2013

An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K-12 Public Schools

Mary E. Vicks
Nova Southeastern University, tyler@nova.edu

An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K-12 Public Schools

by

Mary E. Vicks

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Computing Technology in Education

Graduate School of Computer and Information Sciences
Nova Southeastern University

2013

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K-12 Public Schools

by

Mary E Vicks

April, 2013

School districts have implemented filtering and safety policies in response to legislative and social mandates to protect students from the proliferation of objectionable online content. Subject related literature suggests these policies are more restrictive than legal mandates require and are adversely affecting information access and instruction. There is limited understanding of how filtering and safety policies are affecting teaching and learning because no comprehensive studies have investigated the issues and trends surrounding filtering and safety policy implementation. In order to improve existing safety policies, policymakers need research-based data identifying end user access issues that limit technology integration in the kindergarten-12th grade (K-12) educational setting.

This study sought to examine Internet filtering and safety policy implementation issues in South Carolina's K-12 public schools to determine their influence on information access and instruction. A mixed methods research design, which includes both quantitative and qualitative approaches, was used to investigate the research problem. Quantitative data were collected from information technology (IT) administrators who were surveyed regarding filtering and safety policy implementation, and school library media specialists (SLMS) were surveyed concerning the issues they encounter while facilitating information access in a filtered environment. Qualitative data were collected through interviews with a subset of the SLMS population, thereby providing further insight about Internet access issues and their influence on teaching and learning. School districts' Acceptable Use Policies (AUPs) were analyzed to determine how they addressed recent legislative mandates to educate minors about specific Web 2.0 safety issues.

The research results support the conclusions of previous anecdotal studies which show that K-12 Internet access policies are overly restrictive, resulting in inhibited access to online educational resources. The major implication of this study is that existing Internet access policies need to be fine-tuned in order to permit greater access to educational content. The study recommends Internet safety practices that will empower teachers and students to access the Internet's vast educational resources safely and securely while realizing the Internet's potential to enrich teaching and learning.

Acknowledgements

I would like to thank God for His ever abiding presence and guidance as I undertook this difficult, but incredible journey. I am so grateful to my husband, Benjamin, for his quiet support and for always asking, “How are you progressing on your research?” Whenever I hit a roadblock and took a brief hiatus, hearing that question repeatedly motivated me to get back to work. I dedicate this dissertation to my late parents, Reverend William Tyler Jr. and Charlese Tyler, who passed away before I could complete my research. Their unshakeable faith in God inspired me to persevere until I reached my goal.

Next, I would like to thank my advisor, Dr. Zink for his exceptional patience, guidance and support as I worked through numerous iterations of my idea paper, proposal and final report. Your faith in my ability to complete this dissertation was a tremendous inspiration. Also, thank you Dr. Abramson and Dr. Littman, for your valuable input and your attention to detail. I am truly grateful for having such a wonderful dissertation committee.

I owe a debt of gratitude to my expert panelists, Dr. Lynn Sutton, Mr. Doug Johnson, Mr. Scott Floyd, Dr. Melissa Johnson, and Ms. Helen Adams for evaluating my research instruments. I am deeply grateful to the school districts that allowed me to investigate their filtering and safety policies. Finally, I extend heartfelt thanks to the IT administrators and school library media specialists who provided the data I needed to answer the research questions.

I could not have done it without all of you!

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

When the World Wide Web and graphical browsers popularized the Internet and made it easier to use, technology enthusiasts predicted the Internet would revolutionize every aspect of society—particularly education. Many educators envisioned a world in which Web-based technology would be the catalyst for educational reform. Students would no longer be passive recipients of knowledge because the Internet would empower them to become active participants in their own education. Students would collaborate with peers in distant lands and subject experts to solve problems. Internet-based education would tear down classroom barriers and the classroom would become the world. This was the promise of the Internet, but it has fallen short of such lofty educational potential (Hope, 2012). Nevertheless, outside of the school walls, the Internet has revolutionized daily life and work, and is at the core of nearly every aspect of society. Gossett and Shorter (2011) state the Internet is a transformative technology that has revolutionized the manner in which users around the world disseminate information.

The Internet has not had the same transformative effect on teaching and learning. An ever-widening inconsistency exists between technology utilization in schools and its utilization in the larger society. Collins and Halverson (2009) purport that outside of

school, technology is highly influential in areas that are the major focus of schools—reading, writing, calculating, and thinking—yet, it is marginalized in schools, fully integrated mostly in specialized courses. The growing disparity between students' technology experiences in and out of school is noted in the National Educational Technology Plan (NETP), released by the U.S. Department of Education in March 2010. The report states, "students use computers, mobile devices, and the Internet to create their own engaging learning experiences outside school and after school hours—experiences that too often are radically different from what they are exposed to in school" (p. 4). The NETP concludes that if students are going to be prepared adequately to live and work in the 21st century, they must have authentic learning experiences using Web tools such as wikis, blogs, and digital content in the same way they are used in the real world—for research, collaboration, and communication.

Researchers have suggested that public school Internet use policies are not aligned with the realities of the 21st century, thus contributing to a culture where Internet technology is fully integrated in students' out-of-school experiences, but marginalized within the school walls (Cramer & Hayes, 2010; Hope, 2012; Lemke, Coughlin, Garcia, Reifsneider, & Baas, 2009). Lemke et al. state school Internet policies still restrict students' use of new technologies such as social networking sites, chat rooms, blogs, wikis, visual media, instant messaging and texting, virtual worlds, and interactive games. The NETP concludes that electronic filtering required by the Children's Internet Protection Act (CIPA) sometimes creates barriers to engaging learning experiences that in-school Internet access should provide students. Increasingly, technology integration experts are advising school boards, administrators, and teachers to re-examine their

technology policies to accommodate the rapidly changing technology landscape and support the incorporation of new Web-based and mobile technologies (Consortium for School Networking (CoSN), 2011). Policymakers must adapt Internet safety and filtering policies so they balance the need for student safety and security with the educational benefits of the Internet. Without Internet policy changes, schools cannot successfully integrate new technologies and the vast educational promises of the Internet will continue to be unrealized for students who do not have access to the Internet outside of school.

Problem Statement

Public schools have instituted Internet filtering and safety policies in response to federal or state legislation, and public pressure to protect students from inappropriate Internet content. Some literature reports that administrators are filtering beyond federal and state mandates (Johnson, 2012; Fuchs, 2012) in order to combat increasing security threats, degraded network performance, and distractions caused by non-educational Internet content (Hua, 2011). Excessively restrictive Internet filtering policies limit access to constitutionally protected information, often involve time-consuming and bureaucratic procedures for unblocking acceptable Web sites, frustrate users, and could potentially make schools vulnerable to First Amendment litigation (Willard, 2010b; Maycock, 2011).

Moreover, proponents for less stringent filtering policies argue that overly restrictive filtering policies prevent use of Web 2.0 applications such as wikis, blogs, and online productivity tools, which are critical to the achievement of information literacy and technology learning standards (Losh & Jenkins, 2012). Twenty-first century teaching and learning necessitates access to technology resources that enable educators and

students to collaborate, create, and share content online (Bosco & Krueger, 2011). Ultimately, blocking of such tools inhibits public schools from accomplishing their educational mission of preparing students to live and work in an increasingly global and digital age.

Recently, anecdotal research has highlighted specific instances of how filtering policies are influencing teaching and learning. In some Los Angeles schools, Losh and Jenkins (2012) report teachers have been granted override privileges to access blocked YouTube™ videos, but the override worked for only 20 minutes. Consequently, teachers were unable to set up YouTube™ videos prior to class, but had to interrupt instruction to input override codes. Losh and Jenkins report this practice "discouraged the instructional use of Web-based materials" (p.18). Moreover, in some Indiana schools, the filtering software blocked access to several important Herman Melville sites because his most famous novel includes "dick" in the title. Other school districts blocked access to participatory platforms such as Twitter™, LiveJournal™, and even materials created for social media platforms by the White House and other government entities. Willard (2010b) also discovered from email discussion group comments that one of the biggest filtering policy issues was blocking of forums. A California discussion group participant reported that any site with a comment area was blocked, including all blogs, and most Web 2.0 sites.

The aforementioned scenarios detail how filtering and safety policies negatively affect teaching and learning. However, not all educators have had negative experiences with filters. Some school districts have found ways to balance safety and security concerns with the need to provide access to the engaging educational resources available

on the Internet (Bosco & Krueger, 2011). An examination of Internet filtering and safety policies was needed to determine the prevalence of the aforementioned restrictive access issues. There was also a need to uncover salient information access issues and trends of relevance to policymakers seeking to adapt their filtering and safety policies to the ever-changing technology landscape.

Goal

This dissertation examined Internet filtering and safety policy implementation in South Carolina's K-12 public schools. The major goal of the study was to update and expand upon anecdotal or small-scale studies examining the influence of Internet filtering on instruction and information access in the K-12 sector. Results of this study, coupled with previous studies, can be used to inform filtering policy evaluation in order to maximize access to legitimate educational content while minimizing access to inappropriate content. Furthermore, this study expands the filtering policy research base and validates the issues identified in previous anecdotal and less comprehensive studies.

A limited number of studies have investigated the effect of filtering policies on teaching and learning. This research supplements existing literature by addressing unanswered questions from previous studies. Finsness (2008) found that Internet filtering configurations limited student access to information necessary for achieving Minnesota's U.S. history and health standards. The study also suggested that further research was needed to determine if students had sufficient access to Web resources enabling them to hone necessary 21st century information technology and literacy skills. This research addressed Finsness' conclusion. Holzhauer (2009) found that filters limited classroom Internet use, but concluded that additional research was needed to learn how school

districts decide what to filter (beyond what legal mandates require) and what changes are necessary to improve Internet use policies. This investigation sought answers to Holzhauer's conclusions.

District information technology (IT) administrators were surveyed to ascertain how filtering and safety policies were implemented. Furthermore, school library media specialists (SLMS[1]), who have historically been advocates for greater information access (Losh & Jenkins, 2012; Maycock, 2011), were surveyed and interviewed to determine how filtered Internet access influenced teaching and learning. Data from the interviews and surveys define Internet use policies that negatively affect teaching and learning and practices that mitigate filtering issues. School districts need filtering and safety policy guidelines as they seek to exploit the educational benefits 21st century digital technologies afford. This study provides those guidelines. Combined with previous studies, this study provides stakeholders (administrators, teachers, SLMS, technology coordinators, and parents) with the data and information necessary to guide filtering and safety policy decisions.

Research Questions

This research investigated the following research questions:

- How are filtering and safety policies being implemented in public schools?
- What issues do SLMS encounter as they facilitate information access on filtered computers?
- How are school districts addressing Web 2.0 safety issues?

[1] SLMS acronym is used for school library media specialist or school library media specialists.

- In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?

Relevance and Significance

Internet-based educational resources have become almost as ubiquitous in today's public schools as the traditional textbook. With the advent of the World Wide Web, educators and government officials enthusiastically embraced the Internet as an important educational tool because of its purported educational benefits (Ott, Beard, Blue, Cleugh, Greenfield, Lee,…Stager, 2010; Fuchs, 2012). Education reformers contend the Internet has not realized its educational potential (Lemke et al., 2009); however, outside of school it has become woven into the fabric of today's society because of its importance in research, communication, and an abundant list of daily activities (Hall, 2011).

As Internet accessibility in public schools has increased, so has concern about preventing students from inadvertently or deliberately accessing inappropriate online content. Despite its educational benefits, the Internet exposes students to an ever-increasing amount of objectionable content. Robinson, Brown, and Green (2010) report that the Web is "riddled with inappropriate and undesirable content" (p. 14) such as dangerous or illegal guides (i.e., bomb-making instructions), pornography, gruesome and violent images, racist/hateful content, and advertising. Efforts to shield minors from exposure to this type of content continue to fuel public debate and present "intriguing policy and practice dilemmas" (Moyle, 2012, p. 403).

In response to rising public concern, Congress enacted legislation on several occasions in an effort to insulate children from exposure to online indecency. The

Communications Decency Act (CDA) (1996) and the Child Online Protection Act (COPA) (1998) were two notable congressional attempts to restrict the distribution of sexually explicit Internet materials to minors. However, free speech advocates challenged the constitutionality of both laws and the Supreme Court agreed, declaring both acts unconstitutional because they violated free speech under the provisions of the First Amendment.

The Children's Internet Protection Act (CIPA) (2000) is Congress' most recent attempt to restrict access to inappropriate online content. CIPA requires schools and public libraries receiving federal funds for Internet access to implement "technology protection measures" to prevent access to "visual depictions that are obscene, child pornography, or harmful to minors" (Section 3601). Reminiscent of its predecessors, free speech proponents promptly challenged the constitutionally of CIPA's filtering mandate. The American Library Association (ALA) filed suit on behalf of public libraries contending that CIPA was unconstitutional and created an infringement of First Amendment protections. In 2002, the United States District Court in Pennsylvania sustained the ALA's claim and overturned the library filtering law, concurring that filtering software blocked access to constitutionally protected Internet expression (*ALA v United States*, 2002). However, in June 2003, the Supreme Court reversed the lower court's decision and endorsed CIPA's constitutionality (*United States v ALA*, 2003).

Even before the Supreme Court upheld CIPA, Internet filtering had become a political necessity in American schools as policymakers sought to provide safer Internet access and avoid potential litigation arising from student exposure to what was deemed harmful online content (Sutton, 2012). Following the Supreme Court's ruling and similar

legislation in many states, filtering became a legal necessity. However, widespread deployment of Intent content controls and legal mandates has not settled the filtering debate. Not only are Web 1.0 access issues fueling the debate, but also Web 2.0 access issues continue to underscore the significance of online safety policy deliberations (Quillen, 2010). Regarding Web filtering policies, Quillen suggests that a "seismic showdown is brewing," (p.20) and "something must change if schools are to continue exploring the use of Web 2.0 tools" (p. 20). Filtering continues to be an important issue for most schools because many schools have implemented aggressive filtering policies that impede student research and inhibit online collaborative activities (American Association of School Librarians (AASL), 2012)

Growing concern about sexual predators preying on minors using social networking sites prompted the U. S. House of Representatives to pass the Deleting Predators Online Act (DOPA) in 2006, which required education rate (E-rate) schools to block access to all social networking sites and chat rooms. Free speech proponents objected to the bill's broad language claiming the law, as written, would have prohibited access to most interactive Web 2.0 sites and services that permit users to create and edit Web content, such as wikis and blogs (Holcomb, Brady, & Smith, 2010; Macleod-Ball, 2011). They also argued that the best approach to online safety was not filtering, but teaching children about safe and appropriate online behavior (Willard, 2010b). After years of deliberation, the Protecting Children in the 21st Century Act (2008), which supplanted DOPA, became law. The act no longer required E-rate schools to restrict access to social networking sites, but mandated that schools educate students "about appropriate online behavior, including interacting with other individuals on social

networking sites and in chat rooms and cyber bullying awareness and response" (Section 215).

The emergence of the read/write Web (Web 2.0) and perceived ineffectiveness of current Internet safety policies continues to fuel deliberations that suggest school districts need to re-examine their filtering and safety policies (Bosco & Krueger, 2011). Some school districts, in an effort to protect children, have blocked Web 2.0 tools—not only social-networking sites, but blogs, wikis, and other online participatory tools that allow teachers and students to create and share content (Losh & Jenkins, 2012; Robinson, Brown & Green, 2010). Adams (2010) suggests that current safety policies rely solely on filters to protect children and fail to emphasize the importance of teaching students how to evaluate information and navigate safely when using unfiltered computers outside of school. Quillen (2010) claims the ability to override the filter rapidly has not been established in many schools and is, therefore, hampering instructional activities. Willard (2010b) concludes that current filtering policies prevent schools from realizing the educational potential of the Internet because of more restrictive filtering policies, increased bureaucracy, and lack of focus on Internet safety education. The widening gap between policymakers and some educators is reflected in the following statement:

> In many schools, any website that has "blog" in the URL or its name is off limits. Photo sharing sites like Flickr don't stand a chance. Even closed networks like a Ning or an invitation-only wiki might be blocked. School administrators may simply not understand what the tools are and how they can be used in school settings. Many rely heavily on the judgment of technology coordinators who have

> (not unjustifiable) concerns about safety and security issues or, in some cases, the loss of control that Web 2.0 tools imply. (Harris, 2009a, p. 58)

However, Manzo (2009) portrays the filtering dilemma from the administrators' perspective in the following statement:

> Faced with concerns about Internet predators, cyber bullying, students' sharing of inappropriate content on social networks, and the abundance of sexually explicit or violent content online, many school leaders and technology directors are placing tighter restrictions on Web access to shield students from potential harm. (p. 23)

IT administrators' primary mission is establishing the most efficient network infrastructure, eliminating security threats (Web viruses, spyware, hacking tools, malicious content, worms), and conserving network bandwidth. Consequently, filtering software is often configured to minimize security threats and to conserve bandwidth in addition to CIPA's requirement to block access to pictures that are obscene, child pornography, or are harmful to minors (Baule, 2010; Hua, 2011). Restrictive filter configurations that block entire content categories (i.e., weapons) may lessen security threats but prevent access to nonthreatening, constitutionally protected information about weapons used during ancient times (Quillen; Hua). Moreover, improperly deployed or erroneously configured filtering systems can have a downside and unintended consequences (Fuchs, 2012; Nicoletti, 2009). An in-depth investigation of filtering policies would elucidate the consequences of filtering policy decisions for end users and provide a deeper understanding of factors contributing to administrators' safety policy decisions.

Research evidence is a key ingredient to improved policy and practice (Tseng, 2012). Research-based evidence is deficient regarding the use and impact of filtering technology in public schools given that there is little research-based evidence to guide filtering and safety policy decisions. In the past decade, school districts' Internet use policies have been characterized by what Willard (2010a) describes as "technopanic"—an intensified apprehension about minors' Internet use that has not been "grounded in actual research" (p. 10). It is important to assess how filtering and safety policy decisions are affecting end users in order to improve existing policies. SLMS have a unique vantage point from which to provide a deeper understanding of the issues and trends surrounding filtering technology implementation and its impact on end users because they support both teachers and students in their quest for information. Consequently, this investigation of media specialists' experiences with filtered Internet access identified filtering and safety policy-related problems and challenges, and provides essential information for improved filtering policy decisions. Inclusion of IT administrators in this investigation provided information about the technical considerations of filtering policy implementation, which can substantially influence information access.

Barriers and Issues

Barriers, bias, and contentious issues presented challenges to accomplishing the research goal. Since the Supreme Court upheld CIPA in 2003, many educators, including SLMS, have accepted filters as a fact of life in American schools and have concluded that the debate is over (Adams, 2010; Fuchs, 2012). Educators' acceptance of filters and their inherent flaws has contributed to the misconception that further deliberations or research on the topic will have little or no influence on filtering policy implementation. Therefore,

reluctance to participate in a research study about policy issues believed to be beyond participants' influence was an issue. This barrier, combined with survey fatigue, may have adversely affected the survey response rate.

Booth (2011) suggests the library profession lacks a research culture and often fails to see the relevance of research to improved practice and policy. This factor has most likely contributed to the lack of scholarly effort undertaken to provide a deeper understanding of the challenges and issues surrounding filtered Internet access as perceived by SLMS. The researcher was cognizant that this barrier could adversely affect participation in the study. The researcher addressed this issue by emphasizing to potential respondents how this research could be used to affect change in filtering and safety policy implementation in public K-12 schools.

The ALA's Code of Ethics urges librarians to refrain from advancing private interests over professional concerns, and conflating personal convictions and professional duties (American Library Association, 2013c). ALA members, many are whom are SLMS, may feel a professional obligation to support the organization's vehement stance against all attempts to restrict access to what some consider inappropriate Web-based information. Consequently, the researcher considered this as a significant barrier because of the potential difficulty of distinguishing the study participants' views from the ALA's and its affiliate associations. To overcome this barrier, survey and interview questions were structured so that the researcher could distinguish SLMS' individual convictions from the ALA's convictions.

Limitations and Delimitations

Limitations

The study was not experimental, but was primarily descriptive; therefore, controlling variables that threatened internal validity was not a major issue. The data was examined to discover if relationships existed between filtering and safety policy implementation factors and the issues users encountered as they sought online information in a filtered environment. Being that the research design was non-experimental, safety policy implementation issues are described as they exist naturally and relationships are described without attempting to explain the cause of the relationships.

Another limitation of this study was the sampling technique employed. Not every South Carolina school district granted permission for the study to be conducted. For that reason, it was impossible to draw a random sample of all South Carolina SLMS and IT directors. SLMS and IT directors from 36 school districts were selected using total population sampling in order to gather sufficient data to address the research questions. Because of the sampling technique employed, generalization of the data to the entire population is limited.

Delimitations

The researcher limited the scope of the study to South Carolina's public schools to narrow the research focus and to make the research goal more manageable. South Carolina is traditionally a conservative state in the "Bible Belt." Moreover, the state has enacted legislation requiring all public schools and libraries to adopt policies intended to reduce the ability of users to access Web sites displaying obscene material (National

Conference of State Legislatures, 2013). Unlike CIPA's filtering mandate, South Carolina's filtering mandate must be implemented regardless of whether schools and libraries elect to accept state funding. Since the inception of the Internet filtering controversy, conservatives have typically been proponents of filtered Internet access in public schools and libraries. Consequently, research participants' perceptions may reflect the state's conservative stance regarding Internet blocking, making it difficult to generalize the results of the study beyond South Carolina's public schools.

Definition of Terms

This section provides definitions of key terms used in this investigation.

Acceptable Use Policy (AUP). AUPs include school board adopted rules, regulations, rights, and responsibilities that govern users' computer-related activities (Rodgers, 2012). This document is sometimes referred to as a safety policy.

Children's Internet Protection Act (CIPA). CIPA is a law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA requires schools and libraries receiving certain federal funds to use technology protection measures that prevent access to offensive online content (Robinson, Brown, Green, 2010).

Filtering Policy. Filtering policies are an extension of an organization's Internet safety policy (AUP), and define the content categories that are blocked, user profiles, and their privileges (Hidalgo et al., 2009).

Internet Filter. Internet filters are software tools that limit, block, or restrict access to Internet content (Moyle, 2012).

Safety Policy. A safety policy is a CIPA-required document that addresses a broader range of computer-related issues. A safety policy, sometimes referred to as an AUP, encompasses access to inappropriate materials on the Internet and includes provisions for handling security issues, for protecting children's privacy, and for dealing with children's use of computers for illegal activity (e.g., hacking into another computer system) (Neighbor Children's Internet Protection Act (NCIPA), Section 254, 2000).

Web 2.0. Web 2.0, also called the read/write Web, is a term referring to online technologies that allow users to socialize, collaborate, and share information without requiring programming skills. Web 2.0 tools include social networking sites, blogs, wikis, social bookmarking sites, and virtual worlds (Robinson, Brown, & Green, 2010; Simkins & Shultz, 2010).

Summary

The Internet offers a wealth of educational resources that can potentially reform and enhance teaching and learning. However, educators have encountered various impediments to full realization of the Internet's educational potential, including restricted access to some constitutionally protected Internet resources. Filtering and safety policies and procedures have a substantial influence on information access. This study examined the issues surrounding the development and implementation of filtering and safety policies in order to determine how these issues impede information access, and limit attainment of 21st century learning standards.

Chapter 2

Review of the Literature

Introduction

This study focused on the issues surrounding K-12 Internet filtering and safety policies and how these issues converge to influence information access and instruction. Several overarching themes emerged from the literature review, which provided a conceptual framework for the study. The literature review focuses on the following themes: the promise and perils of Internet access for K-12 education, Internet safety legislation and First Amendment issues, the influence of Internet safety legislation on Internet filtering and safety policies, issues related to Internet filtering technology and how it works, filtering and safety policy implementation issues, Internet safety policy issues and 21st century learning standards, and the implications of filtering and safety policy implementation. The final section focuses on the contributions of the current study to the research in this domain.

The literature, which reflects the complexity and controversial nature of Internet content controls in public schools and libraries, is often more prescriptive and experiential than research-based as noted by Jaeger and Yan (2009). Informational, anecdotal, and experiential pieces have been included in the literature review because they underscore the significance of the Internet filtering debate and pinpoint the need for

more research-based evidence to guide filtering and safety policy decisions. Moreover, pertinent early research and prescriptive literature has been included to frame the background of the current study and to illustrate the manner in which the need for the current study has evolved. Initially, Jaeger and Yan attested to the need for more research focusing on the implications of Internet content controls when noting that CIPA and its requirements have not generated much research into how the legislation affects schools, libraries, and clientele of these institutions. More recently, Ahn, Bivona, & DiScala (2011) suggested there was a need for research to advance understanding of how technology policies influence educator practices. This investigation incorporates the aforementioned identified gaps in the literature.

The Promise and Perils of Internet Access for K-12 Education

In its infancy, the Internet was an important communication tool for scientists and academic researchers, but the emergence of the World Wide Web and graphical browsers made Internet navigation easy for everyone (Hall, 2011; Internet, 2011). These developments were instrumental in the Internet becoming a valuable commercial, communication, entertainment, and educational tool. Public schools eagerly embraced the Internet; its many educational resources holding promise for significant instructional improvement and enhanced student learning. The Internet facilitates access to vast amounts of information, enhances communication, and broadens students' connections to diverse people and perspectives. Supporting this conclusion, the National Educational Technology Plan (NETP) (U.S. Department of Education, 2010) suggests online technologies offer limitless opportunities to "create engaging, relevant, and personalized learning experiences (p. vi)." The promise of an enormous range of educational

experiences and materials spurred phenomenal growth of Internet connectivity and Internet accessible technologies in the K-12 sector. According to the most recent National Center for Educational Statistics report, public school Internet accessibility has risen from less than 10% in 1995 to almost 100% in 2008 (U.S. Department of Education, 2012).

Much of the growth in Internet connectivity can be attributed to the education rate (E-rate) program. Recognizing the increasing importance of the Internet and its potential to improve education, the U. S. Congress created the E-rate program as part of the Telecommunications Act of 1996, to provide discounts on telecommunications, Internet access, and internal networking to schools and libraries. The main goal of this program is to lessen the so-called "digital divide" by ensuring Internet access equity across poor and rich, rural, urban and suburban areas, and highly served and underserved areas (Manzo, 2010; Holt & Galligan, 2012).

A number of challenges have diminished realization of the Internet's educational potential. One of the most significant and controversial challenges involves the possible exposure of minors to inappropriate online content including, pornography, hate speech, and other controversial materials. Public concern about the proliferation of objectionable online content has prompted various legislative attempts to shield minors from exposure to offensive Internet content (Ott, et al., 2010; Gros & Hancock, 2011). The limited success of these legislative attempts and ongoing debate about minors' online safety underscores the delicate balance between First Amendment free expression rights and government regulation of Internet activity to protect youth from online obscenity and indecency.

Internet Safety Legislation and First Amendment Issues

From its inception, the Internet has been unregulated and autonomous in nature in that anyone with technical skills could post any kind of information including offensive and illegal content. The Internet is also a global medium. These factors have complicated any efforts to regulate online content because it is extremely difficult to develop one standard by which to regulate this medium (Hall, 2011; Gossett & Shorter, 2011; Leberknight, Chiang & Wong, 2012). Legislative efforts to restrict access to objectionable online content incorporate two kinds of technology--adult verification technology, which restricts access on the publisher end and software filters, which restrict access on the user end. Congressional legislation initially relied upon adult verification technology to zone Internet speech into adult zones and minor zones, but when this regulatory approach failed constitutional scrutiny, subsequent legislation relied upon filtering software to protect minors (Gros & Hancock, 2011; Macleod-Ball, 2011). Recently, congressional legislation has evolved to include more comprehensive and proactive approaches beyond restrictive measures emphasizing technology, to focus on Internet safety education and awareness (Essex, 2009). Table 1 provides an historical perspective of major Internet safety legislation having direct or indirect implications for K-12 Internet filtering and safety policy development.

The Communications Decency Act and the Child Online Protection Act

The Communications Decency Act (CDA) (1996) was Congress' initial attempt to regulate indecent online materials. CDA made it a criminal offense to send or post obscene material through the Internet to youths under the age of 18. The Internet's democratic nature and fears that government regulation would diminish this important

Table 1. Historical Overview of Major Internet Safety Legislation

Legislation	Summary	Internet Safety Approach	Status/Outcome
Communications Decency Act (1996)	Prohibited posting/sending obscene online material to individuals under 18	Adult Verification Technology	Ruled Unconstitutional
Child Online Protection Act (1998)	Prohibited commercial Web sites from displaying material deemed harmful to minors	Adult Verification Technology	Ruled Unconstitutional
Children's Internet Protection Act (2000) & Neighborhood Children's Internet Protection Act (2000)	Required schools and libraries receiving certain federal funds to use technology protection measures to prevent minors from accessing obscene materials	Filters and Internet Safety Policy	Enacted into law
Protecting Children in the 21st Century Act (2007)	Prohibited access to a commercial social networking website or chat room unless used for an educational purpose with adult supervision	Expanded content filtering to include social networking sites and chat rooms	Revised version excluding expanded filtering provision, but including Internet safety awareness and education passed the Senate
Broadband Data Improvement Act (2008); Title II, Protecting Children in the 21st Century Act (2008)	Requires schools with Internet access to educate minors about appropriate online behavior, including online social networking and chat room	Internet safety awareness and education	Enacted into law

Table 1 (continued)

Legislation	Summary	Internet Safety Approach	Status/Outcome
	interactions and cyber bullying awareness and response		

venue of free expression motivated free speech proponents such as the American Civil Liberties Union (ACLU), the American Library Association (ALA), the National Education Association (NEA), Internet Free Expression Alliance, and several gay and lesbian groups to oppose vehemently any attempts to regulate Internet activity (Hall & Carter, 2006; Internet, 2011). Consequently, CDA was immediately challenged. The Supreme Court ultimately struck down the CDA, ruling that the statute was too ambiguous and not narrowly constructed to meet the government's goal of protecting children, while maintaining First Amendment rights (Gros & Hancock, 2011; Macleod-Ball, 2011).

The Child Online Protection Act (COPA) was Congress' next attempt to protect minors from an ever-increasing body of pornographic Internet materials. To avoid the vagueness and constitutional problems inherent in CDA, COPA was more narrowly focused. Instead of focusing on all online indecency, COPA (1998) targeted commercial entities on the Internet, rather than e-mail, chat rooms, or online bulletin boards, and criminalized "any communication for commercial purposes that is available to any minor and that includes material that is harmful to minors" (Section 231). The legislation required that minors' access to these materials be restricted using adult verification techniques such as credit cards, digital age verification certificates, or other verification methods (Gros & Hancock, 2011). In 2003, a federal court blocked COPA's initial

enforcement because the age verification techniques it required disproportionately infringed upon adults' free expression rights. COPA effectively died in January 2009, after a decade of litigation, when the Supreme Court refused to hear the government's final appeal (Supreme Court, 2009). During the appeals process, the Court ruled user-based filters were a less speech-restrictive, but similarly effective means of protecting minors from objectionable online content (Macleod-Ball, 2011).

