all of their energies and assets toward the education of children. The federal government should not be allowed to place stipulations on the people's tax dollars before they will allow them to be sent back to the communities. The money sent from the federal government should be focused and address a need in a community and there should be no strings attached that would deny the local community the right to raise their children in the way they that see fit.

There was a time when the only focus a school district had was educating the children of the community. The rules of the community were the law within the schoolhouse, and the parents and teachers were the last word on any issue. In the past, and still in the present in a select few school districts, if the school needed a fence repaired, or rooms repainted, or some money to buy instruments, uniforms, or even to buy some sports equipment the parents were there at the school the minute they learned there was a need. In my own hometown of Clinton, MS, it was hard to

get past the PTA mothers outside the TG&Y and Treasury Drug selling cakes and cookies, and all assortment of deadly pastries to earn money for whatever the school might need. If a fence needed repairing, the local hardware store donated materials, and every able bodied man and boy was made to show up for work, probably by the mother of the house, and they were right there handing out drinks and directing the work in their own way. Currently we have a society that is spoiled rotten. If they don't get their way, or if their child is not treated as they see fit the potential is there for the school to be dragged into the court system.

The current set of solutions involve more money, staff, and time invested by the schools in order to protect the students and themselves. The issue becomes the fact that this money is taxpayer dollars that are having to be diverted away from education. The ultimate solution is for schools to become what they once were, cherished and protected institutions that were seen as being one step away from a sacred building, or hallowed house of worship. The people that worked within it were worthy of respect, and were an integral part of the community and enjoyed an almost "celebrity" status within the community. A return to those values would mitigate the need for more lawyers, more spending, and ultimately more separation from the community.

References

Anderson, L. (1996). Guidebook for developing an effective instructional technology plan. Mississippi: Mississippi State University.

Children's Internet Protection Act. (2011). Retrieved June 04, 2016, from https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Filtering Software: The Educators Speak Out. (n.d.). Retrieved June 02, 2016, from http://www.educationworld.com/a_tech/tech155.shtml

Greene, B. (2014). The School Administrator's Responsibility for Implementing the Safe and Appropriate Use of Technology in Our Schools. Amazon Digital Services LLC.

How to Sue a School District. (n.d.). Retrieved June 02, 2016, from http://www.legalmatch.com/law-library/article/how-to-sue-a-school-district.html

The Internet Censorship Controversy. (n.d.). Retrieved June 02, 2016, from http://courses.cs.vt.edu/professionalism/Censorship/notes.html

Is the Five Year Technology Plan Dead? (2015). Retrieved June 02, 2016, from http://telecomreseller.com/2015/02/09/is-the-five-year-technology-plan-dead/

Libraries and the Internet Toolkit. (n.d.). Retrieved June 02, 2016, from http://www.ala.org/advocacy/intfreedom/iftoolkits/litoolkit/legalissues_CIPA_filtering

National Education Technology Plan - Office of Educational Technology. (n.d.). Retrieved June 04, 2016, from http://tech.ed.gov/netp/

Park, S., Na, E., & Kim, E. (2014). The relationship between online activities, netiquette and cyberbullying. *Children and Youth Services Review*, *42*, 74-81. doi:10.1016/j.childyouth.2014.04.002

Willard, N. (1998). A legal and educational analysis of K-12 internet acceptable use policies. Eugene, OR: Oregon School Study Council.