The Children Internet Protection Act and the Neighborhood Children's Internet Protection Act

The Children's Internet Protection Act (CIPA), signed into law in 2000, was Congress' third attempt to regulate minors' access to online obscenity and indecency. Hoping to avoid the constitutional issues that undermined CDA and COPA, Congress changed its approach with CIPA (Jaeger &Yan, 2009; Spurlin & Garry, 2009). Instead of placing restrictions on Web publishers, CIPA placed restrictions on schools and libraries receiving Library Services and Technology Act (LSTA) funds, Title III of the Elementary and Secondary Education Act (ESEA) funds, Museum and Library Services Act funds, or E-rate funding (Jaeger & Yan; Menuey, 2009; Sutton, 2012). CIPA (2000) required libraries and schools receiving funds from the aforementioned sources to use technology protection measures (filters) on all computers to restrict access to indecent online materials.

Free speech advocates, including the ALA and ACLU, immediately brought court challenges against the law, claiming its filtering mandate infringed upon users' First Amendment rights. A federal district court declared CIPA unconstitutional on First Amendment grounds because the filtering mandate prevented users from accessing legitimate Web sites as filters inadvertently block legitimate content while blocking

objectionable online materials (Menuey, 2009). Menuey adds that CIPA's constitutional challenge did not include public schools and school libraries; therefore, the district court ruling did not apply to schools. Schools were not included in the court challenge because previous legal precedent gave them wider latitude in limiting students' free speech (Hall & Carter, 2006; Sutton, 2012). Unlike public libraries, schools serve a subset of the community not the entire community. Nevertheless, CIPA withstood legal challenges when the Supreme Court ruled it constitutional in a plurality decision in 2003 (Internet, 2011).

CIPA and a related act, The Neighborhood Children's Internet Protection Act (NCIPA), are part of a larger appropriations law (PL 106-554).The language is similar in the CIPA and NCIPA sections of PL 106-554, but there are important differences. CIPA stipulates what must be filtered (visual images that are obscene, child pornography, or harmful to minors) and requires the implementation of an Internet safety policy. NCIPA focuses on what must be included in a school or library's Internet safety policy and is applicable only to schools and libraries participating in the E-rate program (Jansen, 2010). Jansen also notes that CIPA defines the phrase "harmful to minors," but NCIPA directs the local school board or governing body to determine what is and is not suitable for minors to access under its Internet safety policy or acceptable use policy (AUP). CIPA and NCIPA impose three mandates on affected agencies. These mandates include a safety policy (also called acceptable use policy), use of a technology protection measure to prevent access to child pornography or materials harmful to minors, and a public meeting informing the community of measures taken to keep minors safe while using the Internet (Menuey, 2009).

Post-CIPA Internet Safety Legislation

Enactment of CIPA and its technology protection measures have not dispelled concerns about children's online safety. Lawmakers continue to introduce Internet safety legislation intended to protect children on the Internet. This suggests CIPA's safety strategies have not kept pace with threats posed by rapidly developing technologies, particularly mobile technologies, wireless technologies, and burgeoning Web 2.0 applications such as social networks, blogs, wikis, video sharing, and photo sharing (Miller, Thompson & Franz, 2009; Spurlin & Garry, 2009; Willard, 2010a). Essex (2009) reports that 15 bills were introduced during the 109th Congress (2005-2006) and 36 bills were introduced during the 110th Congress (2007-2008) that referenced child exploitation, sexual predators, Internet safety, and related online threats. Essex suggests that the growing popularity of social networking Web sites and increased awareness of online predators prompted a significant increase in Internet safety legislation during the 110th Congress (2007-2008). Among the 36 Internet safety bills introduced during the 110th Congress, there were various responses, approaches, or solutions to Internet dangers and online child exploitation.

Prompted by rising public concern that sexual predators were using social networking sites and chat rooms to locate potential abuse victims, the Deleting Online Predators Act of 2006 (DOPA) was passed in the House of Representatives (Gros & Hancock, 2011). DOPA would have expanded CIPA's filtering mandate by requiring E-rate funding recipients to prohibit minors from accessing social networks and chat rooms in addition to blocking access to obscene, pornographic or "harmful to minors" materials. DOPA was included in a related Senate bill, the Protecting Children in the 21st Century

Act of 2007 (S. 49), which did not pass in the Senate chamber. However, a reworded version of the Protecting Children in the 21st Century Act (S. 1965) passed the Senate by unanimous consent in May, 2008 (Essex, 2009). Essex states S. 49, which incorporated DOPA, included a filtering and an Internet safety awareness approach, but S.1965 deleted the filtering approach, expanded the awareness approach, and added an education approach. Senate bill 1965 subsequently became part of Public Law 110–385, the Broadband Data Improvement Act of 2008. The law, also known as the Protecting Children in the 21st Century Act, requires schools receiving federal E-rate funding to educate students "about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber bullying awareness and response" (Section 215). While online safety legislation has diminished with subsequent Congresses, state legislatures continue to debate online safety and pass legislation designed to protect students from Web 2.0-related safety threats (Adams, 2010; King, 2010; Pierce, 2012). Whether at the national or state level, most online safety legislation either directly or indirectly influences school technology use policies.

In addition to federal Internet filtering and safety legislation, many states have enacted filtering laws to prevent minors from accessing sexually explicit, obscene, or harmful content. According to the National Conference of State Legislatures (2013), 25 states have filtering laws applicable to public schools and libraries. Most of these laws require the affected agencies to adopt Internet safety policies that protect minors from inappropriate online materials while some laws specifically require the installation of filtering software.

The emergence of interactive social technologies has also prompted state

legislators to pass laws to protect minors from online predators and cyber bullying. Cyber bullying legislation has been passed in 20 states according to King (2010). These laws differ in scope, but describe the tools of cyber bullying as electronic communication, Internet technologies, and several states include cell phones (Miller et al., 2009). King adds that most of the state cyber bullying laws focus on public schools, requiring school boards to establish policies prohibiting cyber bullying.

The prevalence of post-CIPA Internet safety legislation reflects legislators' ongoing concern about Internet dangers and child exploitation on the Internet (Essex, 2009) and the inability of legislative policy to keep pace with rapidly changing technology (Fuchs, 2012; Miller et al., 2009). Moreover, school level policy implementation lags behind legislative enactment by several years, thereby propelling school technology policy development and implementation into a state of flux (Adams, 2010). Educational policy emerges from multiple levels—federal, state, school district, and building level—which complicates policy coordination. Censorship and First Amendment issues are also inextricably linked to safety policies. Therefore, policymakers must balance individual rights with safety concerns. Schools do not have a significant amount of legal precedent upon which to base safety policies, making Internet policy development a more difficult task (Miller et.al.).

Filtering and First Amendment Issues

The First Amendment states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances" (U.S. Constitution). The potential

erosion of free speech rights has been at the core of the filtering debate. The ALA and ACLU are two of the largest and most vocal organizations leading the fight against the use of Internet content controls. Both groups believe the use of filtering software in public schools and libraries violate the First Amendment's assurance of free speech and expression (Fuchs, 2012; Spurlin & Garry, 2009). Filters cannot limit blocking solely to what CIPA mandates—materials harmful to minors, obscenity, and child pornography—without blocking constitutionally protected information.

The First Amendment is the basis for the ALA's Library Bill of Rights, which affirms the library's responsibility to uphold the principles of intellectual freedom—unfettered access to information and ideas regardless of its source, background, or viewpoint. Article V of *The Library Bill of Rights* was amended in 1980 to include "age" and reaffirmed this stance in 1996 (American Library Association, 2013b) in response to mounting public concerns about minors having free access to inappropriate Internet materials in libraries. In an interpretation of the Library Bill of Rights, the library organization contends that limiting access to non-print resources or information technology based on age abridges library use for minors. The ALA believes minors should have access to these resources with or without parental permission (American Library Association, 2013a). This philosophical stance has prompted the ALA to oppose legislation such as CIPA—the goal of which is to restrict minors' access to inappropriate Internet materials.

Minor's First Amendment Rights and Court Precedents

The ALA's philosophical position raises the question of whether minors have the same right to access information as adults in the eyes of the courts. Generally, the courts

have granted schools greater latitude in limiting students' First Amendment rights (Alexander & Alexander, 2012; Chmara, 2010; Hoover, 2009). Several landmark court cases have framed the extent of minors' First Amendment rights in public school settings. These cases demonstrate the tension between balancing First Amendment ideals with educational officials' responsibility to inculcate values (Hall & Carter, 2006). In the landmark case of *Tinker v. Des Moines Independent Community School District* (1969), the Supreme Court clearly protected students' freedom of expression in the public school settings. The Court's famous statement—"It can hardly be argued that either students or teachers shed their constitutional rights to freedom of speech or expression at the schoolhouse gate"—establishes a precedent supporting minors' rights to free expression within the school setting. On the other hand, the Court in handing down the *Tinker* decision reiterated the school's authority to inculcate and to intervene and take appropriate action when student expressions cause disruptions to the educational environment.

In another landmark case, *Board of Education, Island Trees Union Free School District, No. 26 v. Pico* (1982), a New York school board had removed several books from a high school library because they were anti-American, anti-Christian, anti-Semitic, and just plain filthy" (Alexander & Alexander, 2012, p. 355). The Court ruled that a school board must be allowed, "to establish and apply their curriculum in such a way as to transmit community values" (Pico, 457 U.S. at 853), but the First Amendment precludes the removal of school library books in order to deny access to ideas believed to be objectionable. Being that the school board's decision was not content neutral, the board was essentially engaging in viewpoint discrimination, a biased or political attempt

to protect certain ideas while suppressing others. Despite its prohibition of viewpoint discrimination, the Supreme Court has given public schools significant latitude to limit minors' access to information if school officials have made an objective judgment that the information is "educationally unsuitable," as opposed to deciding to limit access to information based upon disagreement with or disapproval of the content of the information (Alexander & Alexander; Chmara, 2010).

There are various opinions about how these cases apply to the constitutionality of Internet content filters in public schools and what, if any, legal challenges could be mounted against the use of Internet filters in public schools. In handing down the *Pico* decision, the Supreme Court distinguished between the acceptable decision of school officials not to purchase books because of pervasive vulgarity or lack of educational suitability and the unacceptable removal of library books in order to suppress ideas considered politically or socially objectionable (Alexander & Alexander, 2012). This legal principle has been made analogous to filtering Internet content in recent court cases involving the constitutionality of Internet filters.

In *American Library Association v. the United States* (2003), the district court adopted the analogy that Internet filtering was like the unconstitutional removal of books from a library; however, the Supreme Court did not agree with this analogy. The *ALA* plurality opinion viewed Internet content blocking as analogous to a library's decision not to include certain material in its collection. In upholding CIPA, the Court concluded that libraries should have broad discretion in determining what materials to include in their collections (Hall & Carter, 2006). Legal precedent regarding minors' rights to access information, and public pressure to protect minors has driven rapid and widespread

implementation of filters in public schools (Jaeger & Yan, 2009). Jaeger and Yan add that there has been little resistance to CIPA in schools as compared to public libraries.

Litigation Resulting from Internet Safety Policy Implementation

Despite widespread deployment, filtering opponents argue one source of litigation arises from the way Internet filtering and safety policies are being implemented in public schools. First Amendment advocates purport the blocking decisions of some filtering programs reflect a particular ideological perspective, which is analogous to viewpoint discrimination, a practice specifically forbidden by legal precedents (Alexander & Alexander, 2012; Willard, 2010b). Willard maintains that districts may unknowingly be engaging in viewpoint discrimination because filtering companies, who protect what they block as a trade secret, may block Web sites based on particular ideological perspectives. Holzhauer (2009) concludes that when schools set filters at the most restrictive level and deploy them based on the vendors' default setting, viewpoint discrimination is likely to occur.

Viewpoint discrimination has been cited in recent ACLU lawsuits against school districts. In May 2009, the ACLU filed a lawsuit on behalf of several students and an SLMS in Tennessee's Knox county and metropolitan Nashville school districts. The plaintiffs argued the districts' filtering software blocked students from accessing sites providing information and resources about gay and lesbian issues, but the filter did not block sites promoting the view that homosexuals could be rehabilitated and become heterosexuals (Manzo, 2009; Staino, 2009). According to Staino, the filtering software the districts were using, when deployed at the default setting, blocked all sites categorized as lesbian, gay, bisexual, and transgender (LGBT). The federal court

dismissed the lawsuit in August 2009, when school officials agreed to unblock the sites (Manzo, 2009).

More recently, the ACLU launched its “Don’t Filter Me” campaign to prevent school districts from filtering pro-LGBT information. The organization contacted several school districts asking them to reset their filters to allow access to this content. Leading filtering software companies were also contacted and asked to remove supportive LGBT Web sites from their blacklists. The ACLU claimed school districts using filters from companies such as Lightspeed Systems, Blue Coat, Fortiguard, and Websense were engaging in viewpoint discrimination (Zwang, 2011). According to the ACLU, school districts were engaging in viewpoint discrimination because these filters reportedly blocked educational or supportive LGBT content while permitting access to sites that oppose LGBT lifestyles. In response to the campaign, some filtering companies, including Lightspeed and Fortigate, changed their filter categories to prevent erroneous blocking of supportive LGBT content (Adams, 2012). Ultimately, the ACLU filed a lawsuit against a Missouri school district alleging improper filtering of educational LGBT content (Quillen, 2011). The lawsuit was settled when the school district agreed to stop blocking the content in question, submit to monitoring, and pay legal fees that were incurred (Associated Press, 2012). The aforementioned legal actions against school districts illustrate the legal challenges districts may encounter if filtering policies are overly restrictive and configured in such a way that they prevent users from accessing resources supporting a particular point of view.

Filters continue to attract legal scrutiny and expose institutions that use them to potential legal action because they provide an imperfect solution to a far-reaching

problem. In July 2003 the Supreme Court ultimately upheld CIPA, which settled the constitutionally of the law. However, legal experts say subsequent challenges to the law may arise from the way the law is implemented. Menuey (2009) explains most of these challenges will not apply to schools, but provides three areas in which additional legal challenges could arise for schools. First, students could raise First Amendment concerns because filters tend to over-block thereby preventing access to materials of interest that is neither "disruptive nor harmful to minors" (p. 45). In addition, legal experts say challenges could also arise because filtering companies essentially decide what materials are being blocked; therefore, school boards are delegating their legal responsibility to make decisions about curriculum content to filtering software companies. Finally, Menuey suggests filtering exacerbates the so-called "digital divide." The divide widens when students with home access to computers are able to access materials at home that are filtered at school, but students without a home computer are denied access to these same materials.

The Influence of Internet Safety Legislation on Internet Filtering and Safety Policies

CIPA and related Internet safety legislation has far-reaching implications for filtering and safety policy implementation. The filtering approach to minors' online safety has garnered most of the attention in the debate surrounding CIPA, but the legislation employs a two-pronged approach, with the second approach being the establishment and enforcement of a comprehensive safety policy (Jaeger & Yan, 2009).

Acceptable Use Policies

Prior to CIPA's enactment, most schools had taken steps to address Internet safety concerns and prevent computer and Internet abuse. One step was the development and

implementation of Acceptable Use Policies (AUPs). AUPs include school board adopted rules, regulations, rights, and responsibilities that govern users' computer-related activities (CoSN, 2011; Robinson, Brown & Green, 2010). Schools usually require all users (and parents of minors) to sign a legally binding agreement indicating they understand the policy's privileges, responsibilities, and policy violation penalties. AUPs typically prohibit use of the Internet for non-educational activities, and forbids malice, recklessness, invasion of privacy, theft, harassment, bullying, copyright infringement, lewd and vulgar expression in all forms (words, pictures, videos, or sounds), and use of technologies to violate other institutional policies (Ahn et al., 2011; Robinson, Brown and Green).

Filtering technology proponents believed AUPs were insufficient protection for children and that limiting access to Internet content would be a better approach. Consequently, pro-filtering groups began lobbying Congress in favor of filtering legislation, which eventually resulted in CIPA's enactment (Fuchs, 2012; Finsness, 2008). CIPA's regulations have greatly influenced the content, implementation, and importance of AUPs in schools.

CIPA-Compliant Filtering and Safety Policies

CIPA compliance requires schools and public libraries to adopt an Internet safety policy, which is commonly referred to as an AUP (Jansen, 2010). CIPA compliance is required if an institution's funding sources include:

- Universal Service (E-rate) discounts for Internet access, Internet service, or internal connections;

- Library Services and Technology Act (LSTA) state grant funding to buy computers used to access the Internet or to pay direct Internet access costs; and
- Title III funding under the Elementary and Secondary Education Act (ESEA) to buy computers used to access the Internet or to pay direct Internet access costs (Gros & Hancock, 2011; Jansen 2010; Sutton, 2012).

In addition to adopting an Internet safety policy, institutions receiving E-rate funds (most schools receive E-rate funds) must provide notice and hold at least one public meeting on the proposed Internet safety policy, and certify annually with the Federal Communications Commission (FCC) that they have adopted and implemented the policy (FCC, 2011), which must include a technology protection measure (filters).

NCIPA, Subtitle C of CIPA, goes beyond the issue of filtering Web pages, requiring E-rate schools to develop and implement a comprehensive policy governing minors' Internet usage (Jansen, 2010). The Internet safety policy must address monitoring minors' online activities (E-rate Central, 2012; Nicoletti, 2009); however, Jansen states electronic monitoring is not required. According to FCC rules, the policy must encompass the following five areas:

- Access by minors to inappropriate matter on the Internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and

- Measures designed to restrict minors' access to materials harmful to minors (NCIPA Section 254, 2000).

CIPA regulations do not specify any brand of filter nor specify a degree of blocking effectiveness, but the filtering policy must be set to block three types of visual depictions including obscenity, child pornography, and material that is "harmful to minors" (E-rate Central, 2012). CIPA defines the phrase, "Harmful to minors," as:

> any picture, image, graphic image file, or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. (Children's Internet Protection Act, 2000)

NCIPA (2000) does not define "inappropriate matter," but allows the local school board to determine what is and is not appropriate for minors to access under its Internet safety policy (Jansen, 2010). This provision allows schools to establish filtering policies that block content beyond the three types of visual depictions specified by CIPA (E-rate Central, 2012).

According to E-rate Central (2012), CIPA compliance also includes enabling filters on all Internet accessible computers regardless of whether the computer is used by minors or adults. The law allows the filter to be disabled for adults only for bona fide research or other lawful use by an adult (Chmara, 2010; Jansen, 2010). E-rate Central notes that the ESEA and LSTA sections of CIPA allow filters to be disabled for both

adults and minors, but there is no disabling provision for minors in the E-rate section. Furthermore, no provision precludes schools from setting different filtering policies for students based on academic or age groups, or on an individual basis.

The Protecting Children in the 21st Century Act (2008) adds an additional Internet safety policy requirement regarding educating minors about appropriate online behavior, specifically including social networking and chat room interactions, and cyber bullying. The FCC has not established specific criteria for a CIPA-compliant Internet Safety policy or AUP, but E-rate Central (2012) suggests that a CIPA-compliant Internet safety policy should:

- Be applicable to minors and adults;
- Include the use of an Internet filtering mechanism and specify conditions under which filtering can be disabled or overridden;
- Address staff responsibilities to monitoring minors' online activities and educating minors on appropriate online behavior; and
- Address NCIPA-specific issues concerning safe use of email and other types of electronic communication, unauthorized disclosure of personal information and illegal online activities.

CIPA Compliance in Public Schools

Before the Supreme Court decided CIPA's constitutionality in 2003, most schools had become CIPA compliant by implementing various safety strategies to prevent students from accessing inappropriate online materials (Jaeger & Yan, 2009). The American Association of School Librarians' (AASL) (2012) most recent *School Libraries Count* filtering survey indicates that most schools have implemented filtering software

and safety policies (AUPs) to help maintain students' online safety. Table 2 also indicates schools have employed additional safety measures including supervising students' online activities, limiting Internet access, and allowing Internet access on a case-by-case basis (AASL, 2012).

Table 2. Internet Safety Strategies in Public Schools

Internet Safety Approach	**Percent of Schools Implementing**
Filtering	94
Acceptable Use Policy	87
Supervise Internet Access	73
Limit Internet Access	27
Internet Access on a case-by-case basis	8

Note: Data from "Filtering in Schools: AASL Executive Summary," by the American Association of School Librarians, 2012.

Jaeger and Yan (2009) note several reasons filters have become as ubiquitous as computing devices in public schools. In addition to legal mandates, schools are subject to societal pressures to filter Internet content. Minors are considered a susceptible group for Internet crimes and child pornography; hence, society has determined schools have a fundamental responsibility to protect children from objectionable online materials. In addition, federal E-rate funds are essential to school budgets (Sutton, 2012). In order to enhance and maintain technology, public schools rely heavily on these funds. Consequently, they cannot afford to forego E-rate funding to avoid CIPA's filtering directive. These are the primary reasons there have been few objections to the comprehensive implementation of filtering policies in public schools as compared to public libraries (Jaeger & Yan).

Although legal, political, social, and financial factors necessitate widespread implementation of filters in public schools (Jaeger & Yan, 2009), the literature pinpoints various Internet filtering and safety policy issues having profound implications for policymakers, administrators, educators, and students. Recent prescriptive, anecdotal and research literature reveals the issues related to filtering technology's blocking techniques, and filtering and safety policy implementation in schools.

Issues Related to Filtering Technology and its Blocking Techniques

Internet content filtering technology is employed to restrict users from accessing Web content that violates an institution's AUP. Much of the controversy surrounding filtering technology emanates from the techniques these tools use to filter or block access to Web-based information. Regardless of the position one adopts regarding the filtering controversy, it is generally agreed that filters are an imperfect solution to a complex problem. Filtering technology either "over-blocks" and denies access to legitimate Web sites, or "under-blocks" and permits access to inappropriate Web sites (Moyle, 2012; Sutton, 2012). Ineffective filtering was particularly problematic with first generation filters. However, filtering technology has evolved from simplistic keyword and URL blocking to more sophisticated tools employing a combination of blocking techniques (Baule, 2010; Houghton-Jan, 2010; Hua, 2011). The latest content filters can be very powerful, according to Houghton-Jan, when they utilize artificial intelligence, image recognition, and complex keyword analysis algorithms at a very granular level.

Keyword Filtering

Keyword filtering is the most basic filtering method. This technique uses a dictionary of blacklisted words or phrases with assigned positive or negative scores.

When users request pages, the page is examined for occurrences of these words or phrases. If a requested page exceeds a user-determined threshold, the page is blocked (Hidalgo et al., 2009; Quillen, 2010). Blacklists have expanded to include millions of keywords and phrases, but updates are performed manually according to Nicoletti (2009). Some vendors allow the customer to update or fine tune the list manually to lessen the occurrence of false positives. For example, the blacklist can be customized to allow a page containing “wire strippers,” but block one containing “strippers” alone.

Keyword blocking is known for blocking innocuous Web pages because it filters Web content without regard its context. However, this technique offers some advantages. One advantage is that keyword filtering can quickly determine if a Web page has potentially harmful content (Banday & Shah, 2010). In addition, the dictionary of objectionable words and phrases does not require continuous updates. As the over-blocking rate is usually unacceptable for most institutions, this filtering technique typically is used in combination with other methods (Chou, Sinha, & Zhao, 2010; Hidalgo et al, 2009).

URL Filtering

URL filtering prevents or allows Web access by checking a requested Web site's URL against a URL database that is categorized according to content (i.e., shopping, gambling, etc.) (Sutton, 2012). Categorization allows network administrators to make blocking decisions based upon content categories. There are two types of URL databases—a black list database that contains URLs of objectionable Web sites and a white list database that contains URLs of acceptable Web sites (Chou et al., 2010). Most filtering solutions that employ this technique use black lists (Hidalgo et al., 2009). This

blocking method can be configured to block entire URLs or only permit access to non-offensive content on the Web site. As with keyword blocking, vendors usually provide a basic URL database requiring the user to perform manual updates. Updates must be performed frequently to keep pace with rapidly expanding Internet content; otherwise, an institution's URL blacklist could easily fall out of compliance with its AUP (Nicoletti, 2009).

This type of filtering is time consuming and resource intensive since most URL blocking systems enlist human reviewers to maintain updated URL lists. Filter developers are increasingly using automated tools to improve the updating process. Automated Web spiders tag potentially offensive sites while human reviewers follow-up to validate the automated classifications (Hidalgo et al., 2009; Houghton-Jan, 2010). Nevertheless, creating and maintaining URL databases continues to be a labor-intensive and expensive process (Banday & Shah, 2010; Chen & Wang, 2010). Therefore, commercial filtering companies typically will not reveal specific Web sites by category because the information is proprietary or a trade secret (Gossett & Shorter, 2011; Houghton-Jan; Willard, 2010b). Since content-based decisions about what is blocked are not shared with customers, filtering software critics argue schools and libraries are relinquishing their responsibility to make content and selection decisions to filtering software companies (Jaeger & Yan, 2009). Sutton (2012) adds that the proprietary claim makes it difficult to move an incorrectly categorized Web site to a more appropriate category.

As speed and accuracy are key attributes of good filtering systems, most commercial and open-source Web filters use URL filtering as the primary filtering technique. Koumartzis and Veglis (2012) suggest that URL filtering technology is easier

to implement and its fast processing speed supports implementation on a massive scale, such as in school districts with distributed locations. However, an inherent fault of site blocking is its focus on HTTP-based traffic, which fails to detect and block instant messaging, email attachments, and file sharing applications that may threaten network security. Therefore, most public schools use commercial filtering products that employ a combination of filtering techniques in order to achieve greater content blocking effectiveness (Chou et al., 2010; Nicoletti, 2009).

Real-time Contextual Analysis and Categorization

URL and keyword-matching filtering, the earliest filtering approaches, cannot effectively filter the many different types of Web content and protocols of today's Internet traffic (Selamat, Zhi Sam, Maaroff & Shamsuddin, 2011). Contextual analysis filtering—also known as intelligent content analysis (Hidalgo et al., 2009)—uses the latest Web filtering techniques to analyze the patterns and context of text to achieve a semantic understanding of the context of the words and phrases on a Web page. This process, when used in conjunction with keyword blocking, reduces over-blocking errors that occur when Web pages contain words that can be objectionable in some contexts. Machine learning techniques categorize Web pages according to salient features, and then the results are cached, including offensive and non-offensive content, to maximize accuracy and performance (Banday & Shah, 2010; Nicoletti, 2009).

With dynamic blocking, URLs and category information is updated dynamically, eliminating the need to manage and update local blacklists manually. This real-time categorization process reduces under-blocking—a primary weakness of URL blocking—that occurs when emerging inappropriate content has yet to be added to the

URL blacklist. Chen and Wang (2010) adds that this filtering approach is advantageous because of its ability to examine various elements of a Web page for classification, including the metadata, links, text, images, and scripts. However, Varadharajan and Cohen (2010) contend dynamically generated content on social networking sites, secure sockets layer security protocol (SSL) and non-HTTP protocols for email, discussion groups, chat, news servers, and instant messaging continue to create technical and practical challenges for filtering technology. The most important disadvantage of real-time content analysis is inadequate performance. Accurate content analysis systems can be developed, but slow processing time makes them inappropriate for most demanding filtering situations (Banday & Shah, 2010; Koumartzis & Veglis, 2012). Consequently, most commercial filtering tools only use this technique to augment more efficient (faster) filtering techniques such as URL filtering (Chou et al., 2010).

Other Filtering Techniques and Technology Protection Measures

Image processing continues to be an active filtering research area because of the ever-increasing volume of images and multimedia on the Internet, and particularly since pornographic images are what CIPA stipulates must be filtered. Most commercial filtering tools classify Web content as pornographic or safe, using text on the Web page. However, text-based processing is not effective with Web pages containing mostly images and minimal or obfuscated text (Chen & Wang, 2010). Image filtering, based on skin detection, is an emerging technique with a high degree of accuracy, but slow performance makes this technique unusable in real-world systems. Consequently, most filtering systems employ moment analysis, textures, histograms, and statistics to produce an algorithm that Hidalgo et al. (2009) purport to be highly effective in recognizing

pornographic images. However, Sutton (2012) and Chmara (2010) assert current filtering technology cannot accurately block only visual depictions of child pornography, obscenity, and material harmful to minors as CIPA mandates.

Content labeling is a self-regulating, self-labeling method of content control. When a Web site is developed, the Webmaster describes the Web site's content using an Internet Content Rating Association (ICRA) generated questionnaire. Content labels are created from the questionnaire results, which are used to either block or to allow access to online content. The RTA (Restricted to Adults) and POWDER (Protocol for Web Description Resources) are similar self- regulating content labeling initiatives. Webmasters are not required to submit content labeling data; therefore, many Web sites are not labeled. Nevertheless, IRCA, RTA, and POWDER labels are available in many different content control software and Web browsers (Bertino, Ferrari, & Perego, 2010; Jeon, Lee, & Won, 2011; Nicoletti, 2009). Content labeling is not regulated, therefore, some publishers intentionally or mistakenly mislabel their Web content, thereby permitting users to access unwanted content (Banday & Shah, 2010; Jeon et al.). Consequently, these self-labeling systems should only be used to augment other Web filtering tools.

Filter Deployment within the Network

Web filtering solutions can be deployed in several different network scenarios, which substantially affect their customization, performance, and manageability (Hidalgo et al., 2009). The software can be installed on individual workstations, a networked proxy server, a caching appliance, or firewall, or can be installed on a dedicated server (Enex Testlab, 2011). Filtering techniques and deployment within the network can substantially

influence information access, requiring administrators to balance a number of issues including performance, flexibility, and costs to maximize information access.

Filters installed on individual workstations (also called client-side filters) are usually part of a full security suite that includes antivirus, firewall, and other security protections. Client-side filtering can be enhanced by the filtering capabilities of most traditional Web browsers. Workstation based filtering/security solutions are only feasible for home users or small schools/districts because of manageability issues. This type of deployment requires individual workstation configuration and cannot accommodate site-wide policies that apply to all computers (Enex Testlab, 2011; Hidalgo et al., 2009). Since most school districts have many networked computers at distributed locations, they require standalone solutions consisting of a dedicated database server and a separate gateway or firewall that executes the content filtering policy (Thomas & Stoddard, 2011). Moreover, tech savvy users can easily bypass client-side filtering solutions to access blocked content.

Filters can be deployed at various points on the network, including on a dedicated server, bridging the filtering server between the access point and the rest of the network or installing the filtering product on a proxy server through which all Internet traffic is routed. Filtering at the network level is a better choice for institutions with distributed locations because filtering policies are created once on the gateway and then pushed down to individual desktops (Enex Testlab, 2011; Hidalgo et al., 2009; Thomas & Stoddard, 2012). Networked filtering solutions require maximum performance as they must monitor and filter traffic from many simultaneous users, a standard that is difficult to achieve unless they are installed on dedicated high performance servers or appliances

with special network hardware. Networked filtering deployment is typically less vulnerable to hacking and similar security risks (Nicoletti, 2009).

A disadvantage of the dedicated appliance solution is the added expense of purchasing and managing two separate hardware devices along with the filtering software. Additional storage is required for the database server as the database of Web sites increases. Websense and SurfControl are two well-known software/server solution vendors. Some school districts choose integrated solutions that combine management and processing on one gateway or firewall, thus reducing hardware and operational expenses. However, when the gateway also houses anti-virus and intrusion prevention, performance can be degraded (Enex Testlab, 2011; Gossett & Shorter, 2012).

Filtering can also occur at the ISP (Internet Service Provider) or carrier level. ISPs offer their customers a full suite of security services, including firewalling, antivirus, anti-spam, and Web filtering. These security solutions, which are suitable for all kinds of institutions and home users, are installed on servers at the ISP level. The quality and extent of customization of this filtering solution depends on the product purchased. Products that offer basic security services do not allow much user configuration, but if higher quality, more expensive filtering/security products are purchased they enable the institution-based IT administrator to implement a full suite of institution-defined filtering policies remotely. ISP-based filtering performance (speed) is usually not an issue as they are optimized to handle millions of concurrent users with minimum delay (Banday & Shah, 2010; Enex Testlab, 2011; Hidalgo et al., 2009).

Content Filtering Challenges

Administrators and policymakers have many options and challenges to weigh when selecting a filtering solution and establishing filtering policies. Increasing online threats from email, chat rooms, peer-to-peer sharing sites, spam, viruses, worms, etc., demand that school districts not only filter objectionable Internet content, but also content that could subject the network to the aforementioned threats (Thomas & Stoddard, 2011). Additionally, filtering policies must combat non-educational use, bandwidth consuming content, legal liability, and security breaches (Hidalgo et al., 2009; Nicoletti, 2009).

To address these challenges, the latest security solutions combine security functions such as firewalls, antivirus protection, Web content filtering, anti-spam, spyware prevention, intrusion detection and prevention, Internet Protocol security, and bandwidth management. These security solutions, also known as unified treat management (UTM) appliances, dynamically control Web traffic at the organization's gateway providing inline examination of Web content, SSL traffic, Web 2.0 applications, and various network protocols to classify dynamic content in real time (Ramaswami, 2010; Enex Testlab, 2011). For most school districts, the greatest challenge to implementation of this type security appliance is cost. According to Ramaswami, “K-12 schools rarely have the budget to invest in these next-generation security tools, which involve the cost of upgrades, maintenance, and user training (p. 27).” Consequently, schools are relying on traditional filtering software, which typically blocks entire sites instead of dynamically scanning Web sites to block inappropriate content and allow appropriate content.

Computer-savvy users have discovered numerous ways to circumvent filters and exploit built in weaknesses of some commercial filtering tools. Some URL filters use only the domain name, not including the IP address, allowing users to input a Web page's IP address to access blocked content. Even when the filter uses both IP addresses and URLs to block content, it is possible for circumventors to take each number in the IP address and convert it to a hexadecimal, then enter it into the browser's address bar. Scripts to compute hexadecimal format are readily available on the Internet. Web publishers use techniques that cause inappropriate content to be unfiltered and passed on to the user (Fuchs, 2012). Illegal content can be disguised using JavaScript, which some filtering software cannot parse or interpret. Another common ploy is to assign safe labels to inappropriate content. Therefore, filtering based on labels is not very accurate (Hidalgo et al., 2009).

The use of proxies to bypass filtering mechanisms is the greatest challenge to content filtering implementation according to Gossett and Shorter (2011). When tech-savvy users want to bypass the filter to access blocked content, they utilize a variety of proxies including public and private Web-based proxy sites, proxy clients installed on flash drives and on remote computers, or by simply changing the browser configuration to use an open proxy (Chen & Wang, 2010; Varadharajan, 2010). The most effective method to counteract circumvention is via packet inspection, certificate examination, and other heuristic techniques (Nicoletti, 2009; Varadharajan). Nevertheless, Gossett and Shorter (2011) claim it is virtually impossible to prevent private proxy servers from being used to circumvent most firewall schemes. The Online Safety and Technology Working Group (OSTWG) (2010)—a group established pursuant to the Protecting Children in the

21st Century Act of 2008—concluded that even though software manufacturers advertise circumvention-proof filtering products, tech-savvy users seem to find a way to outsmart the filter to access prohibited content.

Users can also circumvent filters using other methods including alternative protocols (i.e. FTP, telnet, HTTPS) or searching in a different language. Language translation can be used to confuse the filter by converting a blocked Web site to a language that the filter does not support. Even when users cannot access external proxies, they can use low-tech circumvention methods such as viewing the cached versions of blocked Web sites via search engines like Google (Hidalgo et al.). Effective filtering solutions support multiple languages, and inspect/rate many different Internet protocols. Filtering solutions have the added challenge of inspecting email traffic and making block or allow decisions based upon the content filtering policy (Nicoletti, 2009).

Establishing a safe and secure online environment has become an ongoing challenge. Nicoletti (2009) characterized the content filtering challenge in the following statement: “Content filtering is a fast-paced battle of new technologies and the relentless trumping of these systems by subversion and evasion” (p. 743). Yet, IT administrators must allow access to information and resources that support the school district’s education mission. In addition to supporting the district’s education mission, filtering policies must also enforce districts' AUPs, which should work in concert with other approaches such as online safety education, digital citizenship education, and constant monitoring of students' online activities (Hidalgo et al., 2009; Johnson, 2012; OSTWG, 2010). Filtering policies that are not carefully configured to minimize over-blocking can lead to censorship, but can be effective tools “when chosen, configured, and monitored

carefully" (Johnson, 2012, p. 87). However, the AUP must clearly delineate appropriate online behavior and specify ramifications when the policy is violated. In summary, the literature suggests that the enormous challenges to achieving online safety for minors can only be accomplished through a multifaceted approach with filtering technologies being one facet (Losinski, 2009; OSTWG; Sutton, 2012; Varadharajan, 2010).

Filtering and Safety Policy Implementation Issues

Filtering Policy Configuration Issues

Filtering policies are an extension of an organization's Internet safety policy, and govern filtering software configuration. Filters work in concert with AUPs to manage users' online access and to prevent Internet abuses such as accessing inappropriate Internet content (Hidalgo et al., 2009; Thomas & Stoddard, 2011). The literature review suggests that the most prevalent filtering policy concerns emanate from the way school districts are implementing filtering policies. The filtering debate continues among educators, not so much in regards to the constitutionality of filtering Internet content, but regarding how filtering and safety policies are being implemented in school districts (AASL, 2012; Fuchs, 2012; Ott et al., 2010). Establishing filtering policies involves the consideration of several factors having considerable influence on end users' access to information and resources. These factors include:

- Determining which categories to block—beyond what CIPA mandates—and whether to fine-tune some blocked categories to allow access to non-objectionable content within the category. Most filtering solutions provide granular category blocking, which allows administrators to block entire content categories or limit blocking to specific subcategories (See Figure 1);

- Determining the level of involvement stakeholders (IT staff, administrators, faculty, parents, and students) will have in filtering policy decisions;
- Determining who will be granted filter override privileges and;
- Determining whether the same filtering policy will apply to all users or whether to customize the filtering policy according to specific user groups (i.e., setting different policies for elementary students, secondary students, and staff).

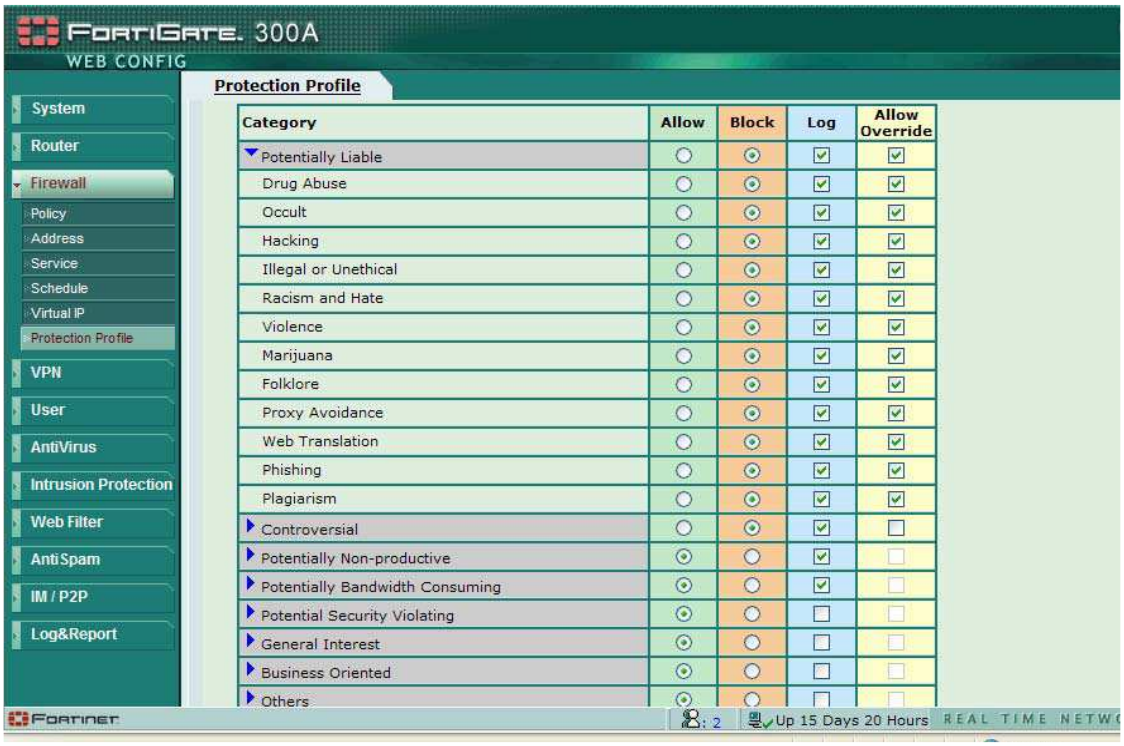

Figure 1. Example of Fortigate's® granular category interface.

The literature outlines various best practices for establishing effective filtering policies in order to maximize access to information in a secure environment. Over-blocking can be minimized if the filtering product provides a granular category list that can be expanded into subcategories (as shown in Figure 1), thereby, enabling IT administrators to set different policy actions for each subcategory (Nicoletti, 2009; Hua,

2011). Filtering policies and rules should be developed by a committee, including representatives from various stakeholder groups in order to lessen filtering issues and provide greater access to education resources (Baule, 2010; Jansen, 2010; Johnson, 2012). Collaborative content filtering decision-making increases staff buy-in as end users will have a greater understanding of the reasons for filtering policy decisions. Hua recommends that filtering policies be tailored for specific user groups such as elementary students, secondary students, educators, and administrators. For example, teachers may need to access certain Web content (i.e., pro-Nazi Web sites) for instructional purposes, but the policy could be set to prevent students from accessing this content. Filtering/usage policies should define what content is blocked in addition to user profiles and their access privileges. An effective filtering solution provides a wide range of categories and makes it possible to establish sophisticated user profiles that meet the research, educational, or professional needs of all user groups (Hua; Ott et al., 2010). Finally, SLMS, administrators, or technical support personnel on each campus should be granted override privileges so users will have timely access to curriculum-related information and resources (Ott et al.; Willard, 2010b).

Recent experiential literature suggests that policymakers, administrators, and IT personnel may be establishing and implementing filtering policies without considering the aforementioned best practices. The literature also implies that these policy decisions are having adverse effects on users' access to information and teachers' abilities to deliver instruction. Baule (2010) notes that districts are also blocking non-educational content and content that threaten network bandwidth, efficiency, and security. Many school districts are interpreting CIPA's requirements too broadly and have established

overly restrictive filtering polices that prohibit access to any Web site that may be potentially troublesome (Johnson, 2012; Maycock, 2011; Pierce, 2012). Issues, such as lack of override privileges for designated school-based staff and highly restrictive filter configurations, are impeding instructional activities and compromising student safety (Willard, 2010b). Lastly, Willard states the override process in many districts consumes too much time and is a major frustration for end users.

Many factors motivate school districts to implement overly restrictive filtering policies. These factors include: fear of negative publicity or litigation, the notion that tighter filters keep students safer, adherence to parent and community sentiment, concerns that looser filter settings will encourage misuse of Internet resources, and bandwidth preservation (Baule, 2010; Fuchs, 2012; Losh & Jenkins, 2012). Additionally, proponents for less restrictive technology policies report that policymakers are implementing more stringent Internet access policies because of fears about Internet predators, cyber bullying, students posting inappropriate content on social networks, and the proliferation of sexually explicit or violent online content (Ahn et al., 2011; Bush & Hall, 2011; Rodgers, 2012).

Misinterpretation of CIPA's regulations may result in highly restrictive filtering policies. The U. S. Department of Education's (2010) NETP concludes that in some cases lack of understanding of CIPA's mandates creates "barriers to the rich learning experiences that Internet access should afford students" (p. 54). Willard (2010b) provides more insight into school districts' decisions to implement tight filtering controls. Willard states that over-blocking is often the result of misunderstanding CIPA's requirements or results when administrators rely solely on filters to prevent non-educational use.

Sometimes, filtering policies are configured according to the mistaken interpretation that CIPA requires schools to block all controversial content and prevent students from communicating with each other online—not strictly to block visual images that are obscene, contain child pornography, or are harmful to minors (Jansen, 2010; Johnson, 2012). However, blocking access to content other than adult sexual materials is at the school district's discretion as NCIPA stipulates. Sometimes filter overriding is prohibited because of misunderstanding CIPA's disabling provision. The confusion stems from the term "disabling," which means turning the filter off and is used in the CIPA law to prevent constitutional challenges; and the term "overriding," which means providing access to sites blocked erroneously. The disabling provision was the key reason the U.S. Supreme Court upheld the constitutionality of CIPA in *United States v. American Library Association*).

Additional Safety Policy Issues

CIPA requires school districts to develop and implement Internet safety policies, in addition to technology protection measures, to prevent the dangers of the Web from infiltrating the educational environment. AUPs generally address users' online rights and responsibilities, outline ramifications for policy violations, describe acceptable and unacceptable uses, and outline a code of ethical conduct for utilizing technology resources (CoSN, 2011; Hidalgo et al., 2009). More recently, the Protecting Children in the 21st Century Act (2008) added an Internet safety education component to the AUP, which was to be implemented no later July 2012. The literature suggests there are various safety policy issues that may be undermining students' online safety. These issues include over reliance on filtering technology and outdated AUPs.

Internet safety authorities maintain relying solely on filtering technology can undermine students' online safety and is counterproductive. Willard (2010a) observes that schools are placing too much emphasis on CIPA's filtering requirement as opposed to its Internet safety policy requirement. Over reliance on filtering technology has resulted in ineffective Internet safety education in schools. Content filtering can also generate a false sense security, causing educators to be less vigilant about monitoring students' online activities (Johnson, 2012; Nantais & Cockerline, 2010; Ott et al., 2010). Willard (2010b) notes that the false security notion leads to a failure to teach students how to respond to or prevent inadvertent access to inappropriate content. Adams (2010) argues that school districts are relying mostly on filters to protect children from Internet dangers, and concludes this approach does not teach students to be informed Internet searchers who know how to evaluate the accuracy of information or how to navigate the Internet safely and responsibly. Adams adds that filters only protect students when they are using the Internet in schools and libraries, not when they access the Internet in unfiltered locations or on wireless devices such as cell phones.

Internet use policies should be continuously reviewed and updated regularly to ensure they are relevant and address the latest technological advances (CoSN, 2011; Hidalgo et al., 2009). Nevertheless, Hidalgo et al. cite recent AUP research that indicated many institutions' AUPs were outdated, inconsistent, and did not address the ever-increasing range of Web-related applications including filtering circumventors (proxies and anonymizers), Web-based file sharing applications, instant messaging, and other Web protocols. Jansen (2010) examined 30 public school Internet safety policies in April, 2010, and found that only a few had been updated since October 2008 and even fewer

had updated their policies to include the Internet safety education component mandated by the 2008 Protecting Children in the 21st Century Act. Outdated AUPs cannot effectively address today's online safety challenges. The literature suggests AUPs, not filters, are the cornerstone of an effective online safety strategy. Successful AUP implementation mandates that the policy is comprehensive, updated frequently, developed collaboratively with all stakeholders, and focuses on safety awareness and education (CoSN; Endicott-Popovsky, 2009).

Internet Safety Policy Issues and 21st Century Teaching and Learning Standards

Outmoded filtering and Internet use policies—developed for Web 1.0 (static, read only Web content)—appear to be refueling the filtering debate (Quillen, 2010), which had mostly been dormant during the years immediately following the Supreme Court's 2003 decision upholding CIPA. The debate is not about whether or not to filter, but about issues surrounding the use of Web 1.0 filtering techniques to filter dynamic Web 2.0 traffic. Moreover, concerns have arisen regarding the use of outdated Internet access policies that do not effectively address Web 2.0 safety concerns (Bosco & Krueger, 2011; Lemke et al., 2009). The evolution of Web 2.0, also known as the "Read/Write Web," provides additional evidence, which implies that school districts may need to re-examine current filtering and safety policies in order to prepare students to live and work in the 21st century (Ahn et al., 2011).

The Promise and Perils of Web 2.0

Web 2.0 is a rapidly expanding and popular genre of Web applications having a marked influence on 21st century culture. Lemke et al. (2009) define Web 2.0 as "an online application that uses the World Wide Web . . . as a platform and allows for

participatory involvement, collaboration and interactions among users" (p. 5). Thousands of free Web 2.0 applications have recently become available. Some of the most used applications include:

- Social networking sites such as Facebook™ and Twitter™ where users create personal pages and interact;
- Blogs (Web logs), online diaries where the originator and readers comment on a variety of topics;
- Wikis such as Wikipedia, which are topical collections of information that users collectively create, add to, and edit;
- Social bookmarking sites such as Del.icio.us™ and Flickr™ where users share Internet bookmarks and create descriptive tags to organize resources such as videos and pictures; and
- Cloud computing applications such as Google Docs™, which are online suites of applications that allow users to import, share or collaboratively edit documents, spreadsheets, and presentations (Bush & Hall, 2011; Lemke et al.; Simkins & Schultz, 2010).

Just as with Web 1.0, technology enthusiasts and many educators are proclaiming the enormous promise of Web 2.0 technologies to transform 21st century teaching and learning. Simkins and Schultz (2010) state the hallmark of the read/write Web is its ability to foster interaction, collaboration, and group productivity. Bush and Hall (2011) purport the participative nature of these applications is shifting the focus from individualized work to collaborative efforts, from isolated learning to collective knowledge, and changing learners from passive recipients of knowledge to active

participants in the creation of knowledge. Web 2.0 has the potential to address the needs of different types of learners and to engage learners; make schoolwork more relevant for learners; enhance communication, collaboration, and critical thinking skills; expand learning beyond the classroom and the school day; and build a sense of community (CoSN, 2011). For many of the same reasons, these collaborative tools can also enhance professional development for educators (Bush & Hall).

There is widespread use of social, participative, and collaborative technologies in the larger society—for personal, business, entertainment, communication, educational, and political purposes. Despite a ubiquitous presence in the outside world and substantial educational potential, Web 2.0 use in schools is restricted (Ahn et al., 2011). These applications have fueled renewed Internet safety concerns and fears of misuse. Consequently, many school districts are setting filters to block access to social networking sites such as Twitter™ and Facebook™ (Ahn et al.; Lemke et al., 2009) to protect students from Web 2.0 perils. Some school districts are going beyond blocking social networking sites to block all Web 2.0 sites, including collaborative tools such as wikis, blogs, Flickr™, Google Docs™, and Del.icio.us™ (Bush & Hall, 2011; Johnson, 2012; Losh & Jenkins, 2012). Schools are denying or restricting access to participative online tools for several reasons including:

- Fear that predators may be lurking on social networking sites to target susceptible youth;
- Concerns that Web 2.0 resources use too much bandwidth;
- Concerns that these tools promote non-educational activities;
- Concerns that students will post inappropriate content online;

- Lack of awareness of the educational value of Web 2.0 technologies;
- The notion that social media is inundated with inappropriate content;
- Concerns that access to these tools will subject schools to litigation; and
- Concerns that students will be exposed to or engage in cyber bullying (Ahn et al.; Brooks-Young, 2010; Lemke et al.; Losh & Jenkins).

Loertscher (2009) defines three categories of technology access policies being implemented in school districts, each having a different effect on Web 2.0 and information access:

- Very restrictive filter settings, no access to cloud computing/Web 2.0 tools.
- Strong firewall allowing access to selected Web sites, multimedia resources, and Web 2.0 tools such as internal wikis, blogs, and internal communication tools.
- Light filtering (only what CIPA requires) allows access to any online tool that has educational potential. The focus is on teaching responsible technology use.

It is difficult to ascertain from the literature the extent to which the three technology access categories are being implemented in school districts, or the extent of Web 2.0 access issues, because few studies have investigated school districts' filter configuration tendencies.

Twenty-First Century Learning Standards

Web 2.0 filtering issues have implications for teaching and attainment of 21st century learning standards. Assessments of existing filtering technologies indicate these technologies are not adept at distinguishing education-specific Web 2.0 content from non-educational Web 2.0 content (Fuchs, 2012; OSTWG, 2010; Quillen, 2010). Therefore, filtering tools typically make a "block all Web 2.0 content" decision, or "allow

all such content" decision instead of allowing the good content and blocking the objectionable content. When the "block all Web 2.0 content" decision is made, access to information and resources necessary for attaining 21st century learning standards is limited (Jansen, 2010). Full integration of Web 2.0 applications into instruction provides a wealth of real-world learning opportunities that prepare students to live and work in an Internet-powered world (Manzo, 2009).

A major goal of the most recent International Society for Technology in Education (ISTE) and American Association of School Librarians (AASL) national standards is to prepare students to thrive in a global and digital world (AASL, 2007; ISTE, 2007). These standards enable students to acquire the Partnership for the 21st Century's (2011) five learning and thinking proficiencies: critical thinking and problem-solving skills, communication skills, collaboration skills, contextual learning skills, and information and media literacy skills. Access to the read/write Web fosters achievement of all these proficiencies, but the participative and collaborative nature of most Web 2.0 resources is particularly critical for attaining 21st century communication and collaboration skills (Jansen, 2010; Ott et al., 2010). Table 3 includes the AASL and ISTE standards that specifically address communication and collaboration skills. Technology integration specialists and educators assert that Internet access policies restricting access to Web 2.0 resources are counterproductive to attainment of these skills (Adams, 2010; Shearer, 2010).

Table 3. ISTE and AASL Collaboration and Communication-specific Learning Standards

International Society for Technology in Education Standards for Students	
Standard	**Communication and Collaboration** Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others. Students: **Performance Indicator a.** Interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media. **Performance Indicator c.** Develop cultural understanding and global awareness by engaging with learners of other cultures.
Standard	**Digital Citizenship** Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior. Students: **Performance Indicator a.** Advocate and practice safe, legal, and responsible use of information and technology. **Performance Indicator b.** Exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity.
American Association of School Librarians Standards for the 21st Century Learner	
Standard	Share knowledge and participate ethically and productively as members of our democratic society. **Skill 3.1.2** Participate and collaborate as members of a social and intellectual network of learners. **Responsibility 3.3.5** Contribute to the exchange of ideas within and beyond the learning community.
Standard	Pursue personal and aesthetic growth **Skill 4.1.7** Use social networks and information tools to gather and share information. **Responsibility 4.3.1** Participate in the social exchange of ideas, both electronically and in person. **Responsibility 4.3.4** Practice safe and ethical behaviors in personal electronic communication and interaction.

The Implications of Filtering and Safety Policy Implementation

CIPA has been fully implemented in K-12 schools for more than a decade, yet few studies have examined how CIPA compliant filtering and safety policies are influencing teaching and learning in institutions implementing these policies. The research literature in this domain is not definitive and is largely anecdotal according to Rodgers (2012). Nevertheless, anecdotal studies provide foundational data, which suggests restrictive technology use policies are hampering technology integration and limiting access to online resources that enhance learning (Finsness, 2008; Fuchs, 2012; Holzhauer, 2009). More definitive and comprehensive studies are required to advance understanding of how technology policies influence end users, and to inform policy development and decision-making. The current study endeavored to address these gaps in the literature. Previous filtering and safety policy related research is described and analyzed in this section to provide the context of the current study. Moreover, pertinent older research (2008-2009) is included to illustrate how the need for this study has evolved.

The Effectiveness of Internet Filters

From the inception of the filtering debate, researchers began to evaluate the effectiveness of Internet filters. Sutton (2012) states there has been an abundance of literature on the effectiveness of filters, including studies and opinion pieces, because of the legal debates emanating from legislative attempts to restrict minors' access to offensive online content. The results of early studies were often used to support the implementation of filters or as evidence that filters were not the best approach to protect minors from online indecency. These evaluations continue to be useful in the filter

selection process as an initial screening of vendors (Hidalgo et al., 2009). Filter effectiveness studies have led to improvements in filtering technology, but both public and private studies concur filters continue to under-block and over-block (Sutton).

Hidalgo et al. (2009) describe two approaches to evaluating the effectiveness of Web filtering tools—industrial evaluations and scientific evaluations. Industrial evaluations typically test several products to determine their strengths and weakness and are performed by a magazine or a third-party laboratory. The authors note several weaknesses of industrial tests including their subjectivity and lack of rigor. For example, performance evaluation is reported in unknown conditions (test set size and composition), testing conditions may favor a specific vendor, performance measures are not supported with statistical tests, and testing procedures are not transparent. Moreover, testing conditions do not mirror real-world scenarios.

Scientific filter evaluations, which are often reported in scientific journals, typically are set up in the context of well-defined experiments and are supported by rigorous procedures and metrics. The experiments are conducted under laboratory conditions, are reproducible, and the results can be compared to similar tests. Following CIPA's enactment in 2001, research studies began using more statistical approaches to determine filtering effectiveness, whereas filter effectiveness tests prior to 2001 tended to be less scientific and more anecdotal (Finsness, 2008).

Scientific filter testing is mostly limited to filtering accuracy (effectiveness)—the degree of over-blocking and under-blocking. Efficiency (processing speed), which is critical to real-world conditions, is rarely evaluated. The most salient deficiency of scientific evaluation is the absence of standard data sets, procedures, and metrics

(Hidalgo et al., 2009). Statistical measures can also be manipulated simply by changing the number of acceptable sites in a test set. It is also difficult to identify a truly random sample of Internet sites; such sites represent actual Web pages that users are likely to access. When statistical filter effectiveness studies report percentage summaries of correctly or incorrectly blocked content, it is often based upon subjective judgments about whether particular Web pages are appropriately blocked.

Despite the methodological issues with scientific filter tests, they persistently conclude filters both over-block and under-block content at consistent and equivalent rates, regardless of the filter or the filter's settings (Houghton-Jan, 2010). Houghton-Jan reports that for filter accuracy studies from 2001-2008, all tests combined yielded an average accuracy rating of 78%. When isolating the results from the 2007-2008 tests, the average accuracy rating increased to 83%, which suggests filtering technology may be improving. However, Houghton-Jan notes filters were still wrong 17% of the time and 54% of the time on image content.

Since 2008, scientific filter tests have substantially diminished (Houghton-Jan, 2010). An exhaustive literature review uncovered only two filter evaluation studies published after 2008, the results of which are similar to Houghton-Jan's conclusions and suggest filter effectiveness has not improved since 2008. Chou et al. (2010) empirically evaluated the performance of three top-ranked filters, CyberSitter™, Net Nanny™, and CyberPatrol™, to assess their performance against a proposed text mining filtering approach. The average overall accuracy rating for the three commercial filtering products was 68%, while an experimental content-based text mining approach achieved a 99% accuracy rating. It is interesting to note the filtering product (CyberPatrol™) employing a

combination of list-based and advanced content-based filtering techniques had an accuracy rate of just 47%, while the two list-based products (CyberSitter™ and NetNanny™) performed much better with accuracy rates of 78% and 66% respectively. The researchers concluded commercial filters were particularly inadequate compared to approaches employing classification algorithms. However, employing classification algorithms, such as text mining, is impractical for most school districts, as they require much more skill and resources than commercial filtering products.

Jeon et al. (2011) conducted a more recent filtering software evaluation of five commercial products, which yielded conclusions similar to Chou et al's (2010). Jeon et al.'s empirical evaluation yielded an average filtering accuracy of 70% when filtering harmful Web sites. The researchers also concluded that these products performed much worse (below 50%) when blocking video, image, and executable files such as those often found on social media and gaming Web sites.

The aforementioned studies indicate filtering technology continues to employ mostly list-based filtering techniques (i.e. URL blacklists, keyword blacklists) which result in considerable over-blocking and under-blocking. Jeon et al (2011) suggest that until machine learning techniques are employed, filtering products will continue under-performing, and increasingly so in the era of ubiquitous social media and mobile technologies. However, advanced filtering technologies that employ machine-learning algorithms are impractical for most schools because of cost and efficiency (speed) issues (Gossett & Shorter, 2011). Consequently, most school districts have implemented less accurate, but more efficient and economical list-based filtering products (AASL, 2012). Considering the inadequacies of technology protection measures, what remains largely

unknown is the effect these tools are having on end users in the K-12 environment. In addition, most filtering tools can be configured to limit over-blocking and under-blocking, but are school districts configuring them to maximize information access?

The Influence of Filtering and Safety Policies on End Users

Finsness (2008) reports that the widespread implementation of filtering technology has shifted the research focus from filter effectiveness to CIPA's actual effect on teaching and learning. Although, research into the influence of CIPA-inspired filtering and safety policies is beginning to emerge, Jaeger and Yan (2009) conclude "relatively small bodies of research have been generated about CIPA's effects in public libraries and public schools" (p. 6) and end users of these institutions. Nevertheless, a few notable studies have investigated issues surrounding Internet blocking technology implementation in public schools and libraries and how these issues affect users.

Holzhauer (2009) investigated the effects of filtering on classroom instruction in one small, rural school district. Teachers, administrators, and technology personnel of two elementary schools, one high school, and one alternative school participated in the study. Using quantitative methodology, the researcher surveyed technology personnel to determine the degree of filtering restrictiveness at the local level and surveyed administrators and teachers to determine if filtering affected classroom Internet usage. The study concluded that the district's filtering policies limited access to Web-based resources required for instruction and contributed to teacher reluctance to integrate computers into instruction. Another significant finding of the study was the apparent lack of communication and stakeholder involvement in the development and implementation of the district's filtering policy. These factors contributed to teacher frustration and

reluctance to integrate technology fully into instruction, but administrators and technology personnel were mostly satisfied with the effectiveness of the filtering policy. This study was also limited in scope as it involved only one school district. A number of filtering policy issues was identified, but what remains unknown is the pervasiveness of these issues in other school districts. The researcher pointed out that the data and research results were relevant specifically for the school district involved in the study, and was not applicable to the larger population. Holzhauer recommended that similar studies be conducted in other school districts for comparative purposes.

Finsness (2008) examined whether content filters prevented high school students from accessing information required for Minnesota's Academic Standards. Finsness also explored how teachers and technology administrators reacted when students were denied access to information required to meet learning standards. This dissertation study was largely qualitative, including in-depth interviews with six district technology administrators and nine high school health and social studies teachers from 9 of Minnesota's 339 independent school districts. The study concluded that the level of filtering (from less restrictive to more restrictive) affected students' ability to access information needed to meet Minnesota's health and social studies standards. The study also concluded that additional research was required to inform CIPA-compliant policy and practice. As with Holzhauer's (2009) research, Finsness' study was limited in scope, involving representatives from only nine school districts. In addressing the study's limitations the researcher states, "The data were anecdotal data collected from a small population" (p.154). Finsness also noted that the results of the study could provide

baseline data for subsequent investigations into the implications of public school Internet filtering.

Fuchs (2012) conducted a critical ethnographic investigation of how filtering the Internet was affecting public education in North Carolina. Through the collective voices of 50 participating IT directors, administrators, and teachers, Fuchs concluded that misapplied local policies and insufficient staff development for using filtered Internet instruction contributed to restricted access to online educational content. The results of this qualitative investigation were similar to the aforementioned studies and add supporting evidence that filtering and safety policies are adversely influencing teaching and learning. However, generalizability of the results is limited because of inherent weaknesses of qualitative methodology.

A few studies have focused on SLMS's views of how filtering and safety polices are affecting teaching and learning. Harris' (2009b) research analyzed SLMS' postings to LM_NET, AASL's (American Association of School Librarians) online discussion group, to determine SLMS' perceptions of online information literacy instructional challenges. The study revealed that Internet use policies and procedures presented a major challenge to teaching students how to search, select, and assess the meaning and value of information found online. SLMS' LM_NET postings reflect frustrations regarding filtering policy implementation and procedures that limited access to online content. They described cumbersome unblocking procedures, blocking entire categories of tools (i.e., wikis and blogs), and certain domains of Web sites (Geocities and Wikipedia). Postings also revealed that in many cases filtering configurations were not fine-tuned so that distinctions were made between education-related Web 2.0 applications

and non-education-related applications. Problems of limited access were exacerbated by SLMS not being granted filter override privileges to provide timely access to erroneously blocked content and poorly maintained filtering and security systems. The major limitation of this study was that it reflected only the views of SLMS who posted messages, not the feelings of lurkers or non-members of the discussion group. Therefore, the findings cannot be generalized to the larger population of SLMS. In addition, Harris noted that the coding process used to analyze the data was subjective, which further limited the applicability of the results to other settings.

More recently, AASL (2012) collected data on filtering in schools as part of its annual *School Libraries Count* longitudinal survey. This survey, which involved 4,299 SLMS, was the most comprehensive filtering/safety policy research to date, relative to the number of participants and the range of filtering/safety policy issues addressed. The study addressed the types of filters, online safety approaches, educational content most often blocked, timeliness of unblocking procedures, differentiated filtering for various user groups, and the impact of filtering on learning. Major conclusions of this study according to Devaney (2013) were that Web filtering impedes learning and prevents students from taking advantage of learning's social potential. More than half (52%) of respondents indicated internet filters impeded student research, particularly keyword searches. Even though most respondents reported filtering decreased distractions and the need for direct supervision, AASL concluded, "filtering continues to be an important issue for most schools" (Title page, para. 2) because many schools are filtering beyond CIPA requirements, thereby impeding learning. This study was comprehensive in many respects; however, it was limited in that only quantitative data were collected and did not

investigate filtering policy decision making from the perspective of technology administrators.

The aforementioned studies mostly focused on the effect of CIPA's filtering strategy on information access and end users, but CIPA employs two strategies to protect minors while online. Few studies have focused on the effect of CIPA's safety awareness strategy. Yan's (2010) quasi-experimental research compared high school students' Internet access in a filtered environment to undergraduate students' access in an unfiltered environment to investigate differences in basic knowledge and perceived cognizance of Internet safety protection strategies. The study also investigated CIPA's influence on students' Internet use at home and school. Yan states Internet safety awareness and sufficient Internet safety educational experiences are fundamental for protecting students from harmful online content and encounters. However, the study found that CIPA's Internet safety strategies did not have a beneficial impact on students' basic knowledge of Internet safety. CIPA has reduced students' Internet use at school, but not outside; thereby reducing exposure to potentially harmful Internet content at school. Nevertheless, CIPA does not positively influence students' online behaviors outside of school. The results suggests that CIPA's filtering and safety strategies, which are only enforced in schools and libraries, are not effective as these venues are not the only places students can be exposed to harmful online materials. Yan's study was also limited in scope in that it involved students from only one high school and focused only on CIPA's Internet safety awareness approach.

A national survey of over 1600 educators also suggests that schools may not be fully implementing CIPA's safety awareness strategy as part of their Internet safety

policies (National Cyber Security Alliance (NCSA), Educational Technology Policy Research and Outreach, Microsoft Corporation, & Zogby International, 2010). The NCSA et al. study revealed no concerted effort exists among educators or administrators to teach safe and secure digital navigation and prepare students to be responsible digital citizens and employees. Instead, the survey showed more than 90 percent of schools relying mostly on filtering and blocking social-networking Web sites to protect students from potentially harmful online materials (Pierce, 2010). This study used valid sampling techniques to choose a broad spectrum of participants, but the survey focused mostly on one aspect of CIPA—cyber safety awareness and education. A comprehensive investigation of other issues surrounding school districts' filtering and safety policy development and implementation was not conducted.

Social Media (Web 2.0) Access Policies

Research is beginning to emerge that provides an indication of how Internet access policies may be influencing access to Web 2.0 resources in schools. To establish a baseline for Web 2.0 policies, practices and perspectives in American K-12 schools, Lemke et al. (2009) conducted a national study involving superintendents, curriculum directors, and technology directors. The study reported that Web 2.0 use is mostly guided by pre-Web 2.0 policies that include AUP's, Web filtering, and informal practices. Policies that specifically address Web 2.0 use are limited, typically are restrictive, and are more reactive than proactive. The majority of the survey respondents agreed that Web 2.0 resources can positively influence teaching and learning, but acknowledged concerns about balancing Web 2.0's educational potential with safety issues.

TICAL (Technology Information Center for Administrative Leadership) conducted an informal survey of educators including principals, district administrators, technology directors, curriculum specialists, SLMS, and classroom teachers to get their perspective on the promise of Web 2.0 tools, obstacles to their use in teaching and learning, and overcoming these barriers. Almost 90% believed Web 2.0 resources had the potential to enhance instruction and increase student engagement. However, nearly half of these respondents said district filtering and Internet safety policies were a major barrier to realizing the educational potential of this technology (Simkins & Schultz, 2010).

More recent studies continue to show there is a stark difference in the use of technology in and out of school, particularly social media technologies. Ahn et al. (2011) analyzed 217 district AUPs to determine how they framed social media access in schools. A major finding was that the majority of AUPs made no mention of social media technologies and 14% of districts banned social media entirely. The researchers concluded that while some AUPs implied social media tools might be useful educational resources, just a few clearly stated that social media had potential educational value. A major recommendation of the study was that additional studies of this nature would forward understanding of how technology policies influence educator practices.

Contribution to the Literature

This study addressed the limitations of the aforementioned studies. These studies were limited because they were either anecdotal or did not use a combination of data collection methods to comprehensively investigate the filtering and safety policy issues identified in the literature. This research enlisted a large number of participants from thirty-six school districts and used multiple data collection methods. Investigating the

research problem on a broader scale enabled a more comprehensive investigation of the major safety policy issues and how they influence information access and 21st century instruction.

This research also addressed existing gaps in the literature about districts' filtering and safety policy predilections. What remained to be determined was the actual level of filtering restrictiveness schools districts were implementing, what specific categories were being blocked, what circumstances prompt filtering category blocking decisions, and how these decisions affect access to information and resources required for 21st century teaching and learning. This study sought to address these unanswered questions, which are essential for district policymakers and stakeholders seeking to revise Internet use policies or evaluate the effectiveness of existing policies.

Filtering and safety policy related literature is largely opinion-based or prescriptive (Sutton, 2012) and lacks a solid research base (Rodgers, 2012), which is an essential element of informed policy making. Researchers have acknowledged the difficulty of designing research studies that determine the effect filters have on information access. This investigation was cumulative in that it added to existing research about the influence of Internet filtering on student learning. It also provides descriptive data about the types of information and resources filters block, and reveals the outcome of filtering policy decisions on attainment of specific 21st century learning standards.

Chapter Summary

This literature review established a conceptual framework for the study of filtering and safety policies, surveyed issues surrounding filtering and safety policy implementation in public K-12 schools, and the manner in which these issues converge to

influence 21st century teaching and learning. An analysis of relevant research was conducted to establish the basis and need for this research.

Chapter 3

Methodology

Introduction

This chapter restates the research problem and reiterates the purpose of this study. It provides an overview of the research design and the rationale for employing the research methodology. This section also describes the data collection instruments, defines the data collection procedures, outlines the measures used to ensure that the research design and instruments yield valid and reliable data, and describes the participants and sample selection procedures. Finally, the data analysis and presentation methods are briefly explained along with a description of the resources used for this investigation.

Restatement of the Problem

School districts have implemented filtering and safety policies in response to legislative and social mandates to protect students from the proliferation of objectionable Internet content. The literature suggests these policies are more restrictive than legal mandates require and are adversely affecting information access and instruction. There is no clear understanding of the manner in which filtering and safety policies are affecting teaching and learning because no comprehensive studies have investigated the issues and trends surrounding filtering and safety policy implementation or the implications of these issues for end users. Policymakers need this type of research-based data as they evaluate

and revise Internet use policies in order to enhance instruction and provide greater access to the most recent online learning technologies.

Purpose of the Study

The goal of this research was to examine Internet filtering and safety policy implementation in South Carolina's K-12 public schools to determine current trends and issues and the way these policies influence information access and instruction. The study investigated the following research questions:

- How are filtering and safety policies being implemented in public schools?
- What issues do SLMS encounter as they facilitate information access on filtered computers?
- How are school districts addressing Web 2.0 safety issues
- In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?

Research Method

To accomplish the research goal, the researcher utilized a mixed methods research design including both quantitative and qualitative approaches. Ivankova et al., (2006) suggest neither quantitative nor qualitative approaches by themselves are adequate to "capture the trends and details of a situation" (p. 3). Therefore, a mixed methods strategy was implemented; quantitative data from mostly closed ended surveys was collected and analyzed. Data analysis from the quantitative phase informed the second phase of the study, which entailed the collection and analysis of qualitative data. Creswell and Plano Clark (2007) state when researchers utilize this approach, they typically use qualitative data to develop a better understanding of the data collected during the quantitative phase

of the study. Moreover, Teddlie and Tashakkori (2009) contend a multi-method research design is superior to single methods because it enables data triangulation, the use of a variety of data sources in a study. The study utilized data collected from multiple surveys, interviews, and analyses of artifacts (AUPs). Triangulation also enabled this investigation to overcome weaknesses or inherent biases of single method studies and provides a deeper understanding of the research problem. Creswell (2009) suggests that combining qualitative and quantitative approaches provide a more accurate portrayal by revealing trends and generalizations and provide an expanded understanding of the research problem.

This investigation was primarily descriptive in nature. Gay, Mills, and Airasian (2011) state quantitative descriptive or survey research is undertaken to answer questions regarding the current status of the research topic or to gather information about preferences, practices, or concerns of a target group. Accordingly, the initial quantitative phase of this study provides an overview of the filtering and safety policy implementation trends and issues in South Carolina's public schools. Teddlie and Tashakkori (2009) explain that "quantitative questionnaires can be used to generate large numbers of responses that produce information across a broad range of survey topics" (p. 240). However, it was not possible to address the research questions sufficiently via quantitative data only. It was therefore imperative to include a qualitative phase to answer the research questions more conclusively.

Instrument Development and Alignment to Research Questions

Prior to developing the online surveys for this study, the researcher was cognizant that online surveys are not as advantageous as once believed and typically have a lower

response rate than paper-based surveys (Lefever, Dal, & Mattiasdottir, 2007). On the other hand, they provide the timeliest and most cost efficient data collection method. Web-based surveys are also practical for well-defined population groups whose e-mail addresses can be obtained easily (Rea & Parker, 2005). Because the intended population was homogeneous with respect to a key variable, profession, lower response rate was less of an issue for this study. Lefever et al. also state online surveys provide an effective way to access large and geographically distributed populations and are particularly useful for collecting preliminary data. This study utilized survey data to obtain an overview of the issues and trends relative to filtered Internet access and follow-up interviews were utilized to gain a deeper understanding of these issues. Consequently, the inherent disadvantages of Web-based surveys were mitigated.

Two surveys, an IT administrators' survey and a SLMS' survey (see Appendix B and Appendix C), were designed to achieve the research goal and answer the research questions. The surveys were grounded in the research literature and gathered descriptive data that enabled a deeper understanding of South Carolina public schools' filtering and safety policy issues. Survey items focused on the following filtering and safety policy issues as identified in the literature: content category blocking decisions and the rationale for those decisions (Jansen, 2010; Johnson, 2012; Manzo, 2009; Willard, 2010b), the implications of over-blocking and under-blocking (Jansen; Maycock, 2011; Willard, 2010b), the efficiency of unblocking procedures (AASL, 2012; Harris, 2009b; Quillen, 2010; Willard, 2010b), the effect of filtering policies on Web 2.0 access (Adams, 2010; Losh & Jenkins, 2012; Manzo, 2009; Quillen, 2010), stakeholder involvement in filtering/safety policy decisions (Baule, 2010; Johnson), distinct filtering policies for

different user groups (AASL, 2012; Hua, 2011), and the role of Internet safety education programs in overall student online safety (Adams, 2010; Willard, 2010a). It is important to show how the research variables relate to the research questions and specific survey items (Creswell, 2009). Table 4 provides a visual representation of the relationship between the filtering and safety policy issues (variables) identified in the literature, the research questions, and response items on the data collection instruments.

Table 4. Filtering/safety policy issues, research questions, and survey items

Filtering/Safety Policy Issue (Variables)	Research Question	Survey Item
Content blocking considerations	Research Question 1: How are filtering and safety policies being implemented in public schools?	IT Survey questions 4, 6,7a, 7b: blocked content categories, rationale for blocking decisions, use of default filter settings, sub-category blocking
Stakeholder involvement in policy decisions	Research Question 1: How are filtering and safety policies being implemented in public schools?	IT survey question 5: who makes blocking decisions SLMS survey questions 2,7a: who makes blocking decisions, stakeholder input
Differentiated access levels for specific groups	Research Question 1: How are filtering and safety policies being implemented in public schools?	IT survey question 7e: differentiated access SLMS survey question 7d: differentiated access
Over-blocking and under-blocking	Research Question 2: What issues do SLMS encounter as they facilitate information access on filtered computers?	IT survey question 9, 10: over-blocking and under-blocking frequency, blocking effectiveness SLMS survey questions 3, 5, 6, 8a,8b, 8c: blocked educational content, over-blocking and under-blocking frequency, blocking effectiveness, over-blocking effect on instructional staff, over-blocking effect on students, under-blocking effect on students
Unblocking procedures	Research Question 2:	SLMS survey questions 4,7b,7c,

Table 4 (continued)

Filtering/Safety Policy Issue (Variables)	Research Question	Survey Item
	What issues do SLMS encounter as they facilitate information access on filtered computers?	8d: timeliness of unblocking process, filter override privileges, blocked page notification, unblocking efficiency IT survey question 7c,7d, 7f,: capability of overriding filter, blocked page notification, filter override privileges
Internet safety education	Research Question 3: How are school districts addressing Web 2.0 safety issues?	IT survey question 8: programs addressing cyber bullying and social networking safety education SLMS survey question 7e, 8f: programs addressing cyber bullying and social networking safety issues, effectiveness of safety policies/practices
Web 2.0 accessibility	Research Question 4: In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?	SLMS survey questions 4, 8e: over-blocking of Web 2.0 resources, access to collaboration and communication tools

The IT administrators' survey was developed to gather descriptive data from IT administrators and mostly addressed the first research question. The first research question sought to determine how filtering and safety policies were being implemented in South Carolina's public schools. The IT survey consisted primarily of closed-ended response items that could be easily analyzed, were less time-consuming for the participant, and encouraged a higher response rate (Williams & Protheroe, 2008). A comment section was included for most questions so that respondents could explain responses or provide additional information. The IT survey sought to collect data about

the types of content filters used in school districts, content categories that were blocked, the rationale for blocking these categories, whether blocked categories are fine-tuned to minimize over-blocking, Web filtering rules and how they were established, procedures for unblocking legitimate content, and whether specific filter settings were established for different user groups.

An SLMS survey consisting primarily of closed-ended response items was developed to collect data about filtering/safety policy procedures/practices, and the challenges end users encountered as a result of filtering/safety policy implementation. The SLMS survey instrument focused mostly on the second research question regarding the issues SLMS experience as they facilitate information access on filtered computers. Most questions included a comment section so that respondents could explain responses or provide additional information. The survey response items were based upon the research literature and were designed to provide a better understanding of how content filtering policies affect end users. Survey items focused on the effectiveness of content filters, filtering/safety policy procedures and practices, instances when over-blocking and under-blocking occurred, the nature of the information that was blocked, and the extent to which filtering policies impeded access to constitutionally protected information.

The third research question sought to determine how school districts were addressing Web 2.0 safety issues. To answer this question, the researcher examined safety policies from 99% of the traditional school districts (excludes charter schools and career centers). These policies, also known as Acceptable Use Policies, were examined using an instrument designed to assess whether they had been updated to reflect the FCC's most recent mandate and referenced Web 2.0 safety issues. This mandate requires

all E-rate discount recipients to amend their AUPs to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms, and cyber bullying awareness and response (Federal Communications Commission, 2011). This AUP amendment was to be implemented by July 1, 2012. Additionally, the SLMS' survey instrument and IT administrators' survey instrument included social networking and safety education related response items and the SLMS' interview protocol included response items that investigated whether social networking safety issues were addressed via Internet safety education programs. This data was analyzed to determine how school districts were using Internet safety instruction to educate students about Web 2.0 safety concerns.

The fourth research question sought to determine how filtering policies impede access to information and resources required to achieve communication and collaboration related national technology and information literacy standards. The researcher identified specific technology and information literacy standards that require online communication and collaboration to address this question (see Table 3). Online communication and collaboration necessitates access to Web 2.0 social technologies such as blogs, wikis, podcasting, forums, and multimedia sharing for collaborative school projects. However, proponents of less restrictive filtering polices suggest that many school districts are configuring filters to block access to these online tools (Shearer, 2010; Losh & Jenkins, 2012). To determine how filtering policies are affecting the use of Web 2.0 collaborative tools, the researcher reviewed school districts' blocked content categories to determine if Web 2.0 resources such as wikis, blogs, and social networks were blocked. The SLMS' survey and interview responses were analyzed to determine if users were unable to access

online communication and collaboration resources. SLMS were surveyed regarding unblocking procedures and whether they provided timely access at the point of need when Web 2.0 resources were blocked.

Qualitative data was collected during the second phase of the study. Qualitative research is undertaken to deepen understandings about the way things are, why they are that way, and how participants view them (Gay et al., 2011). Gay et al. also state interviews are advantageous for qualitative data collection because they enable the researcher to probe and explain phenomenon, are flexible to use, and can be recorded for subsequent analysis. Teddlie and Tashakkori (2009) add that when interviews and questionnaires (surveys) are used together in a study, they generate complex mixed data. Quantitative survey data added breadth to the study and qualitative data allows depth of understanding.

The interview protocol mirrored the survey in that it addressed each research question and the issues identified in the literature (see Appendix E). The interview protocol consisted of five question sets that addressed the following themes and respective research questions (RQ): stakeholder involvement in policy decisions (RQ1), unblocking/blocking procedures and practices (RQ1, RQ2), influence of over-blocking and under-blocking on teaching/learning (RQ2), Internet safety education programs (RQ3), and Web 2.0 safety and access issues (RQ3, RQ4). SLMS were asked to share their perceptions of stakeholder involvement in Internet policy decisions, unblocking/blocking procedures and practices, the influence of over-blocking and under-blocking on teaching/learning, the effectiveness of Internet safety education programs, and Web 2.0 safety and access issues. Qualitative data collected via the interview

protocol added depth to the study by providing the personal experiences and impressions of participants concerning filtering and safety policy implementation.

Validity and Reliability

Validity

There were various threats to the validity of the study and the researcher took steps to minimize these threats. Validity refers to the extent to which an instrument measures what it is supposed to measure (Gay et al, 2011). A valid instrument has content validity. That is, it fairly and comprehensively covers the domain or issues that it purports to cover (Cohen, Manion, and Morrison, 2011). When designing the survey instruments, the researcher ensured that the response items aligned with the research questions. The researcher also ensured that the questionnaires were grounded in the literature. That is, the questionnaires addressed the issues of concern enumerated in the filtering and safety policy literature. Table 4 presents a visual display of significant filtering and safety issues identified in the literature, identifies survey items that address these issues, and aligns survey items to the research questions.

To increase validity, a panel of experts with extensive subject related background reviewed the data collection instruments. The panel included two college professors, a university library dean, and two IT administrators (see Appendix A), all of whom have published articles or research relating to the research topic. Each panelist independently rated each data collection item for relevance to the research questions, using a four-point Likert scale: not relevant, slightly relevant, quite relevant, and very relevant. The numerical values ranged from 4 for very relevant to 1 for not relevant. The mean score for each item ranged from a high of 4.0 to a low of 3.2 (see Appendix A). Since the

average rating for each item was above 3.0, no item was deleted from the instruments. The expert evaluation instrument also included a space for reviewers to suggest changes for each item. Appendix A outlines how each data collection item was changed in response to expert reviewers' recommendations.

Creswell (2009) states pilot testing is important to establish an instrument's content validity and to improve questions, format, and the scales. Similarly, Cohen et al (2011) conclude that pilot testing increases an instrument's reliability, validity, and practicability. Cohen et al suggest that pilot testing should:

- Assess whether survey items and instructions are clear;
- Provide feedback on the validity of the response items (Do they measure what they are supposed to?);
- Identify redundant items;
- Provide feedback on response item format;
- Assess whether the survey's length is appropriate; and
- Provide feedback on the layout, sectionalizing, numbering, and itemization of the instruments.

Accordingly, the data collection instruments were pilot tested with a subset of the population of SLMS and IT administrators. Fourteen SLMS and IT administrators were invited to pilot test the surveys and eight participated in the pilot test. Pilot test participants were asked to indicate problems encountered while taking the surveys and submit suggestions for survey improvement on the final survey screen. Participants did not recommend any changes or encounter problems during the pilot test. Therefore, the survey was launched with the changes the expert panel recommended. Survey pretesting

ensured that the data collection instruments consistently collected the data required to answer the research questions.

Nonresponse was also an important threat to external validity or generalizability of research, particularly if non-respondents results are systematically different from the respondents' results (Teddlie & Tashakkori, 2009). To minimize the threat to external validity and to maximize the survey response rate, researchers must employ an extensive follow-up method that consists of reminders and resending surveys to non-respondents. Ye (2007) and Cohen et al. (2011) suggest a variety of strategies to increase response rates. These strategies include electronic pre-notices, follow-up reminders with the survey links, follow-up telephone calls, stressing the importance and benefits to the target group, employing a simple and technically uncomplicated survey design, and ensuring that respondents' privacy was protected. The researcher utilized these strategies to maximize the survey response rate and increase the external validity of the research conclusions.

Triangulation entails the use of two or more methods of data collection and "is a powerful way of demonstrating concurrent validity" (Cohen et al, 2011, p.112). When different methods of data collection yield similar results, concurrent validity is established. Collecting and analyzing both quantitative and qualitative data enabled the researcher to explain more completely the richness and complexity of the issues of focus. To enhance data triangulation, the IT and SLMS surveys included identical items on stakeholder involvement in content filtering decisions, filter effectiveness, on-campus override privileges, blocked page notifications, different access levels for specific user groups, and safety education programs that educate users about Web 2.0 safety issues.

Reliability

Reliability refers to the consistency with which an instrument measures whatever it is intended to measure (Gay et al., 2011). Developing instruments with good questions ensures a consistent data collection experience for all respondents according to Fowler (2009). Fowler explains that good questions, "mean the same thing to every respondent" (p. 89), and "the kinds of answers that constitute an appropriate response to the question are communicated consistently to all respondents" (p. 89). To design reliable survey response items, the researcher was careful to employ the following survey design recommendations:

- Avoid inadequate wording;
- Avoid terms or concepts that have multiple meanings;
- Avoid asking two questions at once;
- Keep response items clear and simple; and
- Whenever possible, use closed ended questions that provide a list of acceptable responses (Fowler).

Population and Sample

The target population included IT administrators and SLMS. IT administrators were included because they are largely responsible for the selection, configuration, and ongoing administration of content filtering programs. This factor allowed them to provide important data about Internet filtering and safety policies and practices. Moreover, SLMS have an advantageous perspective from which to provide a deeper understanding of the issues and trends surrounding filtering technology implementation and its impact on end

users. SLMS facilitate user information access and are keenly aware of the information access issues end users encounter while using filtered computers.

The population of IT administrators and SLMS were well-defined; in most cases, their e-mail addresses were readily accessible, and they had Internet access to facilitate completion of the Web-based surveys. The researcher acquired SLMS' email addresses from the South Carolina Association of School Librarians (SCASL) online listserv, school Web sites or via telephone contact. Email addresses for IT directors were obtained from school districts' Web sites or via telephone contact. Prior to contacting the target population, the researcher requested school district authorization to conduct research with the target population groups (see Appendix G).

Thirty-six of 81 traditional South Carolina school districts agreed to participate in the study. After obtaining research authorization and IRB approval (see Appendix H), the target population was invited to participate in the study via email (see Appendix I and Appendix J). The email invitation included a link to the surveys, which were hosted on the SurveyGizmo™ Web site.

Data Collection Procedures and Time Frame

The time frame for collection of data from four sources—IT survey, SLMS survey, SLMS interviews, and analysis of AUPs—was approximately four months. The SLMS survey was launched at the end of May 2012 and remained open until the end of June 2012 while the IT survey was launched in mid-June and remained open until the end of July 2012. To improve the response rate, the surveys remained open for several weeks as much of the data collection period coincided with summer break, when the target population is mostly away from school and may not check school email on a daily basis.

Interviews were conducted with a subset of the SLMS population over a two-week period in mid-August 2012. The analysis of AUPs was performed from mid-July 2012 until mid-September 2012.

SurveyGizmo™, an online survey tool that allows users to develop, customize, and distribute Web-based surveys, was used to conduct the surveys. This survey tool allowed participants' responses to be recorded electronically, and summary data was available immediately. The researcher selected SurveyGizmo™ to create, disseminate, and collect the survey because of its reputation, ease of use, and flexibility (Marie & Weston, 2009). Moreover, SurveyGizmo's™ surveys are low cost and flexible. The survey tool allows collected data to be downloaded in a variety of formats, including Excel spreadsheet format for data analysis.

Eighty-one traditional South Carolina school districts were contacted to obtain permission for the target population to participate in the study. School districts were sent a letter explaining the proposed research (see Appendix G) and a copy of each survey (see Appendix B and Appendix C). Thirty-six school districts granted permission for their SLMS and IT directors to be contacted and invited to respond to the surveys. This factor made it impossible to draw a random sample of the entire population of South Carolina SLMS and IT directors. The 36 participating school districts consisted of approximately 463 SLMS and 36 IT directors (or their designees). In an effort to increase the number of respondents, the researcher's goal was to email the survey to the entire population of SLMS and IT directors, excluding pilot test participants.

The researcher collected the email addresses of 428 SLMS from the SCASL listserv, telephone contacts, and individual school Web sites. The SLMS survey

instrument was then launched using SurveyGizmo™. An email message containing consent information and a link to the online survey was successfully delivered to 398 media specialists. The survey link allowed recipients to respond anonymously to the survey. One hundred twenty-three SLMS responded to the survey for a 32% response rate. Email addresses for 36 IT administrators were obtained from school districts' Web sites and telephone contact. One IT director participated in the pilot test, therefore the survey invitation was sent to 35 IT directors. Twenty-one IT administrators responded to the anonymous IT survey for a 60% response rate. To increase the response rate, two reminders were sent to both groups while the surveys were open.

During the subsequent qualitative phase, the researcher conducted interviews with a subgroup of SLMS to gain a more in-depth understanding of SLMS' convictions and concerns about the impact of filtering and safety policies upon end users. The last page of the survey included a note stating the researcher was seeking four-to-five respondents to participate in a brief follow-up interview. To preserve the anonymity of the survey responses, respondents were asked to contact the researcher via email or telephone if they were willing to be interviewed. Six respondents indicated they wanted to be interviewed; ultimately, five respondents participated in the interviews. The interviews were conducted after the IT and SLMS surveys were closed and preliminary data analyses were completed. The researcher reviewed the interview protocol based upon the preliminary data analyses to determine if the protocol needed modifications. No modifications were necessary in order for the protocol to collect qualitative data that added depth to the quantitative data. Prior to conducting the interviews, the researcher mailed a hard copy of the informed consent document to each interviewee for signature.

After the signed consent form was returned, the researcher contacted the prospective interviewees to review the consent form and to schedule the interview. The consent form outlines interviewee rights and steps the investigator took to ensure the interviewee's confidentiality (see Appendix K). Interviews were conducted over a two-week period in August 2012. The investigator took copious notes during each interview session. Interview data were thematically analyzed for presentation.

An analysis of AUPs from 80 of 81 traditional school districts was conducted over a two-month period from mid-July 2012 to mid-September 2012. The researcher used the protocol for analyses of artifacts (see Appendix D) to assess how school districts were updating their Internet safety policies in response to Web 2.0 safety issues and recent legislative mandates to educate minors about Internet safety, particularly Web 2.0 safety. The researcher located school districts' AUPs on their Web sites in most cases. If a school district's online AUP was outdated or was not on the district Web site, the researcher contacted the district to request a copy. The data was quantified for presentation to show how schools have updated their AUPs to address Web 2.0 safety concerns.

Data Analysis and Presentation

This research sought to gain a deeper understanding of filtering and safety policy implementation in public K-12 schools. Data collected during the survey phase were analyzed using descriptive statistical methods, which provided an understanding of the nature of Internet safety policy implementation issues and their relationships. According to Teddlie and Tashakkori (2009), descriptive statistical methods include techniques for summarizing numeric data with tables, graphs, or single representations of a group of

scores in order to understand the data, detect trends and patterns, discover relationships between variables, and better communicate the results. The most appropriate data analysis methods for this study include frequency tables and graphic displays. Graphic displays and frequency tables coupled with accompanying summaries paint a realistic picture of safety policy implementation issues and their relationships.

Follow-up qualitative interviews were conducted with a small number of SLMS. Data collected from interviews, which took place during the second phase, were thematically analyzed to provide a deeper understanding of filtering and safety policy issues and how they influence information access and instruction. This phase of the study revealed the manner in which policy issues influenced user access to Internet resources. Teddlie and Tashakkori (2009) state most qualitative analytic techniques involve generating emergent themes that evolve from the study of specific pieces of information that the investigator has collected. Interview notes were transcribed and color-coded to identify common themes and categories. Open-ended survey comment items were also thematically analyzed and combined with interview data. Thematic development facilitates comparisons among variables, thus leading to a better understanding of the research questions (Teddlie & Tashakkori).

School districts' AUPs were also analyzed to determine if they had been updated to address Web 2.0 safety concerns. Wording in the AUP was also examined for references to Internet safety education and whether they addressed cyber bullying awareness and response, chat room interactions, and social networking interactions. This data was quantified for presentation in table format.

Resources

Professional experience and expertise coupled with external resources contributed to this study. The investigator was a SLMS for 30 years and has experience facilitating access to information at all K-12 public school academic levels. Some of the investigator's professional experience was in a filtered environment. This experience provided personal knowledge of some access issues that users encounter while accessing information in a filtered environment.

The Nova Southeastern University Library was the principal source of online and print resources relevant to the study. SCASL's Listserv, individual school Web sites, and school district Web sites provided most of the email addresses of the target population. The target population of IT administrators and SLMS coupled with school districts' AUPs were sources of data for the study. SurveyGizmo™, a Web-based survey development and hosting utility, allowed direct input of survey participants' responses, while maintaining their anonymity. SurveyGizmo™ and Excel Data Analysis ToolPak were used for data analysis and presentation of the research results.

Summary

In order to describe filtering/safety policy implementation and its influence on teaching and learning accurately, a mixed methods design was utilized. Quantitative methodology during the first phase included two surveys, one for SLMS and one for IT administrators. Additional data collection during the qualitative phase involved interviews with a small number of SLMS and an analysis of artifacts (AUPs). Expert review, pilot testing, and member checking was used to establish the validity and reliability of the data. The data were used to describe the manner in which filtering and

safety policies were being implemented, the issues users encountered as a result of filtering and safety policy implementation, measures used to address Web 2.0 safety issues, and the manner in which filtering and safety policies prevented access to resources necessary to attain 21st century communication and collaboration standards.

Chapter 4

Results

Introduction

This study was undertaken to investigate filtering and safety policy implementation in South Carolina's public K-12 schools and its influence on teaching and learning. The study utilized a mixed methodology, in which both quantitative and qualitative data were collected to answer the following research questions:

- How are filtering and safety policies being implemented in public schools?
- What issues do SLMS encounter as they facilitate information access on filtered computers?
- How are school districts addressing Web 2.0 safety issues?
- In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?

Quantitative data using an anonymous online survey questionnaire were gathered from SLMS and IT directors (or their designees) to gain a general understanding of filtering and safety policy implementation and how it influences information access. Subsequent one-on-one telephone interviews with five SLMS provided a deeper understanding of Internet safety practices and how these practices either impede or enhance information access. AUPs were also examined to determine whether districts were educating minors about Web 2.0 safety issues. The data collection instruments

contributed to a comprehensive depiction of filtering and safety policy implementation. This portrayal is presented from the perspective of stakeholders (IT administrators) with first-hand knowledge of safety policy development and implementation, and stakeholders (SLMS) with first-hand knowledge of how safety policies affect end users.

The data analysis presented in this chapter summarizes the findings of the research. The researcher drew connections from Phase 1 data, the personal experiences and perceptions of the interviewees from Phase 2, and the AUP analysis. The researcher looked for interconnections among the data in order to portray accurately filtering and safety policy implementation and its effect on end users. To address the research questions, the investigator employed both quantitative and qualitative data. As Creswell and Plano Clark (2007) state:

> It is not enough to simply collect and analyze quantitative and qualitative data; they need to be "mixed" in some way so that together they form a more complete picture of the problem than they do when standing alone. (p.7)

Analysis of both phases provided insight into the research questions. The data analysis and findings are presented in reference to each research question using frequency distribution tables, graphs, and relevant participant observations.

Demographics and Filtering/Safety Policy Context

The SLMS survey was successfully delivered to 398 email addresses, which were obtained from public South Carolina school Web sites, SCASL's listserv, and via telephone contact. One hundred twenty-three usable SLMS responses were submitted via SurveyGizmo's™ website, constituting a 32% response rate. The IT survey was successfully delivered to 35 email addresses, which were obtained from school districts'

Web sites and via telephone contact. Twenty-one usable IT responses were used in the analysis yielding a 60% response rate.

At the beginning of each survey, demographic information was collected. The first SLMS survey item asked respondents to specify their job title and the academic level of the students they served. The first IT survey item asked respondents to provide their job title. In response to the job title question, 104 (84.5%) SLMS survey respondents specified media specialist or library media specialist, 15 (12%) specified librarian or teacher librarian, 1 (<1%) specified computer teacher, 1 (<1%) specified information technology specialist, and 1 (<1%) specified learning commons teacher as their job title (see Table 5). Thirteen (62%) of IT survey respondents claimed the title, director of technology or technology director, 2 (9.5%) stated technology coordinator, 1 (4.8%) stated chief financial and operations officer, 1 (4.8%) stated IT security manager, 1 (4.8%) stated IT specialist, 1 (4.8%) stated infrastructure and support officer, 1 (4.8%) stated network tech, and 1 (4.8%) stated technology support in response to the job title question. As Table 5 indicates, there were instances when the respondents' job title was not, "SLMS" or "IT director." However, in those instances the job title respondents provided was closely related to or synonymous with the job titles identified for the target population groups, "SLMS" and "IT director."

Table 5. Respondents' Job Titles

Respondents' Job Titles	**Population N=144**	
	N	**%**
1a) SLMS Survey Respondents	N=123	
Library Media Specialist/Media Specialist	104	84.5
Librarian/Teacher Librarian	15	12
Computer Teacher	1	<1%
Information Technology Specialist	1	<1%
Learning Commons Teacher	1	<1%

Table 5 (continued)

Respondents' Job Titles	**Population N=144**	
	N	**%**
No Response	1	<1%
1) IT Survey Respondents	N=21	
Director of Technology/Technology Director	13	62
Technology Coordinator	2	9.5
Chief Financial and Operation Officer	1	4.8
IT Security Manager	1	4.8
IT Specialist	1	4.8
Infrastructure & Support Officer	1	4.8
Network Tech	1	4.8
Technology Support	1	4.8

To gain an overview of the academic levels SLMS respondents represented, they were asked to provide the academic level of the schools where they served. Academic level data is summarized in Table 6. The largest percentage of respondents, 38.2% (N=47), was elementary SLMS. Nineteen percent (N=23) were high school SLMS and 19% (N=23) were middle school SLMS. Several respondents worked at schools with a combination of academic levels. Four percent (N=5) worked at combined middle/high schools, 8.1% (N=10) at combined elementary/middle schools, and 2.4% (N=3) at combined elementary/middle/high schools. Eight percent (N=10) of respondents did not respond to this item. One respondent (<1%) indicated "Master's Degree" for this item, which suggests a misunderstanding of the question. Responses from SLMS who served only elementary level students were compared to those who served middle or high school students to determine if there was a difference in the information access issues they encountered.

Table 6. Respondents' Academic Level

1b) SLMS' Academic Level	Population N=123	
	N	%
High School (9-12)	23	19%
Middle School (6-8)	23	19%
Elementary (K-5)	47	38.2%
Middle/High Combined	5	4%
Elementary/Middle Combined	10	8.1%
Elementary/Middle/ High Combined	3	2.4%
No Response	10	8%
Irrelevant Response	1	<1%

To establish a context for school districts' filtering and safety policy implementation, the IT survey asked respondents whether their school districts participated in the federal E-rate program and what filtering product was utilized.

Table 7. Filtering Products Used in School Districts

Filtering Products	Population N=21	
	N	%
Lightspeed Systems	10	48%
Barracuda	2	9.5%
iPrism	2	9.5%
Fortinet/Fortigate Web Filtering	2	9.5%
CIPAFilter	1	4.8%
Marshall 8e6	1	4.8%
SmoothWall	1	4.8%
SonicWall	1	4.8%
SquidGuard	1	4.8%

One hundred percent (N=21) were E-rate participants, and thus were required to filter Internet access and implement CIPA-compliant AUPs. Table 7 identifies the types of filtering products school districts were deploying, and reveals the number and percentage of districts in which the product is used. A review of each product's Web site concluded that these filtering solutions provide a variety of Web security features including URL

filtering, gateway-based spyware and virus protection, application protocol blocking, such as IM and P2P, and HTTPS scanning.

Research Question 1

Research Question 1 asked, "How are filtering and safety policies being implemented in public schools?" Several items on the IT survey, the SLMS survey, and the interview protocol addressed the question. Survey and interview items focused on three filtering and safety policy implementation issues (variables) that were identified in the literature review (see Table 4). These variables include content blocking considerations, stakeholder involvement in policy decisions, and differentiated access levels for specific user groups.

Content Blocking Considerations

Important filtering and safety policy implementation considerations include deciding what content should be blocked, the level of blocking within each content category, and whether to deploy the filter's "out of the box" or default settings. Factors that influenced filtering and safety policy decisions included CIPA compliance, bandwidth preservation, non-educational network usage, potential litigation, network security, student safety, and community opinions. The IT survey, SLMS survey, and interview protocol items focused on these considerations.

IT survey question 4 solicited responses regarding the content categories that were filtered and the level of filtering within those categories. Table 8 summarizes this data. Some survey respondents did not select an answer choice for each content category; therefore, the results show the frequency and percentages of survey participants who selected an answer choice.

CIPA requires school districts receiving E-rate discounts to block access to visual images that are obscene, contain child pornography, or are harmful to minors. One hundred percent (N=21) of school districts filtered adult/mature and pornography/nudity content as CIPA requires. Most school districts (95.2%, N=20) filtered all, and 4.8% (N=1) filtered some adult/mature and nudity/pornographic content. School districts filtered categories in addition to obscene content, including controversial and questionable content. Eighty-one percent (N=17) filtered all gambling content, 9.5% (N=2) filtered some, and 4.8% (N=1) filtered none. Most (77.8%, N=14) respondents filtered all alcohol/tobacco related content, 22.2% (N=4) filtered some, while 0% filtered none. All hate/racism content was filtered in 76.5% (N=13) of responding school districts, 17.6% (N=3) filtered some, and 5.9% (N=1) did not filter this content. All drug related content was filtered in 66.7% (N=12) of responding school districts, 33.3% (N=6) filtered some, and 0% filtered none. More than half of all respondents (66.7%, N=12) filtered all criminal/illegal content, 27.8% (N=5) filtered some, and 5.6% (N=1) filtered none of this content. Similarly, more than half (62.5%, N=10) filtered all cult/occult content, 25% (N=4) filtered some, and 12.5% (N=2) filtered none. All violent content was filtered in 53.3% (N=8) of school districts, 46.7% (N=7) filtered none, and 0% filtered none. Most (58.8%, N=10) filtered all weapon related content, 35.3% (N=6) filtered some, and 5.9% (N=1) filtered none of this Web content. A smaller percentage (46.2%, N=6) filtered all alternate lifestyles (LGBT) content, 38.5% (N=5) filtered some, and 15.4 (N=2) filtered none. Fewer than half (40%, N=6) filtered all intimate apparel and swimsuit content, 53.3% (N=8) filtered some, while 6.7% (N=1) filtered none. A

smaller percentage of respondents (20%, N=3) filtered the entire sex education category, 66.7% (N=10) filtered some, and 13.3% (N=2) filtered none.

Table 8. Filtered Content Categories

Content Categories	Filters All %	N	Filters some %	N	Filters None %	N	Total Responses
Adult/Mature	95.2	20	4.8	1	0.0	0	21
Pornography/Nudity	95.2	20	4.8	1	0.0	0	21
Alcohol/Tobacco	77.8	14	22.2	4	0.0	0	18
Gambling	81.0	17	9.5	2	4.8	1	20
Hate/Racism	76.5	13	17.6	3	5.9	1	17
Drugs	66.7	12	33.3	6	0.0	0	18
Criminal/Illegal	66.7	12	27.8	5	5.6	1	18
Cult/Occult	62.5	10	25.0	4	12.5	2	16
Violence	53.3	8	46.7	7	0.0	0	15
Weapons	58.8	10	35.3	6	5.9	1	17
Alternative Lifestyles (LGBT)	46.2	6	38.5	5	15.4	2	13
Intimate Apparel/Swimsuits	40.0	6	53.3	8	6.7	1	15
Sex Education	20.0	3	66.7	10	13.3	2	15
Hacking/Proxy Avoidance	84.2	16	10.5	2	5.3	1	19
Malicious sites	83.3	15	16.7	3	0.0	0	18
Internet Radio/TV	55.6	10	44.4	8	0.0	0	18
Media downloads/file sharing	46.7	7	53.3	8	0.0	0	15
Telephony (VoIP)	36.4	4	45.5	5	18.2	2	11
Social Networking	58.8	10	41.2	7	0.0	0	17
Email/Chat/Instant Messaging	50.0	7	50.0	7	0.0	0	14
Blogs/Wikis	23.1	3	69.2	9	7.7	1	13

School districts also filtered content posing possible security threats and bandwidth consuming content. Most districts (84.2%, N=16) filtered all hacking and

proxy avoidance Web sites, 10.5% (N=2) filtered some, and 5.3% (N=1) filtered none. Similarly, 83.3% (N=15) filtered all malicious sites, 16.7 (N=3) filtered some, and 0% filtered none of this content. Bandwidth consuming content was also filtered in most school districts. More than half (55.6%, N=10) blocked all Internet radio and television sites, 44.4% (N=8) blocked some, 0% blocked none. Less than half (46.7%, N=7) blocked all media download and file sharing sites, 53.3% (N=8) blocked some, and 0% blocked none. A smaller percentage of respondents (36.4%, N=4) blocked all telephony (VoIP) Web sites, 45.5% (N=5) blocked some and 18.2% (N=2) blocked none.

Web sites that support communication and collaborative activities (Web 2.0) were filtered in some school districts. All social networking sites were filtered in 58.8% (N=10) of school districts, 41.2% (N=7) filtered some, and 0% filtered none. Fifty percent (N=7) filtered all email, chat, and instant messaging sites, 50% (N=7) filtered some, while 0% of respondents filtered none. Less than one-fourth (23.1%, N=3) filtered all blogs and wikis, 69.2% (N=9) filtered some, and 7.7% (N=1) filtered none of this content.

IT survey questions 7a and 7b were asked to determine whether districts customized filter configurations to limit content over-blocking. When asked if the district used the filter's default settings, 75% (N=15) of respondents answered no and 25% (N=5) answered yes. In response to item 7b, "when appropriate, the filter is configured to block specific sub-categories," 95.2% (N=20) responded yes, and 4.8% (N=1) responded no.

The literature review revealed several factors that influence content filtering decisions. To determine the extent to which these factors affected filtering and safety policy implementation decisions, IT survey respondents were asked to indicate the degree

to which specific factors influenced filtering decisions on a 1-5 point scale where 1 represented no influence and 5 represented substantial influence. As seen in Table 9,

Table 9. Factors Influencing Content Filtering Decisions

Influencing Factors	Mean	SD	Rank	Total Responses
CIPA Compliance	4.95	0.21	1	21
Maintaining Student Safety	4.80	0.39	2	21
Maintaining Network Security	4.76	0.44	3	21
Preserving Bandwidth	4.38	0.65	4	21
Preventing Litigation (Lawsuits)	4.23	0.97	5	21
Preventing Non-educational Use	3.76	0.97	6	21
Community or Parental Opinions	3.62	1.25	7	21

CIPA compliance (M=4.95) exerted the greatest influence on policy decisions. However, school districts blocked considerably more content than CIPA requires. Student safety (M=4.80) and network security (M=4.76) exerted almost as much influence as CIPA compliance. The need to preserve bandwidth (M=4.38) and prevent litigation (M=4.23) were highly influential considerations as well. The importance of the foregoing factors may explain why most districts elected to block more content than CIPA compliance requires. Although still important, preventing non-educational use (M=3.76) and community or parental opinions (M=3.62) exerted less influence on policy decisions. The level of influence that each factor exerted on filtering and safety policy decisions was greater than the average mean (3). This implies each factor was an important consideration for policymakers. The relative importance of each of these factors to filtering decisions may explain why districts implemented restrictive filtering policies.

Stakeholder Involvement in Policy Decisions

To ascertain the level of stakeholder involvement and influence in policy decision making, the data collection instruments included items focusing on stakeholder input in filtering policy decisions. IT survey item 5 and SLMS survey item 2 was asked to determine whether representatives from various stakeholder groups (i.e., teachers, students, parents, media specialists, administrators) were involved in filtering policy decisions. SLMS survey item 7a also asked if input from all stakeholders was considered when content filtering decisions were made. Question set 1 of the interview protocol asked participants to describe how stakeholders were involved in policy decisions and whether stakeholder involvement positively influenced information access and student safety. IT administrators' and SLMS' responses in Figure 2 suggest that most content blocking decisions were made by district-based personnel or left to the software developer. Ninety percent (N=18) of IT respondents and 41.8% (N=51) of SLMS stated

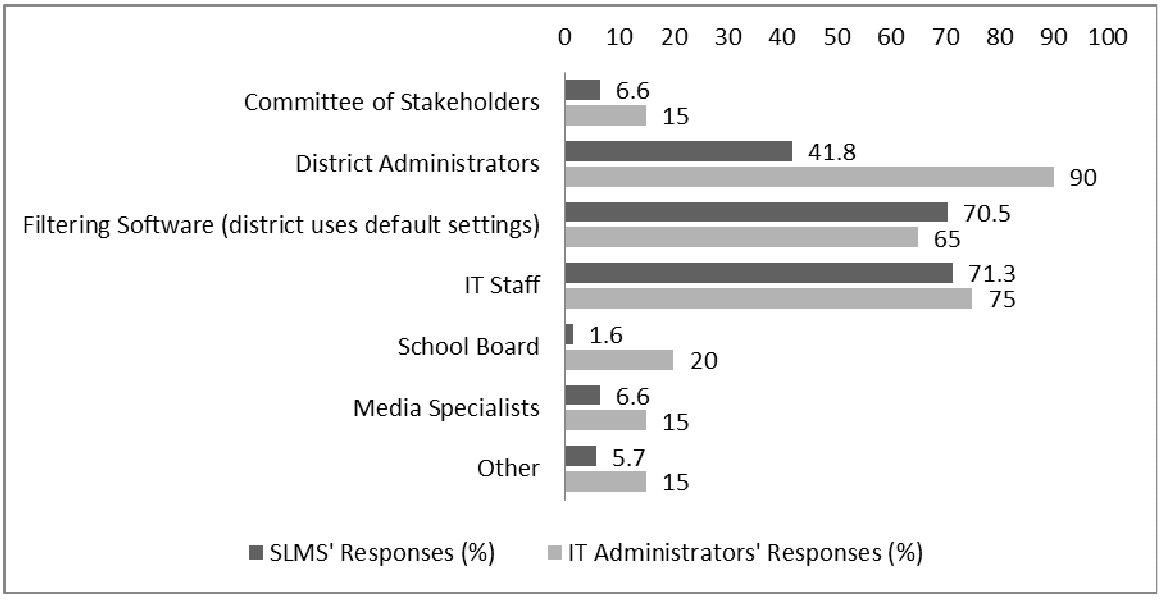

Figure 2. Who makes content filtering decisions?

that district administrators decided what content should be blocked. Sixty-five percent (N=13) of IT respondents and 70.5% (N=86) of SLMS said the filtering product made content filtering decisions because the product's default settings were used. A similar proportion of respondents, 75% (N=15) of the IT group and 71.3% (N=87) of media specialists, replied that IT staff decided what content was filtered. Conversely, survey responses suggest school boards (1.6%, N=2 /SLMS, 20%, N=4/ IT respondents), stakeholder committees (6.6%, N=8 /SLMS, 15%, N=3/ IT respondents), media specialists (6.6%, N=8 /SLMS, 15%, N=3/ IT respondents), and other groups (5.7%, N=7/SLMS, 15%, N=3/ IT respondents) were minimally involved in filtering decisions. Additionally, when SLMS survey item 7a asked whether input from all stakeholders was considered when content filtering decisions were made, 50% (N=58) said no, 40.5% (N=47) were not sure, and 9.5% (N=11) said yes.

A thematic analysis of open-ended survey comments and interview data provided additional insight into stakeholder involvement in filtering and safety policy decisions. Lack of stakeholder involvement was a major theme that emerged from participant comments. Interviewee 1 recalled being involved in AUP development at an earlier time, but indicated SLMS were no longer involved the process. Interviewee 4 broadened stakeholder noninvolvement to students and parents when she stated, "There is no involvement. Students and parents have no say so whatsoever."

Respondent statements reveal some districts' filtering policy decision making was largely done in the technology department without the involvement of other stakeholders. Interviewee 3 indicated the technology department made most filtering and safety policy decisions when she stated, "All that (filtering/safety policy decisions) is handled in the

technology department at the district level….We have no input at this point." An SLMS survey respondent expressed stronger sentiment regarding technology administrators' control of technology policy decision making in the following comment:

> Our IT director makes all of these decisions single-handedly. She would say that she gets input from our district administration, but she is the one who tells them about content blocking and is their sole source of information on this topic (SLMS survey comment).

Some districts attempted to get input from stakeholders; however, these attempts were unsuccessful because of ineffective implementation. One SLMS survey respondent commented that when the district attempted to involve a committee of stakeholders in the decision making process, IT staff with no teaching experience ultimately decided what content was blocked. Another SLMS survey respondent commented that the district's committee did not include K-2 teachers. Consequently, filtering policies continued to block educational sites for younger students, such as Cyberchase™ and PBSKids™. The aforementioned comments suggest a committee of stakeholders is not a panacea for the issues that evolve from filtering and safety policy implementation, particularly when the committee's recommendations are disregarded or when the committee is not representative of all end users.

Even when respondents indicated stakeholders were involved in technology policy decisions, this involvement was limited mostly to submitting blocking and unblocking requests. For example, an IT survey respondent commented that all employees were "empowered to identify and report" inappropriate sites to IT and these sites would be blocked immediately. In response to the stakeholder involvement inquiry,

Interviewee 2 reported that parents and students could report concerns or requests to unblock Web sites to school staff, and these requests would then go directly to the district office. Interviewee 2 added that when teachers and media specialists voiced their opinions about online content that should be unblocked; the district was receptive to these requests because teachers and media specialists were viewed as professionals who would only submit unblocking requests for educational content.

Some participants' comments suggest end users should be more involved in Internet use policy decisions. Interviewee 1 stated, "We're in the trenches, we're using the resources. It makes perfect sense that we are involved in establishing the guidelines that govern the use of the resources." Interviewee 4 also thought the district should seek input from students and teachers about content that should be blocked.

The aforementioned interview participant statements and survey respondent comments provided a deeper understanding of stakeholder involvement in filtering and safety policy deliberations. Survey and interview data suggest stakeholder involvement in Internet use policy decisions was minimal, limited mostly to submitting requests to block or unblock content. This data also provides insight into the access issues that arise when end users are not involved in filtering and safety policy deliberations.

Differentiated Access Levels

Filtering products typically allow customization of filter settings for specific user groups to increase access to information and educational resources. IT survey item 7e and SLMS survey item 7d asked whether distinct access levels had been set for different user groups such as elementary students, secondary students, and staff. Table 10 summarizes survey data about differentiated access implementation. When asked if differentiated

access had been implemented, 47.5% (N=56) of SLMS said yes, 36.4 (N=43) said no, and 16.1% (N=19) were unsure, while 76.2% (N=16) of IT administrators said yes, 23.8% (N=5) said no, and none were unsure. Substantially more IT administrators than SLMS reported that differentiated access levels had been implemented. One explanation of the discrepancy between SLMS' responses and IT administrators' responses could be that SLMS were unaware differentiated access policies had been implemented.

Table 10. Implementation of Differentiated Access Levels

Data Source	**SLMS N=118 %**	**IT N=21 %**
(Survey item 7e (IT) and 7d (SLMS) Different Access levels have been established for specific user groups		
Yes	47.5	76.2
No	36.4	23.8
Not Sure	16.1	0.0

Analysis of survey comments and interviewee comments suggest that differentiated access levels were established mostly for staff in some school districts. Access levels were rarely differentiated according to student age levels. For instance, an SLMS survey respondent reported that staff and students had different access levels, but there was no difference for any student levels. In another district, teacher and staff logins allowed them to access streaming video and other "coached" sites temporarily. Some districts implemented different access levels in addition to time of day restrictions. In these instances survey respondents reported that teachers could only access TeacherTube™ and YouTube™ before and after school. Finally, another SLMS survey respondent commented that different access levels had been discussed, but the respondent was uncertain whether differentiated access levels had been implemented.

Interview participant statements about differentiated access levels were similar to survey participant comments and suggest staff and students had different access levels, but students, regardless of age level, had the same access privileges. Interviewee 4 commented that SLMS could "roam at will," but teachers could not access Web sites such as YouTube™. Interviewee 5 specified that different access levels had been established for teachers and students. Teachers could access Facebook™ and YouTube™, but students were unable to access these Web sites. Interview and survey data suggest differentiated access levels were implemented in some school districts, but access levels were not tailored to meet the unique information needs of all user groups.

Research Question 2

Research question 2 asked, "What issues do SLMS encounter as they facilitate information access on filtered computers?" To address this research question, the data collection instruments focused on filtering issues that were identified in the literature (see Table 4). To determine the scope of these issues and the way in which they affected teaching and learning, data was collected about filter over-blocking frequency, under-blocking frequency, filter effectiveness, specific types of blocked educational content, and the efficiency of unblocking procedures.

Over-blocking and Under-blocking

Over-blocking and under-blocking are inherent issues with all Internet filtering tools. To gauge the frequency of these filtering issues, IT survey item 9a and 9b asked respondents how often they received requests during a typical week to block inappropriate content and to unblock educational content that had been blocked inadvertently. SLMS survey item 5a and 5b asked how often the filter permitted access to

objectionable content (under-blocking) during a typical week and how often it prevented access to educational content during a typical week.

According to Table 11, 4.8% (N=1) of IT respondents never received requests to block inappropriate content, 47.6% (N=10) rarely received requests to block inappropriate content, 42.9 (N=9) sometimes received requests to block inappropriate content, and 4.8% (N=1) frequently received requests to block inappropriate content.

Table 11. Over-blocking and Under-blocking Frequency

Survey Item	Never %	Rarely %	Sometimes %	Frequently %
IT Survey Item 9		**Total Responses (N=21)**		
During a typical week, how often do you (or the person responsible for blocking/unblocking content) receive requests to:				
a) block inappropriate content	4.8 N=1	47.6 N=10	42.9 N=9	4.8 N=1
b) unblock educational content that has been unintentionally blocked	0.0 N=0	15 N=3	70.0 N=14	15.0 N=3
SLMS Survey Item 5		**Total Responses (N=120)**		
During a typical week, how often does the filter:				
a) Permit access to objectionable content	16.7 N=20	55.0 N=66	24.2 N=29	4.2 N=5
b) Prevent access to information/resources that support educational, professional, or personal growth	3.3 N=4	15.0 N=18	41.7 N=50	40.0 N=48

When asked how often they received requests to unblock educational content that the filter had blocked inadvertently, 0.0% stated never, 15% (N=3) stated rarely, 70% (N=14) stated sometimes, and 15% (N=3) stated frequently. When asked how often the filter permitted access to objectionable content, 16.7% (N=20) of SLMS replied never, 55% (N=66) replied rarely, 24.2% (N=29) said sometimes, and 4.2% (N=5) replied frequently.

When asked how often the filter prevented access to information/resources that support educational, professional, or personal growth, 3.3% (N=4) responded never, 15% (N=18) responded rarely, 41.7% (N=50) responded sometimes and 40% (N=48) responded frequently. Less than 30% of SLMS respondents reported under-blocking, which suggests that under-blocking is less of filtering issue than over-blocking. More than 80% of SLMS sometimes or frequently encountered over-blocking of educational content, which implies that over-blocking was a more pervasive filtering issue.

To assess further the effectiveness of implemented filtering solutions, IT survey items 10a and 10b, plus SLMS survey item 6 asked respondents to rate the filter's efficacy in blocking inappropriate content and permitting access to educational content. Regarding the filter's effectiveness in blocking inappropriate content, 14.3% (N=3) of IT administrators responded very ineffective, 4.8% (N=1) responded somewhat ineffective, 9.5% (N=2) responded somewhat effective, and 71.4% (N=15) responded very effective. In response to item 10b, which asked IT respondents to rate the filter's effectiveness in permitting access to educational content, 9.5% (N=2) rated it very ineffective, 9.5% (N=2) somewhat ineffective, 19% (N=4) somewhat effective, and 61.9% (N=13) very effective. SLMS survey item 6 asked, "Considering the filter's over-blocking and under-blocking efficiency, how would you rate the filter's overall effectiveness?" In response, 8.3% (N=10) of SLMS replied very ineffective, 15.8% (N=19) replied somewhat ineffective, 13.3% (N=16) replied neutral, 45.8% (N=55) replied somewhat effective, while 16.7% (N=20) replied very effective. A comparison of IT and SLMS responses reveals that more than 80% (N=17) of IT respondents rated filter efficacy as either somewhat effective or very effective, while a smaller percentage (52.5%, N=75) of

SLMS rated filter efficacy as somewhat effective or very effective. This indicates that end users were less satisfied with the filtering products deployed in school districts than the individuals who deployed them.

Filters are implemented to protect minors from deliberately or unintentionally accessing inappropriate content, but under-blocking and filter circumvention sometimes hinder technology protection measures from protecting minors. Item 8c asked SLMS whether they agreed that the district's filtering solution prevented users from deliberately (circumvention) or unintentionally (under-blocking) accessing inappropriate content. In response to this item, 1.7% (N=2) strongly disagreed, 6.8% (N=8) disagreed, 63.6% (N=75) agreed, 22.9% (N=27) strongly agreed, and 5.1% (N=6) were neutral. This data suggests content filtering protects students from most inappropriate content.

Although, most respondents believed filters adequately protected students, interview participant comments convey the context of filter circumvention and under-blocking in public schools. Interview participant comments show that filter circumvention was more of an issue in the secondary school setting. When secondary SLMS interviewees were asked whether they were aware of instances when students bypassed the filter to access blocked content, their responses suggest filter circumvention was a common occurrence at the secondary level. Interviewee 1 was not sure of the correct terminology to describe how students circumvented the filter. Students knew how to "infiltrate" or "debug" the filter, according to Interviewee 1. Moreover, students tried to "fake it out" (the filter) so they would have more access rights than they were supposed to. Interviewee 4 said students circumvented the filter "all the time." Before the district began blocking proxy avoidance sites, students would type "proxy" in as a

Google™ search to find directions for circumventing blocked content. Even though the district began blocking access to proxy avoidance Web sites, Interviewee 4 reported students had figured out how to get around the filter to access YouTube™ videos. In fact, students had shared this circumvention tactic with teachers who were using it to access YouTube™ videos for instructional purposes. Similarly, Interviewee 5 recounted that students circumvented the filter "on a weekly basis." Instead of being a tool to protect students, Interviewee 5 believed the filter provided "a personal challenge" for some students to discover ways to outsmart the filter.

When elementary SLMS were asked whether they were aware of students bypassing the filter, Interviewee 2 commented, "No, not in elementary school. They can't figure that out yet." Similarly, Interviewee 3 replied, "I'm sure middle school and high school students are savvier, but personally, I've not had any problems." These statements imply that filter circumvention is more of an issue at the secondary level than at the elementary grade level.

Regarding filter under-blocking, Table 11 shows that almost half (47.7%, N=10) of IT respondents indicated they sometimes or frequently received requests to block inappropriate content. This suggests that filters cannot completely protect minors from inappropriate content and must be supplemented by other safety measures. Interviewees provided under-blocking scenarios when asked if they could give specific instances when under-blocking adversely influenced instruction or student safety. Interviewee 1 described under-blocking issues perceived to be the result of policymakers' failure to involve school-based staff in policy decisions. Although school-based staff had asked for Google™ images to be blocked, they were not blocked. As a result, students accessed

inappropriate images several times a week. Interviewee 1 described a particularly disruptive incident when a student typed in a pornographic actress' name, accessed numerous pornographic images of her, and printed them. Interviewee 4 described less disruptive under-blocking situations. Under-blocking mostly resulted in students accessing "borderline inappropriate" content at Interviewee 4's school. Examples of inappropriate access included a student who visited a chat room and used inappropriate terms to describe himself while in the chat room. "The worse thing I've seen" according to Interviewee 4, "is kids looking at pictures of local prisoners." The aforementioned under-blocking scenarios along with survey data suggest under-blocking was not as pervasive as over-blocking, but when it occurs, it can disrupt the educational setting. These under-blocking incidents further underscore that filters cannot entirely prevent students from deliberately or inadvertently accessing inappropriate online content.

Survey item 3 asked SLMS to select the types of educational content the district's filtering solution over-blocked. This item, which asked respondents to select all content that applied, was asked to ascertain how filtering policy decisions impact learning and information access. Figure 3 shows that 18.8% (N=22) of SLMS selected business and finance, 58.1% (N=68) selected controversial content (i.e., alternative lifestyles, hate groups, cults, occult), 45.3% (N=53) selected educational games, 52.1% (N=61), selected health and sex education, 25.6% (N=30) selected sports and recreation, 84.6% (N=99) selected streaming media (i.e. YouTube, UStream.tv, Internet radio), 35.9% (N=42) selected virtual worlds, 45.3% (N=53) selected visual images, 66.7% (N=78) selected Web 2.0 (i.e. wikis, blogs, social bookmarking tools), and 16.2% selected other, which included topics such as popular culture, entertainment, shopping/marketing, and travel

information . The majority of respondents (more than 50%) encountered blocked streaming media, health and sex education Web sites, controversial content, and Web 2.0 resources, which implies that filter settings prevented users from accessing a substantial amount of educational content.

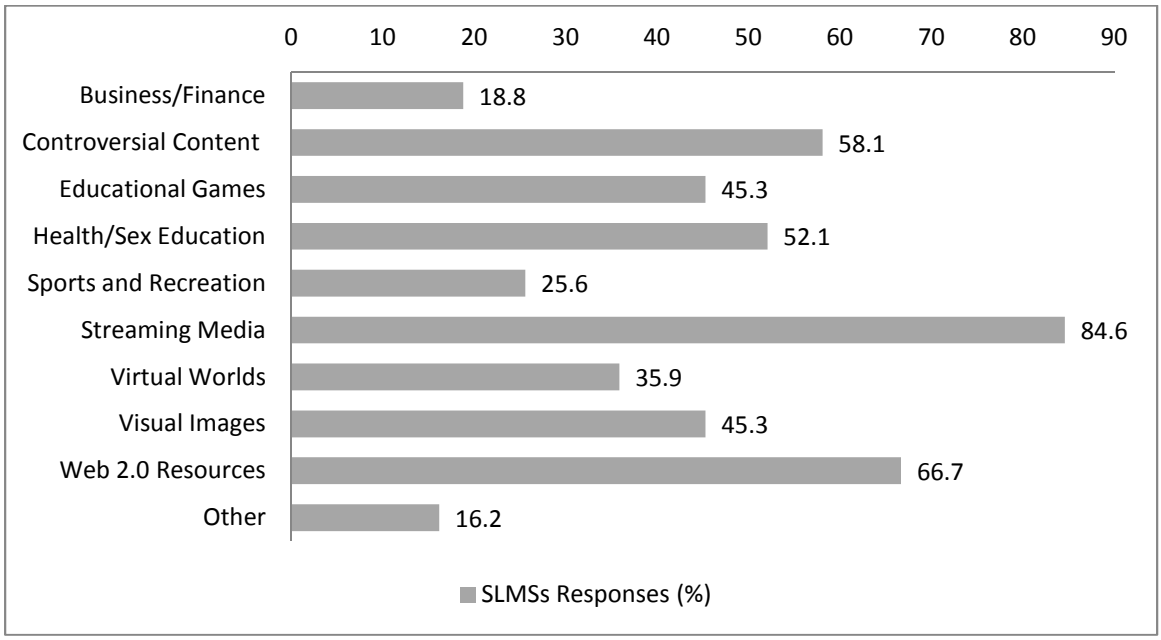

Figure 3. Over-blocked content.

SLMS survey items 8a and 8b served to investigate further the influence of over-blocking on teaching and learning. Item 8a asked SLMS to specify the extent of their agreement with the following statement: "The Internet filter prevents instructional staff from accessing resources needed for instructional or professional activities." Four SLMS (3.4%) strongly disagreed, 21.2% (N=25) disagreed, 50.8% (N=60) agreed, 14.4% (N=17) strongly agreed, and 10.2% (N=12) were neutral about this statement. Item 8b asked SLMS to select the extent of their agreement with the following statement: "The Internet filter prevents students from accessing information and resources needed for classroom assignments." Seven SLMS (5.9%) strongly disagreed with this statement, 28% (N=33) disagreed, 40.7% (N=48) agreed, 8.5% (N=10) strongly agreed, and 16.9% (N=20) were neutral about this statement. More SLMS (65.2%, N=77) agreed or strongly agreed that filtering policies blocked access to instructional resources than SLMS (24.6%, N=29) who disagreed or strongly disagreed that filters blocked access to

instructional resources. Similarly, a greater proportion of SLMS (49.2%, N=58) agreed or strongly agreed that filtering policies blocked student access to educational resources while a lesser proportion disagreed or strongly disagreed (33.9%, N=40). This data suggests that district filtering policies were having an adverse influence on information access for many end users, including instructional staff and students.

Interviewees' statements provide additional evidence of how over-blocking influenced end user access to educational content. Interview participants were asked whether they believed over-blocking adversely influenced student or teacher access to educational resources. They were also asked to provide specific examples of when over-blocking prevented students from accessing resources needed for assignments or teachers from accessing resources needed for instruction or professional development.

Interviewees' observations featured instances when over-blocking prevented teachers from implementing lesson plans. Interviewee 5 reported that teachers often develop lesson plans at home, but when they get to school, the Web site they need is blocked. It was impossible to unblock Web sites immediately in Interview 5's district because the unblocking process required about 24 hours. Interviewee 1 recounted a personal experience when a request to unblock a Holocaust Web site was denied. After preparing at home to teach a lesson that required taking students to a Holocaust Web site, the SLMS recalled that the site was blocked at school. The unblocking process entailed submitting a request to the principal who then forwarded the request to the IT director. After almost four weeks, the IT director informed Interviewee 1, via the principal that the images of emaciated bodies on the site were too graphic for students; therefore, the unblocking request was denied. Interviewee 1 expressed the kind of frustrations some teachers feel when someone without classroom experience disregards their professional opinion about what is appropriate for students when she stated, "It's upsetting that they

don't respect my professional integrity." Administrators restricted access to content for reasons other than inappropriateness of the content. Interviewee 5 related how over-blocking resulted from using filters to manage bandwidth when she stated, "For a while, the teachers and everybody, we were blocked from streaming video sites because of bandwidth problems."

Interviewee observations suggest over-blocking adversely affected educators' inclination to incorporate innovative online resources into classroom instruction. Interviewee 4 described a time when she tried to convince a "techy" teacher to incorporate an innovative online resource into his lessons. The teacher's response was "I gave up on that a long time ago because so much stuff is blocked." Interviewee 4 described another instance when over-blocking prevented educators from using an online resource. The SLMS stated, "Once I was at a conference and I learned about using Google Earth™ for 'lit trips.' I emailed some of my teachers about it from the conference. One [teacher] replied, 'I just tried it and it was blocked.'" These observations illustrate how over-blocking can limit integration of Web-based technology. Moreover, end user frustration about over-blocking was evident when Interviewee 4 commented, "I've talked to teachers and some feel like many Web sites shouldn't be blocked in the first place."

Interviewee observations describe how over-blocking adversely influenced students' ability to complete assignments. Interviewee 5 suggested, "It's hard for students to complete assignments if they can't get to the online resources they need." Furthermore, Interviewee 5 was concerned that over-blocking exacerbated the digital divide between students with home Internet access and students without home Internet access when

asserting, “The students with home Internet access just go home and access the sites that are blocked at school. The students without home access just can’t get to it. It’s like we’re back to the haves and have-nots.” Interview 4 observed that the filter prevented students from searching for breast cancer information because it blocked Web sites that included the word “breast.” The SLMS also described how students were unable to insert a Web-based image into a PowerPoint presentation because the download capability had been disabled. Interviewee 5 recalled a time when several students were doing research on the history of gaming and many of the gaming Web sites were blocked. Consequently, these students were unable to complete their research at school. Over-blocking negatively affected student research at all levels, including elementary students. Conducting research on filtered computers involved “a lot of trial and error,” according to Interviewee 3, an elementary SLMS. Interviewee 3 related an over-blocking incident involving a 5th grader who had been conducting research at home on an immigration Web site, but when the student tried to access the same Web site at school, it was blocked.

The aforementioned over-blocking scenarios provide a deeper understanding of the types of information filters over-block. They also describe how over-blocking adversely affected lesson planning, completion of student assignments, the digital divide, and limited opportunities for educators to incorporate innovative Web based technologies in their lessons.

Unblocking Procedures

The literature review revealed that the adverse effects of filter over-blocking could be minimized with efficient unblocking procedures. The data collection instruments included several items about school districts’ unblocking practices and

procedures to determine how effectively they minimized the adverse effects of over-blocking. IT and SLMS survey items asked whether filter settings could be adjusted to unblock educational content, what staff had been granted override privileges to unblock content, whether users were informed of unblocking procedures, and how efficiently the procedures allowed access to over-blocked educational content. To gain a deeper understanding of unblocking procedures and their impact on end users, interview participants were asked to describe their district's unblocking procedures and whether unblocking procedures impeded or facilitated information access.

Table 12. Content Unblocking Configuration

IT Survey Item 7c **Filter settings can be overridden or adjusted to access educational content that has been blocked unintentionally.**		
	%	**N**
Yes	95.2	20
No	4.8	1
Not Sure	0.0	0

The literature review confirms that fine-tuning capability is a key feature for effective filtering solutions, and should be implemented to provide maximum information access. IT survey item 7c (see Table 12) asked respondents whether filter settings could be overridden or adjusted to permit access to blocked educational content. Twenty (95.2%) responded yes and 4.8% (N=1) responded no, and no respondent was unsure. Configuring filters so that on-campus staff can override the filter creates a more efficient unblocking process according to the literature review. IT survey item 7f and SLMS survey item 7b (see Table 13) asked participants whether filter override privileges had been granted to designated on-campus staff. Thirty-four (29.1%) of SLMS replied yes, 65% (N=76) replied no, and 6.0% (N=7) were unsure if someone on campus had been

granted filter override privileges. Fourteen (66.7%) IT respondents indicated that filter bypass privileges had been granted, 33.3% (N=7) replied no, and no IT respondent was unsure about this item.

Table 13. Filter Override Privileges and Blocked Page Notification

Survey item 7f (IT) and 7b (SLMS) **Filter override privileges have been granted for designated on-campus staff (i.e., administrators, media specialists, technology specialists)**	**SLMS Responses**		**IT Responses**	
	%	**N**	**%**	**N**
Yes	29.1	34	66.7	14
No	65.0	76	33.3	7
Not Sure	6.0	7	0.0	0
Survey item 7d (IT), 7c (SLMS) **When users encounter blocked content, the blocked page notification instructs users how to get the content unblocked.**				
	%	**N**	**%**	**N**
Yes	53.4	63	95.2	20
No	39.8	47	4.8	1
Not Sure	6.8	8	0.0	0

Compared to IT respondents (66.7%), a much smaller proportion of SLMS (29.1%) said filter override privileges had been granted to on-campus staff. One possible explanation of the disparity between SLMS and IT responses may be that some SLMS were unaware that override privileges had been granted to on-campus staff. In some circumstances, even though school-based staff was given override privileges, extenuating circumstances sometime delayed access to blocked content. One SLMS survey respondent explained that each school was given a filter override password. However, the respondent stated, “Sometimes the password will allow the user access; sometimes it won't, resulting in an educator sending an email to the technology office to get the Web site unblocked.”

SLMS survey item 7c and IT survey item 7d (see Table 13) asked respondents whether the blocked page notification instructed users how to get blocked content unblocked. In response to this item, 53.4% (N=63) of SLMS answered yes, 39.8% (N=47) answered no, and 6.8% (N=8) were unsure. Twenty (95.2%) IT administrators answered yes, 4.8% (N=1) answered no, and there were no IT respondents unsure about this item. A smaller percentage of SLMS (53.4%, N=63) said the blocked page notification instructed users how to get blocked content unblocked than IT administrators (95.2%, N=20). The discrepancy between IT administrators' and SLMS' responses for this item implies unblocking instructions might not have been adequately explained or may not have been perceptible to end users on the blocked content notification page. Interviewee 4's comments support this conclusion. The SLMS stated, "I don't know that people are told how to get something unblocked. The link on the blocked page is very subtle. The unblocking process is not well known."

Several IT directors and SLMS survey participants submitted comments describing unblocking procedures that had been implemented. Most unblocking procedures required end users to submit a request to unblock content. For example, one SLMS survey respondent wrote, "In order to get a site unblocked we have to submit a technology work order," and another commented, "We can ask for sites to be unblocked." Some districts' unblocking procedures allowed users to submit unblocking requests directly from the blocked page by clicking on a link. In some cases, direct input from the blocked page allowed immediate access to blocked content. One IT survey respondent wrote, "When a site is blocked, a request form can be completed at that moment. The request comes to me and it is unblocked immediately if [the site is] a legitimate site. If

[there is] a question, the superintendent is contacted." In other cases, access to blocked content was delayed even when users submitted unblocking requests via a link on the blocked page, as the following IT respondent explanation illustrates:

> [When] users (student or staff) receive a blocked page, they can enter the request to unblock. The Lightspeed Company checks the site to see if it is in the correct category and often changes it, which allows access. It takes 2-4 hours. The following day upper level district IT checks the list of blocked sites and manually approves or denies the request. In any case, an email is sent to the requester explaining the action taken. (IT Respondent Comment)

The aforesaid unblocking process delayed access to content because the unblocking request went through multiple bureaucratic layers (Lightspeed and district IT staff). Cumbersome unblocking processes were evident in other IT respondents' explanations as well. For example, an IT respondent explained that unblocking requests were sent via "email from an administrator to the director of IT."

SLMS also described cumbersome unblocking procedures requiring requests to be sent through multiple bureaucratic layers. These procedures likely lead to delays in accessing blocked content. One SLMS commented, "Media specialists can forward requests from teachers to the IT staff to request that specific sites be unblocked." Another SLMS commented, "If something needs to be unblocked at the school level, we tell our principal and he/she requests that it be unblocked." Survey respondent comments suggest protracted delays also resulted when technology administrators were too busy with other duties to unblock sites. Another SLMS survey respondent wrote, "[We have] very limited override. There are unblocking instructions, but our Tech administrator is too

overwhelmed to have the time to unblock sites." Another SLMS survey respondent stated, "We have to submit a request to the IT department to unblock a site. That process takes 2-4 weeks."

SLMS survey comments such as "Faculty members can request IT unblock specific sites," and "Teachers and other district employees can send requests to have Web sites unblocked," suggest some districts only permitted staff members to submit unblocking requests. However, a few districts accepted requests from any user as the following survey comment suggests: "Any user can submit requests to have sites unblocked and any user can recommend that sites be blocked." Although users encountered delays in accessing blocked content, survey comments suggest most unblocking requests were granted. A SLMS commented, "….requests are usually honored," and another stated, "If a site we want to use is blocked, we can request it be unblocked and it usually is."

An analysis of interviewee observations revealed themes similar to those that emerged from SLMS' survey comments about districts' unblocking procedures. Interviewees described similar impediments to accessing blocked educational content. Their statements indicate some end users were required to go through multiple bureaucratic layers, experienced long delays, or were uncertain about unblocking procedures.

Interviewee 1 and Interviewee 5 described unblocking procedures requiring requests to be sent through multiple bureaucratic layers. Interviewee 5 reported, "If someone emails the principal the Web site to be unblocked, she emails someone at the district office who looks at the site, then emails the principal, and she emails back to

you." Interviewee 1 described similar procedures when she stated, "When something is blocked by the filter, I submit a request to the principal, and he submits the request to the director of IT." Interviewee 1's observation that waiting "as long as four weeks to get something unblocked" suggests these cumbersome procedures resulted in substantial delays in accessing blocked content. Similarly, Interviewee 5 suggested the districts' unblocking procedures were inefficient when stating, "Our access policies are inconvenient; it takes longer than it should to get something unblocked."

Interviewee 2 and Interviewee 3, who were elementary SLMS, expressed less frustration about unblocking procedures than the secondary interview participants (Interviewee 1, 4, & 5). Elementary interview participants' comments indicate approval of their districts' unblocking procedures, despite having to wait several days for content to be unblocked. Their statements suggested that unblocking procedures permitted timely access to blocked content. For instance, Interviewee 2 stated, "It takes less than a week to unblock a Web site….There's great turnaround time." Similarly, Interviewee 3 commented, "This is a good process. I've never had to wait more than two days." In Interviewee 2's district, instructional staff contacted the help desk to submit unblocking requests. Interviewee 2 expressed approval of the unblocking process when she stated, "They look at requests on a daily basis. They know we're professionals, that if we ask for something to be unblocked, that obviously we need it. I haven't heard of anything not being unblocked." Interviewee 3, who also believed her district's unblocking procedures were efficient, described an unblocking process that required users to click on a blocked page link to access an unblocking request form. As part of the request, users were required to provide the rationale as to why the requested Web site should be unblocked.

Elementary SLMS' willingness to tolerate the inconvenience of delayed access to blocked content may reflect their perspective that younger students are especially susceptible to indecent content and should have more restricted online access. This perspective was evident when Interviewee 3 commented, "Middle school and high school students may have the right to access more, but honestly I'm in elementary school, I'm still concerned about what's inappropriate."

Interviewee statements also indicate some end users may have been uncertain about unblocking procedures. According to Interviewee 4, there was an imperceptible link on the blocked page that provided unblocking instructions. The unblocking process, which took about one day, entailed sending an "email to a guy over a bunch of technicians." Since the unblocking link was not easily discernible, the SLMS stated, "I don't know how well it's [unblocking process] known."

Most survey and interview respondents described unblocking procedures that required users to submit a request and wait for content to be unblocked, sometimes for up to four weeks. To gain a better portrayal of how long users waited for content to be unblocked, SLMS survey item 4 asked participants how long users typically waited for unblocking requests to be granted. Figure 4 shows that in response to this survey item, 2.5% (N=3) selected immediately unblocked, 12.4% (N=15) selected less than 1 hour,

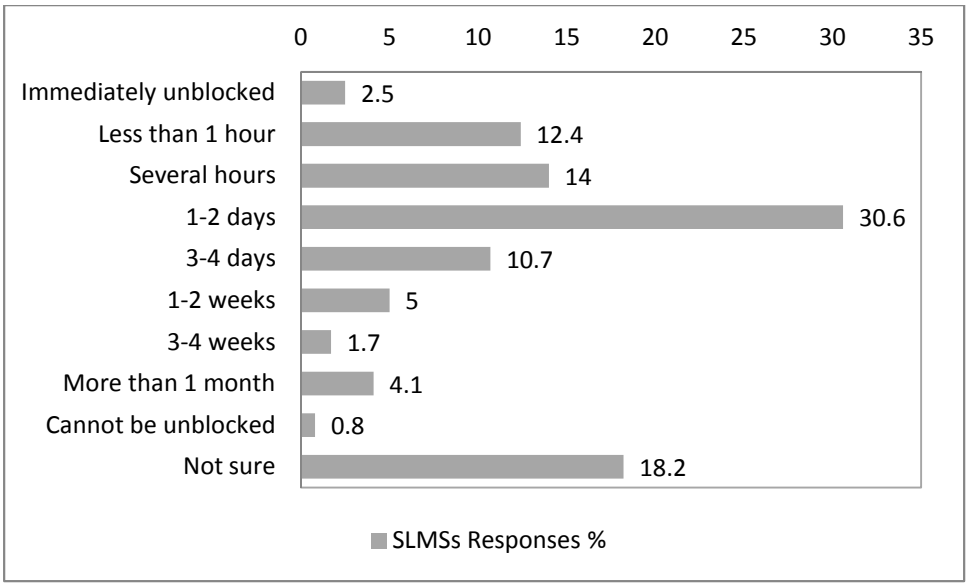

Figure 4. Timeliness of unblocking procedures.

14% (N=17) selected several hours, 30.6% (N=37) selected 1-2 days, 10.7% (N=13) selected 3-4 days, 5% (N=6) selected 1-2 weeks, 1.7% (N=2) selected 3-4 weeks, and 4.1% (N=5) selected more than a month. Figure 4 also shows that <1% (N=1) selected content cannot be unblocked and 18.2% (N=22) were unsure how long it took to unblock content. One explanation for the "not sure" selection could be that end users were not aware that content could be unblocked or had never submitted a request to unblock content. A large portion of respondents (66.6%) waited several hours or more to access blocked content, which meant blocked content was inaccessible at the point when end users needed it.

SLMS survey item 8d provided additional data about the efficiency of unblocking procedures. To assess further the efficiency of unblocking procedures, SLMS were asked whether they agreed that filter override procedures allowed timely access to blocked resources and information. In response to this item, 7.7% (N=9) strongly disagreed, 27.4% (N=32) disagreed, 35% (N=42) agreed, and 7.7% (N=9) strongly agreed that filter

override procedures allowed timely access to blocked content, while 22.2% (N=26) were neutral about the timeliness of unblocking procedures. Despite delays, more respondents (42.7%) agreed than disagreed (35.1%) that unblocking procedures provided timely access to blocked content. This suggests that many SLMS accepted delayed access to blocked content as an inevitable outcome of educators' obligation to protect students from online indecency.

Research Question 3

Research question 3 asked, "How are school districts addressing Web 2.0 safety issues?" To answer this research question, the investigator analyzed districts' AUPs to determine how they have been adjusted in response to Web 2.0 safety concerns and legislative mandates. SLMS and IT survey questions focused on the implementation of Internet safety education programs to address specific Web 2.0 safety issues. SLMS were also asked their opinions about the effectiveness of Internet safety approaches such as Internet safety education.

Safety Policy Adjustments in Response to Web 2.0 Safety Issues

The investigator reviewed safety policies (AUPs) from 80 of 81 traditional school districts in South Carolina to determine whether AUPs were addressing Web 2.0 safety issues via Internet safety education. The Protecting Children in the 21st Century Act (2008) required E-rate recipients to educate minors about Web 2.0 safety issues including interacting with other individuals on social networking Web sites and in chat rooms and cyber bullying awareness and response. The FCC required E-rate participants to include the Web 2.0 education provision in their safety policies by July1, 2012. Safety policies were examined to determine when they were last updated and for references to Web 2.0

safety issues, and for references to educating minors about Web 2.0 safety issues. Table 14 summarizes the data resulting from the safety policy analysis.

The safety policy analysis revealed that 66.6% (N=53) of school districts had updated their safety policies during the last three years (2010-2012), but only 45% (N=36) had updated them to include references to educating minors about Web 2.0 safety issues including interacting on social networks, in chat rooms and cyber bullying awareness and response. Of the safety policies that have been updated in the last three

Table 14. Web 2.0 Safety Policy (AUP) Adjustments

Web 2.0 Safety References	**Last Updated**									
	2010-2012		**2007-2009**		**2004-2006**		**1996-2003**		**Total**	
	%	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**
No references to Web 2.0, no references to educating minors	8.8	7	6.3	5	7.5	6	7.5	6	30.1	24
References Web 2.0 safety issues, but no references to educating minors	6.3	5	1	1	0	0	0	0	7.3	6
References instructing minors about appropriate Internet use, but no reference to educating minors about Web 2.0 safety	6.3	5	7.5	6	2.5	2	1	1	17.5	14
References educating minors about Web 2.0 safety issues, including interacting on social networks, in chat rooms and cyber bullying awareness and response	45	36	0	0	0	0	0	0	45	36
Total	**66.6**	**53**	**14.8**	**12**	**10**	**8**	**8.5**	**7**	**100**	**80**

years, 8.8% (N=7) made no mention of educating minors about Internet safety, 6.3% (N=5) referenced Web 2.0 safety (i.e., cyber bullying, social networking, etc.), but did

not mention educating minors about Internet safety; and 6.3% (N=5) referenced instructing minors about appropriate Internet use, but did not include Web 2.0 safety issues. When AUPs referenced Web 2.0 safety issues but made no reference to educating minors about Web 2.0 safety, they included statements such as "social networking sites are strictly prohibited." Twelve school districts (14.8%) last updated their AUPs during the 2007-2009 time period, none of which included references to educating minors about Web 2.0 safety issues. In this group, 6.3% (N=5) made no mention of educating or instructing minors about internet safety, 1% (N=1) mentioned Web 2.0 safety, but did not mention educating minors about Internet safety. Six (7.5%) AUPs mentioned instructing students about appropriate Internet use, but made no reference to educating minors about Web 2.0 safety issues.

Eight (10%) school districts last updated their safety policies during the 2004-2006 time period, none of which referenced educating minors about Web 2.0 safety. Six (7.5%) did not mention educating minors and 2.5% (N=2) included references to instructing minors about appropriate Internet use, but not specific Web 2.0 safety issues. Seven (8.5%) school districts last updated their AUPs during the 1996-2003 time period. Of these districts, six (7.5%) made no references to educating minors or to Web 2.0 safety, 1% (N=1) referenced instructing minors about appropriate Internet use, but made no mention of Web 2.0 safety. This safety policy analysis suggests that school districts were relying mostly on Internet filters to protect students and were not adjusting their AUPs in response to Web 2.0 safety concerns. Seventy-six percent of the safety policies that referenced Web 2.0 safety education were updated within the past year (2012), which implies that Web 2.0 safety education is in a state of flux and that district-wide safety

education is in the beginning phase of implementation. Twenty-seven (32.5%) districts have not updated their AUPs in more than three years, which suggests safety policies may not be the focus of Internet safety in these districts. This analysis, IT content blocking data, and SLMS responses to the blocked content item suggests that school districts are mostly blocking access to Web 2.0 resources to address Web 2.0 safety concerns.

Safety Education Implementation

IT survey item 8 and SLMS survey item 7e asked respondents if their school district had implemented an Internet safety education program. In response to this question, 39.8% (N=47) of SLMS replied yes, 41.5% (N=49) replied no, and 18.6% (N=22) were unsure about this question (see Table 15). Table 15 also shows that 90% (N=18) of IT respondents replied yes, 5% (N=1) replied no, and 5% (N=1) were unsure about this item.

Table 15. Internet Safety Education

Survey Item	**SLMS N=118**		**IT N=20**	
Survey Item 8 (IT), 7e (SLMS) The district has implemented an Internet safety program that educates students about appropriate online behavior, including social networking and chat room interactions, and cyber bullying awareness and response.				
Response	**%**	**N**	**%**	**N**
Yes	39.8	47	90	18
No	41.5	49	5	1
Unsure	18.6	22	5	1

Compared to the IT respondents, a smaller percentage of SLMS (39.8%) than IT respondents (90%) indicated that their school district had implemented an Internet safety education program to educate students about inappropriate online behavior, including

Web 2.0 safety issues. The difference in SLMS and IT responses to this survey item suggests these programs were not being implemented district-wide in many districts or that some SLMS may have been unaware of their district's Internet safety education program. Another possible explanation for the difference between SLMS and IT responses could be that some IT respondents viewed their AUPs as the district's Internet safety education program. IT survey comments in response to the Internet safety education item support this conclusion. For instance, one IT respondent commented, "The district has an Internet safety policy in place and we are currently updating [it] to include cyber bullying." Likewise, another IT respondent commented, "We will be implementing a cyber bullying policy and are already providing information to students and parents. We do have an acceptable use policy in place."

Interviewee and survey respondent observations clarify how Internet safety education was implemented in school districts. Overarching themes that emerged from analysis of these observations include lack of safety awareness programs, uncoordinated or passive Internet safety awareness efforts, uncertainty about safety awareness programs, and in a few situations, effective online safety awareness programs. Some respondent statements indicated that a district-wide Internet safety awareness program had not been adopted and implemented. Regarding district-wide safety education programs, Interviewee 1 commented, "There's nothing in place." The SLMS' comments suggest teachers and media specialists were expected to educate minors about Internet safety, but had not been provided specific guidelines or a curriculum. The result was haphazard Internet safety education efforts as was evident when Interviewee 1 commented, "I do digital citizenship units of instruction with the kids. The district leaves it up to media

specialists and teachers. If they [teachers and media specialists] say it's not important, they don't do it." Similarly, a SLMS survey respondent commented, "An internet safety education program is not mandatory at all schools in the district. Each school initiates its safety education program."

Other respondents were uncertain whether a district-wide Internet safety awareness program had been adopted and implemented. For example, Interviewee 4 stated, I don't know what the computer and keyboarding classes are doing. I can't tell you." Uncertainty was evident when Interviewee 4 stated, "…there's no official course or online training program. Librarians haven't been told officially about it. Maybe computer and business classes have a program, but I'm not aware of any." The school district had made passive efforts to inform students about online safety, but these efforts did not involve direct instruction. The SLMS stated, "A while back, a group including media specialists developed posters on Internet safety and ways to stay safe on the Internet. These posters were displayed in classrooms." Interviewee 4 also described a more recent district-wide effort to inform student about online dangers when she stated, "We also had something this year, some information about bullying and online bullying explaining how to protect yourself online. This came from the district. It was an instructional thing to put in your room."

Uncertainty about district-wide cyber safety education programs was apparent when Interviewee 5 stated, "The only thing that I know they do is that we have a one-day program in the freshman 101 class where the technology integration specialist does a jeopardy game on Internet safety." District-wide efforts to educate minors were uncoordinated and sporadic as was evident when Interview 5 reported, "…students also

get a little bit of instruction when they pick up their iPad devices. Teachers sporadically address Internet safety, but it is not addressed district-wide." Uncertainty was also apparent when a SLMS survey respondent commented, "I am not sure if there is a program created by the district to address these concerns." Regarding district wide efforts to implement cyber safety education, the respondent' explained, "[The] media specialist includes such information during our lessons on Internet use. Board policies are in effect, but teachers are responsible for sharing that information with students." This explanation implies uncoordinated Internet safety efforts as there is no mention of an Internet safety program or district mandated cyber safety curriculum.

On the other hand, a few participants' statements suggest their districts had issued clear Internet safety education guidelines or had adopted a formal Internet safety curriculum. For example, Interviewee 2 remarked, "We were given a requirement as of last year saying we have to have a formal program in place and we had to have proof that every child is educated every year." Interviewee 2's school also made efforts to involve parents by sending a flyer home and advertising Internet safety programs on the school's Web site. Similar to Interviewee 2's observation, parental involvement was a key part of the Internet safety program Interviewee 3 described. According to Interviewee 3, the district Internet safety program "provides instruction for kids and workshops for parents." The SLMS considered the program to be effective as the statement, "It's a good one," suggests.

IT survey respondent observations indicated Internet safety education was in various stages of implementation. One IT respondent reported that the district had implemented a multi-level program entitled, "NetSmartz from [the] Center of Missing

and Exploited Children." Another IT responded stated, "This is in [the] planning stages with implementation scheduled at the beginning of next school term." The latter statement implies that up to this point some school districts may have been relying mostly on filters for Internet safety instead of using multiple Internet safety approaches, including a fully integrated district-wide safety education program.

The literature review suggested that multiple Internet safety approaches are required to prepare students to be safe and responsible Internet users, particularly in unfiltered environments. To ascertain the effectiveness of district-implemented Internet safety approaches, SLMS survey item 8f asked respondents whether they agreed that filtering and safety policies/practices (i.e., AUPs, Cyber safety education, monitoring, etc.) prepared students to be safe and responsible users in unfiltered environments. In response to this item, 10.3% (N=12) strongly disagreed, 23.9% (N=28) disagreed, 38.5% (N=45) agreed, 6.8% (N=8) strongly agreed while 20.5% (N=24) were neutral about this item. Fewer than half of SLMS respondents (45.3%) agreed or strongly agreed that their district's Internet safety approaches effectively prepared students to make safe and responsible decisions while using online resources. Interview participant observation enabled a better understanding of factors that contributed to ineffective Internet safety approaches. Moreover, interviewee observations detail factors that contribute to effective Internet safety approaches.

Some interview participant observations support the safety policy analysis findings. Their observations suggested that current Internet safety efforts relied mostly on filters to keep students safe, which resulted in overly restrictive filtering policies, uncoordinated Internet safety education efforts, or minimal emphasis on AUPs. When

Interviewee 5 stated, “They [the district] have the mindset that if we block all the bad stuff, they don’t have to worry about teaching Internet safety,” the remark implied the district was relying mostly on strict filtering policies to protect students from online indecency instead of instructing students about online safety. Interviewee 4 was concerned that reliance on strict filtering policies interfered with efforts to educate students about online safety. She used the following thought-provoking analogy to convey her concern:

> You can have all the safety education you want, but if everything is blocked, we can’t train them on how to be safe online. It’s like teaching first graders and kindergartners all about scissor safety, but never putting scissors in their hands so they can practice cutting. We’re blocking so much that we can’t practice. For instance students don’t have email, can’t access blogs, forums. We can’t teach safety when they can’t access these online tools.

Other interview participants suggested their school districts were minimizing the importance of AUPs as an Internet safety approach. For instance, Interviewee 1 remarked, “They [the district] started something new, they’re saying more and more we don’t need that [signed AUPs]. Students don’t sign AUPs anymore, they did away with that saying it’s too much paperwork.” Likewise, minimal use of AUPs to promote Internet safety was implied when Interviewee 4 stated, “We have a great AUP that nobody knows about in the student handbook. Students are not required to sign any forms.” Interviewee 4 added, “In the handbook there’s one page that talks about the Internet. The handbook is sent home for parents to read, they contact the school if they have questions or concerns,” which suggested efforts to involve parents in Internet safety

was not proactive. It can also be construed that few students or parents read the AUP because the policy did not require students' or parents' signatures.

The aforementioned participant observations highlighted factors contributing to ineffective Internet safety strategies in school districts. Nevertheless, some participants described effective Internet safety approaches in their districts. Constant reinforcement of digital citizenship guidelines was a common theme that emerged when participants described effective district-wide Internet safety education programs. When asked what factors contributed to the success of their district's Internet safety program, Interview participant 3 replied, "The program they [the district] use is not a stand-alone lesson, there're projects. It's not like a one-time thing. Internet safety is constantly reinforced." Interview participant 2 replied, "Safety education is reinforced in the library and the computer lab." Similar survey respondent comments include: "We have a strong Internet safety program in place for our students and clear guidelines for our teachers and staff," and "The media specialist goes over Internet safety constantly."

Interviewee observations exemplify other factors that contribute to effective digital citizenship practices, including stakeholder involvement in Internet safety program implementation and integrated district-wide Internet safety efforts. When Interviewee 5 remarked, "It [Internet safety] probably should be integrated into every course, and [there] should be a system-wide plan to teach and reteach this thing of Internet safety and etiquette," it suggested integrated district-wide Internet safety instruction was an important factor in implementing effective Internet safety programs. Interview observations also suggest stakeholder involvement in program development is a critical component of effective Internet safety program implementation. Interviewee 5 asserted

that district Internet safety efforts were ineffective because instructional staff were not involved in policy decisions. The SLMS explained, "….the people who are making the decisions are not instructional staff, but are technicians." The need for stakeholder involvement in Internet safety program implementation was echoed in other interviewee comments. Interview 1 stated, "They need to involve media specialists; we've got to be involved in that process." Similarly, Interviewee 4 stated, "There needs to be more input from people who are teaching the students." Interviewee 3, who viewed her district's Internet safety program as "…a good one," described how stakeholders were involved in the program's implementation. The SLMS stated, "It's a specific thing [program]. The technology teachers got with the district office to choose what they'll use."

Interviewee observations, survey data, and the AUP analysis suggest Internet safety education has not been a major focus of Internet safety policies. Safety policies (AUPs) have not evolved to encompass 21st century computing technology and its inherent safety issues as the following Interviewee observations suggest: "…policies have not kept up with what it means to be a 21st century learner," (Interviewee 1) and "...the district's Internet use policies reflected a 1980's mentality" (Interviewee 4). Interviewee observations also suggest that when safety education is implemented with stakeholder involvement, on a district-wide basis, and reinforced often, it can be an effective Internet safety approach.

Research Question 4

Research question 4 asked, "In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?" The standards that were the focus of this question include the

communication and collaborative standards identified in Table 3. To answer this question, IT and SLMS survey items sought to determine whether Web 2.0 resources, which promote the acquisition of communication and collaborative skills, were accessible or blocked. Question set 5 on the interview protocol also sought to define specific Web 2.0 access issues and safety concerns that prompted administrators to limit access to this content.

To discover how filters impeded access to Web 2.0 resources, wikis, blogs, and social networking sites, were included as content categories in IT survey question 4. Table 8 shows that 23.1% (N=3) of responding school districts filtered all wikis and blogs, 69.2% (N=9) filtered some wikis and blogs, while 7.7% (N=1) filtered no wiki/blog content. The majority (58.8%; N=10) of school districts blocked all social networking tools, 41.2% (N=7) blocked some, and there were no school districts that did not block all or some social networking sites. To ascertain how filtering policies influenced end user access to Web 2.0 tools, SLMS survey item 3 asked respondents to select the types of educational content that were most often over-blocked. Web 2.0 content was one of the answer choices for this item. Seventy-eight (66.7%) SLMS said Web 2.0 resources were over-blocked in their school districts (see Figure 3).

SLMS were also asked whether they agreed that their district's filtering and safety policies facilitated easy access to online collaboration and communication tools (Web 2.0). Eighteen (15.8%) SLMS strongly disagreed, 30.7 (N=35) disagreed, 24.6% (N=28) agreed, and 4.4% (N=5) strongly agreed that their district's filtering and safety policies facilitated easy access to Web 2.0 resources. Twenty-eight respondents (24.6%) were neutral about this item. A greater portion of SLMS strongly disagreed/disagreed (46.5%)

than agreed/strongly agreed (39.9%) that their district's filtering and safety policies facilitated access to communication and collaboration tools. IT and SLMS survey data inferred that district-implemented filtering policies impeded access to many Web 2.0 resources necessary for attainment of 21st century learning skills.

Additionally, impeded access to Web 2.0 resources was a recurring theme of interview participant observations. Interviewees were asked if Internet access policies or practices limited access to Web 2.0 tools that foster online communication and collaboration. Interviewee responses described specific communication and collaboration tools that were inaccessible. Interviewee 5 stated, "There's no Twitter™, no Facebook™, and no YouTube™." The media specialist also described sporadic access to Wordle™ when she stated, "Its sporadic, sometimes we get access, sometimes we can't." Interviewee 4, whose statements: "The only Web 2.0 tools we're able to access is Edmodo™," and "We just can't get to anything," also suggest very limited access to online communication and collaboration tools.

Even when access to specific Web 2.0 tools was allowed, some features of these sites were disabled. For example, Interviewee 5 stated, De.lic.ious™ is available, but for some reason they block the toolbar icon that allows you to add a Web site to your account." Interviewee 1, who recounted a similar experience involving disabled Web 2.0 features, stated, "When we use Web 2.0 tools, email capability is blocked. Students can't send articles to their personal email addresses."

If interview respondents indicated their district's Internet use policies restricted access to Web 2.0 resources, they were also asked to explain how these policies limited attainment of 21st century information literacy and technology standards. Interviewee

responses suggest that restricted Web 2.0 access limited opportunities for students to interact appropriately with others, to create content, connect with experts, and become self-directed learners. Interviewee 4 stated, "….students aren't getting to practice interacting appropriately with people on a live interaction tool," which illustrated how restricted Web 2.0 access limited opportunities for students to interact appropriately. When Interviewed 4 stated, "They [students] can't create content, aren't learning how to use that," the remark implied that Web 2.0 access policies limited opportunities for students to create and share content.

Interviewee observations also described how Web 2.0 access policies restricted individual student collaboration. For example, Interviewee 4 stated, "Web 2.0 makes it easy to connect with experts, but students are almost stuck with letter writing. They can be communicating with authors or chemists, but that's not happening because they can't access the online communication tools." Interviewee 5, who described similar Web 2.0 access restrictions, reported, "District policies restrict collaboration with others outside of the district." The district's technology policy allowed teacher access to collaborative tools, but prevented students from accessing these tools. Interviewee 5 defined how this access policy limited opportunities for student interaction when she remarked, "If the teacher wants to collaborate with another class, she can only do it using the teacher's account. I think our students should get the same opportunity to do it [collaborate] individually." Interviewee 1 was concerned that restricted Web 2.0 access limited opportunities for students to become self-directed learners. The SLMS stated, "The district says we're supposed to develop self-directed learners, we're supposed to be

teaching them to be self-directed. She questioned, “How can students be in charge of their own learning if all these restrictions are in place?”

Student safety had a substantial influence on content blocking decisions as Table 9 illustrates. When asked what safety concerns prompted policymakers to restrict Web 2.0 access, interview participants’ responses convey administrators’ concerns about student safety. Interviewee responses include the following recurring student safety issues: cyber bullying, online predators, and posting inappropriate content online. Interviewee 4 stated, “They’re [policymakers] worried about cyber bullying; they’re afraid that a student will email inappropriate messages and do inappropriate things that would put a bad mark on the school.” Interviewee 2 added that policymakers’ “biggest concern is bullying and students getting in contact with someone not at school who might be a predator.” Interviewee 5 indicated that policymakers restricted Web 2.0 access because of “all the stuff on the news about somebody being lead to meet with somebody online. Interviewee 5 further explained that policymakers were “afraid that kids will post inappropriate things; they’re worried about inappropriate verbiage and a whole list of things.” These statements call attention to the inherent safety issues that accompany Web 2.0 usage. In response to these concerns, policymakers have mostly used a one-dimensional Internet safety approach; block access to potentially unsafe content or controversial content, including Web 2.0 resources. Interviewee 3 likened this Internet safety approach to “throwing out the baby with the bathwater.”

Some data indicates that policymakers are beginning to realize the educational benefits Web 2.0 resources afford. Though initially subjected to wholesale blocking, Web 2.0 resources were becoming more accessible for students and teachers in some school

districts. Regarding increasing Web 2.0 access, Interviewee 2 reported, “I noticed that access denials or blocks have opened up more.” Interviewee 2 named specific Web 2.0 tools that had become available for instructional use, including SharpSchool™ and Edmodo™. The SLMS suggested that Web 2.0 access for students was also becoming less restricted when asserting, “Access has been restricted more for students, but it’s beginning to open up.” Similarly, Interviewee 1 explained, “They’re [district administrators] starting to relax policies, but I’d love to be able to email articles to students’ personal email addresses.” The following SLMS survey comment illustrates that increased Web 2.0 access is an evolving process requiring communication between educators and administrators, some trial and error, and clear usage guidelines:

> We initially had and still have some difficulties in utilizing Web 2.0 tools, but are working with IT and the administration on these issues and use of certain tools, some being very open now and others requiring more tests and/or supervisory guidelines (SLMS Survey Comment).

Interviewee 3’s school district was beginning to embrace social networking and online collaboration as well. However, limited student access to Web 2.0 resources was an issue. Interviewee 3 described this issue and district plans to expand students’ access in the following statement:

> We do the social networking thing. We do collaborative projects with people at different schools. There’s a bigger problem though. We Skype™ under the umbrella of the teacher login, but that’s something that’s going to be addressed. The school district is going to be using Google™; everyone will have Google™

> accounts. As a whole the district will embrace Google™ docs and other Google™ communication apps. (Interviewee 3)

Some of the aforementioned SLMS observations described limited access to a variety of Web 2.0 resources, which inhibited communication and collaboration within and outside of school. However, some districts were loosening restrictions on Web 2.0 tools, but access was still hampered by access issues such as staff-only Web 2.0 access policies, which prevented individual student collaboration and communication. The integration of Web 2.0 resources into instruction was also hampered by disablement of features on some sites, including email capability and toolbar features that enable users to add Web sites to their accounts. Overall, survey and interview data regarding Web 2.0 access suggest that many end users were denied opportunities to develop 21st century communication and collaboration skills because of restricted access to the read and write Web.

Comparison of Elementary and Secondary School Access Issues

The investigator compared elementary (K-5) and secondary (6-12) SLMS responses on survey items about content access issues such as over-blocking to ascertain how filtering policies affected users in each academic group. If SLMS survey respondents indicated that their school included any grade level beyond grade 5, they were included with the secondary group. Figure 5 shows that a greater percentage of secondary SLMS than elementary SLMS encountered over-blocking in all but one content category, educational games. The percentage difference between secondary SLMS and elementary SLMS experiencing over-blocked visual images, virtual worlds, heath/sex education content, and other content was greater than 10 percentage points. For

these content areas, 43.8% of secondary SLMS and 26.4% of elementary SLMS experienced over-blocking of virtual world content, 50% of secondary SLMS and 39.6%

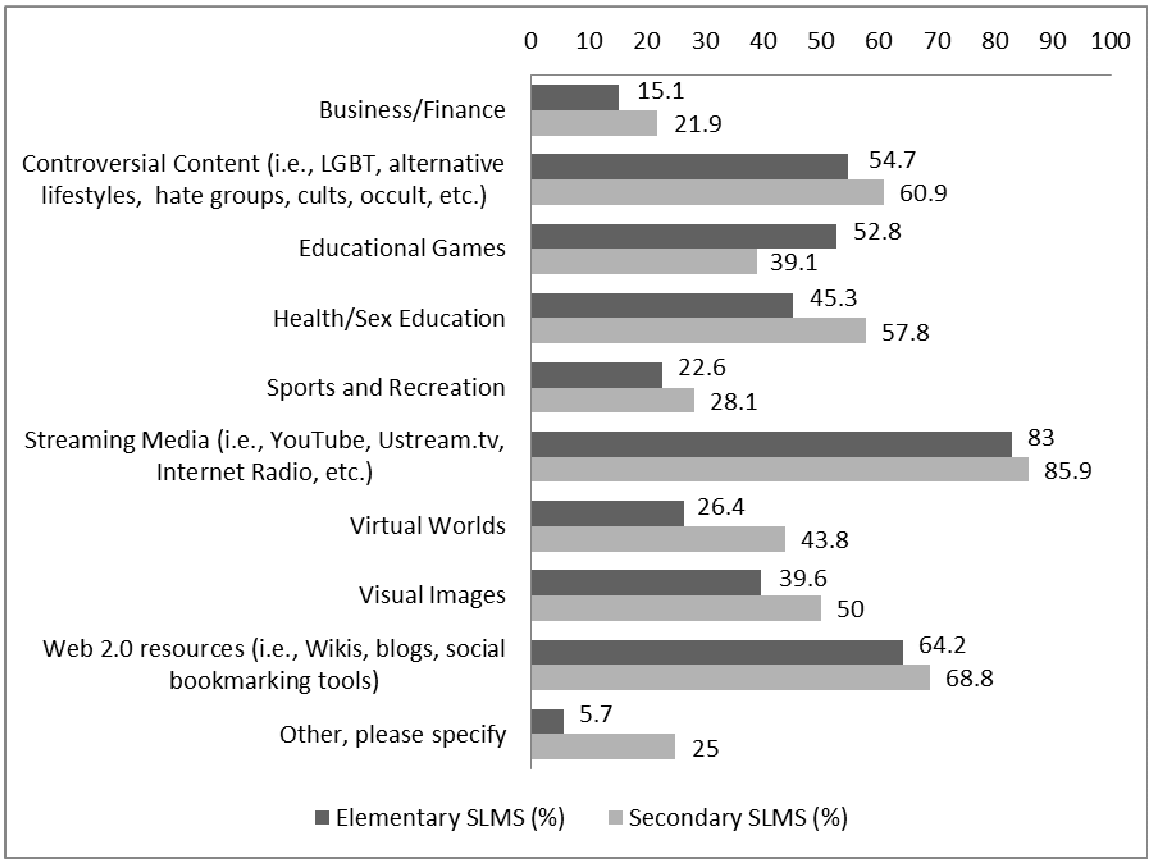

Figure 5. Comparison of elementary and secondary school access issues.

of elementary SLMS experienced visual image over-blocking, and 57.8% of secondary and 45.3% of elementary SLMS experienced health/sex education content over-blocking. Twenty-five percent of secondary SLMS compared to 5.7% of elementary SLMS experienced over blocking of other content, such as popular culture, entertainment, online ordering/shopping (i.e., school supply sites), and educational sites including Scholastic.com and PBS.org. A greater proportion of elementary SLMS (52.8%) than secondary SLMS (39.1%) encountered blocked educational games. This data suggests that elementary users need greater access to education games and secondary users need

greater access to virtual worlds, visual images, health/sex education subject matter, and other specified content.

Compared to secondary SLMS, a smaller percentage (5-10 percentage points smaller) of elementary SLMS indicated that business/finance, sports/recreational, and controversial content was over-blocked. Fourteen secondary SLMS (21.9%) and 15.1% of elementary SLMS reported instances when business and financial content was over-blocked. A larger portion of secondary SLMS (28.1%) experienced blocked sports and recreational content while a smaller portion of elementary SLMS (22.6%) experienced blocked content in this domain. This finding hints that secondary users have a greater need for business/financial and sports/recreational content. The majority (more than 50%) of both groups experienced blocked controversial content; however, more secondary (60.9%) than elementary (54.7%) SLMS indicated controversial content was over-blocked. The fact that the majority of both academic levels encountered blocked content of this nature could be construed that both academic levels require greater access to subject matter that filters categorize as controversial.

Figure 5 shows that streaming media over-blocking and Web 2.0 over-blocking occurred with a majority of both groups, as compared to every other content area except controversial subject matter. However, the percentage difference between the elementary and secondary SLMS is less than five percentage points for both content areas. Streaming media content was over-blocked for 83% of elementary SLMS and 85.9% of secondary SLMS. Web 2.0 resources were over-blocked for 64.2% of elementary SLMS and 68.8% of elementary SLMS. This data suggests that over-blocking is an issue with both

academic levels, and that filtering policies need to be adjusted to allow greater access to streaming media content and Web 2.0 resources.

Table 16. Comparison of Secondary and Elementary SLMS' Perceptions of the Influence of Filtering/Safety Policies on Instructional Staff

Survey Item	Elementary SLMS		Secondary SLMS	
SLMS Survey Item 8a **The Internet filter prevents instructional staff from accessing resources needed for instructional or professional activities.**				
	N=52		**N=66**	
Response	**%**	**N**	**%**	**N**
Strongly disagree	5.8	3	1.5	1
Disagree	30.8	16	13.6	9
Neutral	9.6	5	10.6	7
Agree	46.2	24	54.5	36
Strongly agree	7.7	4	19.7	13

Secondary and elementary SLMS' perceptions about the influence of filtering policies on end user access to online content was compared to ascertain whether one user group experienced more access issues. As Table 16 shows, a greater proportion of secondary SLMS (74.2%) than elementary SLMS (53.9%) agreed/strongly agreed that district filtering policies prevented instructional staff from accessing resources needed for instructional or professional activities. Likewise, Table 17 shows that a greater portion of secondary SLMS (60.6%) than elementary SLMS (34.6%) agreed/strongly agreed filtering policies prevented students from accessing information and resources needed for classroom assignments. When asked whether they agreed that filtering and safety policies facilitated easy access to online collaboration and communication tools (Web 2.0),

Table 17. Comparison of Secondary and Elementary SLMS' Perceptions of the Influence of Filtering/Safety Policies on Students

Survey Item	Elementary SLMS		Secondary SLMS	
SLMS Survey Item 8b **The Internet filter prevents students from accessing information/resources needed for classroom assignments.**				
	N=52		**N=66**	
Response	**%**	**N**	**%**	**N**
Strongly disagree	7.7	4	4.5	3
Disagree	36.5	19	21.2	14
Neutral	21.2	11	13.6	9
Agree	30.8	16	48.5	32
Strongly agree	3.8	2	12.1	8

a greater portion of secondary SLMS (53.9%) disagreed/strongly disagreed than elementary SLMS (36.7%) (see Table 18). This data analysis indicates filtering and safety policies were having a more adverse effect on secondary users' access to educational information. The data also implies that secondary users need greater access to online content.

Table 18. Comparison of Secondary and Elementary SLMS' Perceptions of the Influence of Filtering/Safety Policies on Web 2.0 Access

Survey Item	Elementary SLMS		Secondary SLMS	
SLMS Survey Item 8e **Filtering and safety policies facilitate easy access to online collaboration and communication tools (Web 2.0)**				
	N=49		**N=65**	
Response	**%**	**N**	**%**	**N**
Strongly disagree	6.1	3	23.1	15
Disagree	30.6	15	30.8	20
Neutral	24.5	12	24.6	16
Agree	34.7	17	16.9	11
Strongly agree	4.1	2	4.6	3

Interviewee statements support the foregoing supposition that filtering restrictions need to be relaxed for older students to allow greater access to online content.

Interviewee 4 suggested that high school students' maturity level enabled them to make better decisions about online content; therefore, high school students should have greater access to online content. The SLMS stated, "I think you should treat high school students pretty close to adults. It's the same with a Website as with a book. Just like they put down a book they don't like, they can do the same with a Website." Interviewee 5 also believed there was a difference in the maturity levels of elementary and secondary students. The SLMS explained, "There's a difference between high school students and elementary students. Things blocked for elementary can be released with no detrimental effect on high school students."

Interviewees 2 and 3, who were elementary SLMS, also acknowledged that elementary and secondary students had different information needs. Interviewee 2 explained that at the elementary level there were fewer unblocking requests, but was certain that "high schools and middle schools get more requests." When Interviewee 2 stated, "…you're probably going to see a big difference between middle and high school media specialists," it was further acknowledgement of the differences in elementary and secondary users' information access requirements. Interviewee 3 also acknowledged that secondary and elementary students have different information requirements when recommending that, "Filter access levels should be tiered so they [high school students] can have access to more."

The foregoing interviewee observations confirm that elementary and secondary level students have dissimilar information needs and maturity levels, which suggests that a one-size-fits-all filtering scheme may not be the best filtering approach for elementary and secondary students. Moreover, a comparison of elementary and secondary SLMS'

survey responses supports the need for fewer restrictions on Internet access at the secondary level.

Attitudes about Filtering and Safety Policies

During the course of this investigation, other themes emerged that demonstrate how end users reacted to filtering policy implementation. A thematic analysis of interviewees' and survey respondents' comments revealed end users' attitudes about district-implemented filtering and safety policies. These attitudes include acquiescence, tolerance, and frustration. Some end users have acquiesced to Internet filter implementation and accept restrictive filtering policies as an unavoidable consequence of legal and social mandates to protect students from harmful online content. As Table 19 shows, some end users acknowledged the technology's over-blocking tendency, but were willing to accept restrictive filtering policies without objection (AR1, AR2, & Interviewee 3).

Other users tolerated restrictive filtering policies while seeking alternative ways to access or utilize blocked educational content. These users applied work-around strategies to access blocked educational content, such as downloading blocked content in advance (AR3), finding similar unblocked content (Interviewee 1), and using staff logins and a projector to share blocked content with students (Interviewee 5). Other respondent observations revealed an unwillingness to accept filtering policies as they were implemented (AR4, Interviewee 1). Frustration about current filtering policy implementation was evident in the use of words like "annoying," "aggravating," and "upsetting." The attitudes summarized in Table 19 provide additional substantiation of the issues users encountered as they sought information in a filtered environment.

Table 19. End User Attitudes about Filtering Policies

Attitude/Reaction	Participant Statements Exemplifying Attitude/Reaction
Acquiescence	It is very hard to find good clip art but I also understand how easily students can find inappropriate images so I try not to get too frustrated with that content being blocking. (AR1)
	You can request an override, but I have never done it. I respect their [administrators] decisions and endeavor to set a positive example for the students. (AR2)
	I don't see it [filtering software] as a problem anymore. It's evolved to the point where I feel as if it's more of a friend than a roadblock. (Interviewee 3)
Tolerance	Teachers should have downloaded what they need for their lessons. We all know the filter is in place. The filter cannot catch everything. (AR3)
	If something is blocked and the students can't get to it, sometimes the teacher can login to it on her computer. They all have projectors so they can share the sites with their students. (Interviewee 5)
	They [end users] use other means such as using another Web site. They just keep trying until they come up with something that is not blocked. (Interviewee 1)
Frustration	Not having access to Scholastic.com is annoying. As a librarian, not being able to jump onto Amazon.com or sometimes bn.com [Barnes and Noble] is very aggravating. (AR4)
	It's upsetting that they [administrators] don't respect my professional integrity. (Interviewee 1)

Note: AR=Survey Respondents' Attitude/Reaction

Summary of Results

This chapter presented the results of the quantitative and qualitative research undertaken for this investigation. This study endeavored to describe how filtering and safety policies were being implemented in South Carolina's K-12 public schools. This investigation also sought to describe how filtering and safety policies influenced end users' access to information. Data collected from IT and SLMS surveys, an interview

protocol, and an analysis of artifacts (AUPs) were combined to answer each research question.

Survey and interview data provided insight into the issues surrounding filtering and safety policy implementation in South Carolina's public schools. Regarding the implementation question and content blocking considerations, IT survey data indicated policymakers were electing to block considerably more Web content than online obscenity. Several factors influenced filtering decisions, the three most influential being CIPA compliance, maintaining student safety, and maintaining network security. IT and SLMS survey data and interview observations suggest that in most school districts, school-based stakeholders had minimal input in policy decisions. The research results revealed many school districts were implementing differentiated access levels for staff, but all students, regardless of age level, had the same access level.

Survey and interview results were combined to portray the issues SLMS encountered as they facilitated information access in a filtered environment. Survey data revealed that filters were effective in protecting students from inappropriate content, but overly restrictive filtering policies prevented most end users from accessing controversial subject matter, streaming media, health and sex education resources, and Web 2.0 tools. Interview data supplemented survey findings by providing concrete scenarios in which filtering policies denied end users access to educational resources. In addition to the over-blocking issue, end users also encountered inefficient content unblocking procedures. Bureaucratic and poorly communicated unblocking procedures and lack of on-campus override privileges delayed access to blocked content.

An analysis of school districts' AUPs coupled with survey and interview data revealed that school districts were relying mostly on filters to protect students from online indecency. The majority of school districts have not adjusted their AUPs to include educating minors about Web 2.0 safety issues, as the Protecting Children in the Twenty First Century Act (2008) requires. Survey and interview data also suggests that Internet safety education is not an important Internet safety approach in many school districts. Over-reliance on filters to protect students from Web 2.0 safety issues has resulted in restricted access to Web 2.0 resources that enable students to acquire 21st century communication and collaboration skills. In essence, the research results show that school districts' filtering and safety policies were mostly outdated, and have not kept pace with 21st century online technologies.

The researcher compared elementary and secondary SLMS responses on survey items specifically related to how Internet use policies influenced end users, including students and instructional staff. Elementary and secondary user groups encountered the adverse effects of overly restrictive filtering policies, but these adverse effects were more pronounced at the secondary level. Over-blocking was more prevalent among secondary users, suggesting that their information needs require access to more of the content that filters typically classify as controversial, potentially liable, or non-educational. Considerable over-blocking occurs when filters are set to block such content.

Overall, school districts have mostly implemented a one-dimensional and one-size-fits-all approach to Internet safety through the application of unnecessarily restrictive

Internet filtering policies. The outcome was frustrated end users with limited access to resources enabling them to experience fully the Internet's many educational benefits.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

This mixed method study examined school districts' implementation of Internet filtering and safety policies and the influence of these policies on end users' access to information. Quantitative and qualitative data collected during the course of this study, provided insight into each of the research questions that guided the study. This chapter will present the conclusions and implications of the research in addition to the recommendations that evolved from analysis and interpretation of the data. Finally, a summary of the dissertation will be presented.

Conclusions

The problem that launched this study was the need for a comprehensive examination of Internet filtering and safety policies to determine how they were influencing information access in South Carolina's K-12 public schools. Specifically, this research sought to detail filtering and safety policy decision making and factors that influenced policy decisions. Internet use policies can be implemented in a manner that either maximizes or minimizes user access to information. Therefore, this research investigated end users' experiences with content over-blocking, content under-blocking, and unblocking practices to determine how these factors influenced teaching and

learning. This investigation also examined the trends and issues surrounding Web 2.0 safety, and the role of filtering, AUPs, and Internet safety education in protecting students from inappropriate online content. Finally, filtering policies were examined to ascertain the manner in which they impeded access to Web 2.0 tools enabling students to hone 21st century collaboration and communication skills. This research provides answers to the aforementioned inquiries. These answers were gleaned from stakeholder groups who were keenly aware of how filtering and safety policies were developed and implemented (IT directors) and the resulting effect of these policies on teaching and learning (SLMS). The conclusions from each of the four research questions will be presented following a brief description of the methodology used to obtain the data.

Research Question 1

Research question 1 asked, "How are filtering and safety policies being implemented in public schools?" To answer this question, survey and interview items focused on three filtering and safety policy implementation issues (variables) that were identified in the literature review (see Table 4). These variables include content blocking considerations, stakeholder involvement in policy decisions, and differentiated access levels for specific user groups. One of the most important policy considerations is deciding what content to block and the level of blocking within each category. An important conclusion drawn from the IT survey data was that in implementing filtering policies, school districts were deciding to block more content than CIPA requires. CIPA requires E-rate discount recipients to filter access to visual images that are obscene, child pornography, or harmful to minors. As E-rate recipients, this mandate applied to all school districts from which the research data was collected.

School districts' decisions to block more than CIPA requires may be explained by the factors that influenced filtering decisions. CIPA compliance had the greatest influence on content blocking decisions. The decision to block more than CIPA requires may be due to misinterpretation of CIPA's guidelines or other factors. With the exception of CIPA compliance, concern for student safety was the most influential factor in filtering policy decisions. Policymakers' concerns about student safety likely lead them to block perceived threatening content such as weapons, violence, alcohol, tobacco, gambling, drugs, criminal, and other illegal content. Maintaining network security and bandwidth preservation were also highly influential on filtering decisions, which may explain why most districts filtered access to hacking, proxy avoidance, and malicious sites in addition to Internet radio/TV, telephony, and media downloads. Concerns about litigation exerted considerable influence on policymakers' filtering decisions as well, which most likely influenced them to filter controversial content such as alternative lifestyles, hate, racism, cult, occult, sex education, and intimate apparel. Although preventing non-educational use and community/parental opinions exerted less influence on filtering decisions than the aforementioned factors, both factors had a considerable influence on filtering decisions. Community pressures and the need to prevent non-educational use could possibly explain why school districts blocked content such as wikis, blogs, and Web-based email, and contributed to decisions to block controversial content.

A prevailing supposition from survey and interview data is that filtering policy decisions were mostly made by district administrators, IT staff, and the filtering software (the software's default/recommended settings are deployed). End user stakeholder groups such as SLMS, teachers, students, or school-based administrators had little input in

filtering policy decisions. Conversely, when asked if the filter's default setting was deployed, most IT respondents indicated the filter's default setting was not implemented. These competing results suggest that districts began filter implementation with the filter's default setting and modified these settings as needed. Nevertheless, end user input in filtering policy decisions was mostly limited to suggesting Web sites that should be blocked or unblocked after the filtering solution had been implemented.

The establishment of differentiated user profiles to meet the research, educational, and professional needs of all user groups was another consideration under investigation. Although districts had implemented some differentiated access levels, they were not tailored to the needs of all user groups, or to provide maximum access to online content. For instance, some SLMS could access Web 2.0 content and YouTube, but other instructional staff could not access this content. In other instances, content such as YouTube was unblocked for staff after school hours, but blocked during the school day and unavailable for instructional purposes. Differentiated access levels were not established to meet the educational and research needs of various student age groups, such as elementary, middle, and high school groups.

School districts have implemented overly restrictive filtering policies mostly without the input of the stakeholders with firsthand knowledge of student and staff information needs. Moreover, minimal steps were taken to tailor filtering policies to the needs of specific user groups.

Research Question 2

Research question 2 asked, "What issues do SLMS encounter as they facilitate information access on filtered computers?" To answer this question, the data collection

instruments focused on filtering issues that were identified in the literature (see Table 4). To determine the scope of these issues and the way they affected teaching and learning, survey and interview data were collected about filter over-blocking frequency, under-blocking frequency, filter effectiveness, specific types of blocked educational content, and the efficiency of unblocking procedures.

The data provided a portrayal of the issues SLMS encountered as they facilitated information access on filtered computing devices, the most prevalent of which was filter over-blocking. A large majority of IT directors received requests to unblock erroneously blocked educational content, but only a few received unblocking requests on a frequent basis. A similar majority of SLMS indicated filters over-blocked educational content, and almost half of SLMS respondents said over-blocking was a frequent issue. End users' acquiescence to and tolerance of filtering policies most likely resulted in fewer unblocking requests. Lack of awareness of unblocking procedures could also have contributed to fewer unblocking requests. These factors may explain why so few IT administrators frequently received requests to unblock resources while many more SLMS frequently encountered over-blocked educational content.

An investigation into the types of blocked content provided furthered understanding of the types of filtering issues end users experienced. Most end users encountered blocked controversial content such as alternative lifestyles, hate groups, cults, and the occult. Most end users experienced blocked streaming media, health and sex education, and Web 2.0 content as well. Slightly fewer than half encountered blocked educational game and visual image sites. Over-blocking of the aforementioned subject matter is directly related to policymakers' decisions to filter all or some potentially liable

content categories such as alcohol/tobacco, criminal/illegal, cult/occult, drugs, gambling, hate/racism, social networking, sex, education, Internet radio/TV, and VoIP.

The results of the abovementioned content being over-blocked were far-reaching. Instructional staff was prevented from accessing resources needed for instructional or professional activities, and students were prevented from accessing information and resources needed for classroom assignments, according to most SLMS respondents. This effect was particularly acute at the secondary level according to a comparison of elementary and secondary SLMS' responses. However, over-blocking occurred at all academic levels. Specifically, teachers were unable to carry out lessons they planned at home because content accessible at home was blocked at school. Students also encountered situations where they conducted research for class projects at home, but could not complete the research at school because of over-blocking. Teachers were reluctant to plan lessons that involved the use of Internet resources because of over-blocked content. Students were unable to add images to PowerPoint presentations because the images they needed were blocked. One specific instance noted that students could not access all the information they needed on the history of gaming because many gaming sites were blocked. These interviewee scenarios portrayed the far-reaching effects of the restrictive filtering policies that have been implemented in many South Carolina school districts.

Many of the adverse effects of over-blocking can be mitigated with efficient and clearly communicated over-blocking procedures. Examination of districts' content unblocking efficiency concluded that unblocking procedures in most districts did little to mitigate the adverse effects of over-blocking. Specifically, most end users waited 24

hours or more for content to be unblocked, and of this group, some waited more than a month for content to be unblocked. Another interesting factor was that almost 20 percent of SLMS were not sure of the unblocking wait period. End-user acquiescence and tolerance could be one explanation for SLMS' uncertainty about unblocking wait periods because users who acquiesce to blocked content may not seek to get it unblocked, while those who tolerate over-blocking attempt to locate alternate content that is not blocked. The result is these users may not submit requests to get content unblocked, therefore they were uncertain about the unblocking wait time.

The prevalence of lengthy unblocking periods may be attributed to the absence of on-campus individuals with filter override privileges and bureaucratic unblocking procedures. Granting filter override privileges to school-based staff such as administrators, SLMS, or technology specialists, facilitates timely access to blocked content. However, most SLMS indicated school-based staff was not given filter override privileges. When on-campus privileges were not granted, end users were required to submit an unblocking request, some of which passed through multiple bureaucratic layers. Even when users could submit unblocking requests directly from the blocked page, there was a wait period. In the final analysis, only a small percentage of school districts provided immediate access to block content.

Another prevalent unblocking issue was uncertainty about unblocking procedures. Most SLMS indicated blocked page notifications did not provide unblocking instructions while almost all of IT respondents indicated the blocked page notifications provided unblocking instructions. This discrepancy suggests instructions may have been provided, but were not clear to end users. For instance, one interviewee stated, "I don't know that

people are told how to get something unblocked. The link on the blocked page is very subtle." In addition, an IT respondent stated, "The filter instructs the end user to contact the system administrator." This unblocking instruction was unclear because the system administrator is not identified; therefore, end users may not have known who to contact to get content unblocked. In addition, most IT respondents indicated override privileges had been granted to school-based staff; however, most SLMS, who are school-based staff, indicated override privileges had not been granted to school-based staff. This finding provides additional evidence that there was widespread uncertainty about unblocking procedures.

Over-blocking was the predominant filtering issue SLMS encountered while facilitating access in a filtered environment, but under-blocking and filter circumvention affected end users as well. SLMS and IT administrators indicated that filter under-blocking was far less of an issue than over-blocking. Almost half of IT respondents received requests to block inappropriate content, while slightly more than one-fourth of SLMS occasionally encountered inappropriate content. Nevertheless, most IT and SLMS respondents believed their districts' filters were effective in preventing users from accessing blocked content. Interviewee observations also suggest that filter circumvention occurred occasionally, but was mostly an issue at the secondary level, since elementary students were not as technologically savvy. Even though under-blocking and filter circumvention occurred less frequently than over-blocking, the fact that these issues occasionally occurred, underscores the flawed nature of filtering technology.

Over-blocking was the most pervasive filtering issue for end users. As a result of over-blocking, end users were denied access to a broad range of educational content. School districts' unblocking procedures exacerbated the negative effects of filter over-blocking. Unblocking delays, uncertainty about unblocking procedures, and lack of on-campus override privileges were factors that exacerbated the negative effects of filter over-blocking. Over-blocking coupled with under-blocking and filter circumvention were factors that emphasized that technology protection measures cannot be the sole Internet safety approach for school districts.

Research Question 3

Research question 3 asked, "How are school districts addressing Web 2.0 safety issues?" School district AUPs were analyzed to determine how they had been adjusted in response to Web 2.0 safety concerns. SLMS and IT survey items focused on the implementation of Internet safety education programs to address specific Web 2.0 safety issues such as social network interactions. SLMS were also asked their opinions about the effectiveness of Internet safety approaches such as Internet safety education. Interview observations concurred with the literature review and indicate that policymakers' Web 2.0 safety concerns included inappropriate student postings, inappropriate student interactions online, and cyber bullying.

The AUP analysis determined that the majority of school districts had not updated their AUPs to address Web 2.0 safety issues. AUPs were examined to determine if they stated that minors were to be educated about appropriate online behavior including social network and chat room interactions, and cyber bullying awareness and response. Federal CIPA guidelines required E-rate discount recipients to include this provision in their

AUPs by July 1, 2012. This mandate applied to every school district included in the AUP analysis, which was conducted after July 1, 2012. Two-thirds of the school districts had recently updated their AUPs (within the last three years); however, one-third of this group did not address educating minors about Web 2.0 safety issues. Moreover, most AUPs in compliance with the federal safety education mandate were updated in 2012, which indicates Web 2.0 safety policies were in a state of flux, and district-wide safety education was in the beginning phase of implementation. Essentially, a coordinated district-wide Internet safety education program has not been a significant part of most school districts' online safety efforts.

SLMS' survey and interview observations support the abovementioned conclusion that safety education was not a significant component of most school districts' online safety efforts. Many SLMS survey respondents indicated that a district-wide safety education program had not been implemented. Others were uncertain whether a program had been implemented. SLMS' interview and survey comments largely indicated poorly coordinated efforts to educate minors about Internet safety. Essentially, school districts had passed the responsibility of Internet safety education to teachers and SLMS without making it a requirement, without providing clear guidelines, or indicating that a specific curriculum was required for compliance purposes. Others indicated that students received safety instruction on a one-time basis at the beginning of the school year or via classroom displays. Consequently, fewer than half of SLMS believed their district's Internet safety approaches (i.e., AUPs, filtering, Cyber safety education, monitoring, etc.) effectively prepared students to navigate an unfiltered Internet environment, safely and responsibly.

Slightly more than one-third of SLMS respondents indicated that a district-wide safety education program had been implemented. Interviewee statements about implemented safety programs suggested these programs were successful because of clear guidelines, constant reinforcement of Internet safety concepts, and a concerted district-wide focus on Internet safety education.

An interesting finding was that a large majority of IT respondents indicated a district-wide Internet safety program had been implemented while far fewer SLMS indicated the same. One possible explanation for the discrepancy between the two groups was that SLMS were inadequately informed about the district's program. Another plausible explanation is that IT respondents' may have equated the district's AUP as its education program. IT respondent survey comments support the latter conclusion. For instance, one IT respondent added the following comment to the survey item about district-wide safety education programs: "The district has an Internet safety policy in place and we are currently updating [it] to include cyber bullying."

At the time of the study's survey, safety policies were in a state of flux with Web 2.0 safety education in the early stages of implementation for less than half of South Carolina school districts. However, most AUPs, some of which have not been updated in more than nine years, were inadequate to address 21st century safety issues because they were written for an earlier technological era. Safety policies and safety education have not been the primary focus of Internet safety efforts. School districts have mostly implemented a one-dimensional, restrictive filtering approach to Web 2.0 and other Internet safety issues, which may be undermining student safety as well as information access.

Research Question 4

Research question 4 asked, "In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?" To answer this question, IT and SLMS survey items sought to determine the accessibility of Web 2.0 resources, which promoted the acquisition of communication and collaboration skills. Interview items also sought to define specific Web 2.0 access issues. Concerns about safety issues such as cyber bullying and inappropriate online interactions prompted policymakers in most school districts to block some or all Web 2.0 resources including wikis, blogs, and social networking sites. Consequently, many educational Web 2.0 sites were inaccessible to end users. SLMS' survey data showed that almost two thirds of SLMS encountered blocked educational Web 2.0 resources. SLMS' survey data also revealed that school districts' filtering policies impeded access to communication and collaboration tools. Similarly, interview data demonstrated that access to the read/write Web was impeded. Interviewees provided scenarios in which Twitter™, YouTube™, blogging sites, and Wordle™ were inaccessible, certain Web 2.0 features including emailing and site bookmarking were disabled, and Web 2.0 access was restricted to staff logins.

Interview participants' statements provide evidence that restrictions on Web 2.0 access limited opportunities for students to develop 21st century communication and collaboration skills. Specifically, many students were unable to practice online interaction with peers and were unable to create online content. Online communication with experts, such as chemists or authors, was also inhibited because of Web 2.0 filtering. Some school districts' filtering policies differentiated Web 2.0 access and allowed staff access but

prevented student access to this content. When communication and collaboration was limited to staff accounts, individual student participation was difficult and it inhibited self-directed student learning. The abovementioned Internet policy situations underscored the manner by which such policies limit development of 21st century skills.

One interviewee's observation that Internet use policies have not "kept up with what it means to be a 21st century learner" was applicable to policies implemented in many districts. However, some school districts were beginning to relax Web 2.0 filtering restrictions. These districts were permitting access to Web 2.0 tools such as Edmodo™, a social networking website for education, embracing Google™ docs and Google's™ collaborative tools, and providing access to Web 2.0 tools via SharpSchool's™ school Web hosting services.

Still, Web 2.0 access was limited in most school districts. Restricted Web 2.0 access restricted student engagement in online interactions, and other online activities that enable students to enhance 21st century communication and collaboration skills.

Implications

This study added to the Internet use policy literature by comprehensively investigating filtering and safety policy implementation and its effect on end users. The study enlisted a large number of participants from 36 school districts who were uniquely positioned to inform the investigation. IT administrators, who typically play a key role in Internet use policy implementation, provided information about content blocking decisions, stakeholder involvement in policy decisions, factors influencing filtering decisions, and specific filter configurations. SLMS, facilitators of end user information access, provided information about school-based stakeholder input in policy decisions,

filter over-blocking and under-blocking and its influence of information access, the efficiency of unblocking procedures, and the implementation of Internet safety education. Accordingly, this study contributed to the filtering and safety policy domain by addressing previously unexplored dynamics such as: 1) school districts' filter configuration details; 2) the degree to which safety, security, and other concerns sway policy decisions; and 3) the influence of a wide range of filtering and safety policy issues on end users.

The study participants were not selected via random sampling; therefore, generalization of the results may be limited. Nevertheless, the results were consistent with related studies (Finsness, 2008; Fuchs, 2012; Holzhauer, 2009), most of which were anecdotal and/or less comprehensive. In addition to previous investigations, the present study supports the need for evaluation and revision of school districts' Internet use policies to permit more integration of 21st century online technologies into the K-12 curriculum.

An overarching theme that emerged from this investigation was that school-based stakeholder groups (i.e., SLMS, teachers, administrators, students, etc.) had minimal input in Internet access policy decisions. The implication of this finding is that when Internet use policies are implemented without stakeholder input, they often fail to balance the need for safety with the information needs of end users. Individuals (IT administrators and district administrators) without direct knowledge of online educational resources and their educational benefits were making all Internet policy decisions. This factor could explain why non-teaching policymakers would elect to block access to all blogging tools, not realizing this decision would restrict access to educational blogging sites as well. This

is just one illustration of the access issues that emerge when school-based stakeholders are excluded from filtering policy decisions.

Student safety, network security, network performance, lawsuits, non-educational online activities, and community opinions are serious issues policymakers must balance when implementing Internet access policies. This investigation revealed that these concerns substantially influenced school districts' filtering and safety policies. The implication of this conclusion is tightly controlled Internet access policies that place so much emphasis on potential safety and security threats that access to educational resources is impeded. Robinson, Brown, and Green (2010) support this supposition when they contend that the more school districts fear security threats, the more restrictive district Internet access policies will be. Input from school-based stakeholders could help policymakers develop and implement Internet access policies that maximize access and while maintaining security.

Another important theme that emerged from this study was lack of communication. School districts' Internet safety policies were not clearly communicated to stakeholders. IT respondents affirmed that end users were informed about unblocking procedures via the blocked page notification, school-based stakeholders were granted override privileges, differentiated access levels had been implemented, and a district-wide Internet safety education program had been implemented. To the contrary, most SLMS respondents indicated that these filtering and safety policy measures had not been implemented. These competing perspectives imply school-based stakeholders were not adequately informed of Internet safety policies and procedures. The following respondent observations confirm this supposition: "Unblocking procedures are not well known,"

"The only thing that I know they do is that we have a one-day program [Internet safety program]," and "I am not sure if there is a program [Internet safety] created by the District." Including school-based stakeholders in policy decisions would result in better-informed end users, and increased end user support for Internet access policies.

The use of a one-dimensional approach to Internet safety—the filtering approach—was also a significant theme emerging from this investigation. The implications of this limited Internet safety strategy are uncoordinated efforts to educate minors about safe and responsible Internet use and ineffective, outdated AUPs. The research results confirmed that both circumstances were occurring, likely because of the one-dimensional filtering approach to Internet safety. The literature suggests that the enormous challenge of maintaining a safe online environment for minors can only be accomplished through a multidimensional approach, with filtering technologies being one dimension (Losinski, 2009; Sutton, 2012; OSTWG, 2010), not the only dimension. Finally, federal legislation mandates that multiple Internet safety approaches including filtering technology, monitoring, AUPs, and Internet safety education be components of districts' Internet safety efforts.

The study clearly demonstrates that significant barriers to technology integration in K-12 education still exist, with restrictive Internet access policies being one barrier. The most salient barrier, access to technology, has largely been overcome with the assistance of the E-rate program and heavy investments in computing technologies. The result has been wired schools where computing technology is available in most settings (Robinson, Brown, & Green, 2010), which sets the stage for full integration of computing technologies in education. Yet availability does not always equal accessibility,

particularly in the case of online technology resources. Restrictive access policies render many informational, interactive, and collaborative online technologies inaccessible. Consequently, frustrated end users may be more reluctant to incorporate computing technologies into educational activities, and technology use inside of school will continue to be markedly different from outside of school, where computing technology is embedded in every aspect of society.

Recommendations

Recommendations for further study

In order to further validate the results of this study and to affect educational policy changes, this study needs to be replicated in different geographical regions and on a larger scale. This study was limited to participants from a socially conservative state; therefore, the results may not be applicable to other less conservative regions. Inclusion of socially diverse participants in a similar study would yield data that are more representative and better inform filtering and safety policy implementation. Similar research with other end user groups such as teachers, students, and school-based administrators would provide additional data with which to evaluate existing Internet access policies.

This research was conducted with the assumption that less restrictive filtering policies result in increased access to online educational resources, less user frustration, increased technology integration, and ultimately, enhanced learning. In order to verify this assumption, research should be conducted comparing how the most restrictive filtering policies and the least restrictive policies affect end users. Additionally, policymakers implementing the most restrictive policies typically cite safety and security

as the basis for these policies, but do restrictive polices lead to safer online environments? An examination of the effectiveness of less restrictive filtering policies and very restrictive policies would verify the aforementioned assumptions, and provide additional data to inform filtering and safety policy decision making.

Another assumption of this research was that consistently reinforced Internet safety education encourages students to exhibit safer and more responsible online behaviors in filtered and unfiltered environments. However, research into the effectiveness of Internet safety education and awareness is lacking. The most recent legislative Internet safety mandate requires school districts to educate minors about safe and responsible Internet use even though little is known about the effectiveness of this Internet safety approach. A qualitative investigation of how Internet safety education influences students' online behaviors within and outside of school would inform Internet safety education and awareness program development.

Recommendations for Improved Policy and Practice

The results of this study underscored a number of filtering practices and procedures that were impediments to information access or delayed information access. The research results suggest that implementation of the following recommendations would lessen the access barriers end users encounter in filtered environments.

- Involve school-based stakeholders (i.e., teachers, SLMS, and administrators, etc.) with direct knowledge of online educational resources and end users' access issues in filtering policy decisions.
- Tailor access policies to the needs of individual user groups, including staff and various academic levels, in order to maximize Internet access for each user group.

- Provide filter override privileges for designated on-campus staff such as technology specialists, SLMS or administrators, to allow immediate access to blocked educational content.
- Clearly communicate unblocking procedures to all end users via the blocked page notification, and allow end users to submit unblocking requests directly from the blocked page to facilitate access to blocked content.
- Implement a multifaceted Internet safety program that balances filtering technology with continuous reinforcement of safe and responsible technology use. This balance can be achieved with an updated safety policy that clearly defines acceptable use and incorporates Internet safety education with the use of 21st century communication and collaboration technologies.

Summary

School districts have implemented filtering and safety policies in response to legislative and social mandates to protect students from the proliferation of objectionable Internet content. Some subject related literature reports that administrators are filtering beyond federal and state mandates in order to combat increasing security threats, degraded network performance, and distractions caused by non-educational Internet content. Anecdotal literature suggested restrictive Internet filtering policies limit access to online resources, often involve time-consuming bureaucratic procedures for unblocking acceptable Web sites, and ultimately limit educators' ability to integrate online technologies fully into instruction. The problem that propelled this study was the need to verify the aforementioned filtering issues and to determine how they were influencing information access and instruction.

The goal of this investigation was to examine Internet filtering and safety policy implementation in South Carolina's public K-12 schools and its influence on teaching and learning. A limited number of studies have investigated the effect of filtering policies on teaching and learning. Therefore, the study intended to update and expand upon anecdotal or small-scale studies examining the influence of Internet filtering on instruction and information access in the K-12 sector. This study sought to provide stakeholders (administrators, teachers, SLMS, technology coordinators, and parents) with the data and information necessary to guide filtering and safety policy decisions.

The following research questions guided this study:

- How are filtering and safety policies being implemented in public schools?
- What issues do SLMS encounter as they facilitate information access on filtered computers?
- How are school districts addressing Web 2.0 safety issues?
- In what ways do filtering policies impede access to information and resources necessary to achieve 21st century technology and information literacy standards?

An extensive review of the literature determined that there were numerous issues surrounding filtering and safety policy implementation. The study focused on the following issues as identified in the literature:

- Content category blocking decisions and the rationale for those decisions,
- Stakeholder involvement in filtering/safety policy decisions,
- Implementation of distinct filtering policies for different user groups,
- The implications of over-blocking and under-blocking,
- The efficiency of unblocking procedures,

- The effect of filtering policies on Web 2.0 access, and
- The role of Internet safety education in student online safety efforts.

A mixed research methodology, including quantitative and qualitative approaches, was used to address the research questions. Anonymous online surveys, which focused on the aforementioned filtering and safety policy issues, were designed to collect mostly quantitative data. The research population consisted of SLMS and IT directors. IT administrators provided data about the technical considerations of filtering policy implementation. SLMS, information access facilitators, provided data about filtering and safety policy issues and the influence of these issues on end users. Subsequent one-on-one telephone interviews with a small number of SLMS provided qualitative data. This data provided a deeper understanding of school districts' Internet safety practices and how they either impede or enhance information access. AUPs were also examined to determine whether districts were adjusting their safety policies to include educating minors about Web 2.0 safety issues.

Survey data was used to describe filtering and safety policy decision making and factors influencing policy decisions. The research instruments collected data that defined end users' experiences with content over-blocking, under-blocking, and unblocking practices. This data provided insight on the manner in which these issues influenced teaching and learning. This investigation also examined Web 2.0 safety issues, and the manner in which content filtering, AUPs, and Internet safety instruction was used to address these safety issues. Finally, filtering policies were examined to ascertain the manner in which they impeded access to Web 2.0 resources that enable students to achieve 21st century collaboration and communication standards.

The research conclusions provide a better understanding of filtering policy implementation from the perspective of IT directors. The data indicated policymakers were configuring filters to block considerably more than visual images that were obscene or harmful to minors (as CIPA stipulates). As noted in the literature review, filtering technology has not advanced to the level where it can efficiently block only images. Nevertheless, several factors influenced filtering decisions, the three most influential being CIPA compliance, maintaining student safety, and maintaining network security. The data also indicated that administrators were configuring filters to preserve bandwidth, prevent litigation, prevent non-educational use, and to a lesser extent, in response to community opinions. IT and SLMS survey data and interview observations suggested that in most school districts, school-based stakeholders had minimal input in policy decisions. The research results revealed many school districts were implementing differentiated access levels for staff, but students, regardless of age, level had the same access level. This one-size-fits-all approach to student filtering resulted in more instances when secondary level users experienced content over-blocking.

Survey and interview results were combined to portray the issues SLMS encountered as they facilitated information access in a filtered environment. Survey data revealed that filters were somewhat effective in protecting students from inappropriate content, but overly restrictive filtering policies prevented most end users from accessing controversial subject matter, streaming media, health and sex education resources, and Web 2.0 tools. Interview data supplemented survey findings by providing specific scenarios in which filtering policies denied end users access to educational resources. In addition to the over-blocking issue, end users also encountered inefficient content

unblocking procedures. Bureaucratic and poorly communicated unblocking procedures and lack of on-campus override privileges delayed access to blocked content.

An analysis of school districts' AUPs coupled with survey and interview data revealed that school districts were relying mostly on filters to protect students from online indecency. The majority of school districts had not updated their AUPs to include educating minors about Web 2.0 safety issues, as the Protecting Children in the 21st Century Act (2008) required. Survey and interview data also suggested that Internet safety education was not an important Internet safety approach in many school districts. Over-reliance on filters to protect students from Web 2.0 safety issues resulted in restricted access to Web 2.0 resources and thus handicapped students in acquiring 21st century communication and collaboration skills. In essence, the research results show that school districts' filtering and safety policies were mostly outdated, and have not kept pace with 21st century online technologies.

The researcher compared elementary and secondary SLMS' responses on survey items specifically related to how Internet use policies influenced end users, including students and instructional staff. Elementary and secondary user groups encountered the adverse effects of overly restrictive filtering policies, but these adverse effects were more pronounced at the secondary level. The fact that over-blocking was more prevalent among secondary users, suggests that secondary school users' information needs require access to more of the content that filters typically classify as controversial, potentially liable or non-educational. Considerable over-blocking occurs when filters are set to block such content.

This study shows that South Carolina school districts were mostly using a one-dimensional and one-size-fits-all approach to Internet safety that resulted in restrictive Internet filtering policies. Consequently, end users had limited access to resources enabling them to experience the Internet's vast educational benefits. School districts can improve filtering and safety policies by including end users in policy decisions; implementing unblocking procedures that permit immediate access to blocked content; differentiating access for staff and tailoring access according to students' academic levels; and using a multi-dimensional approach to Internet safety that includes filtering, enforced AUPs, monitoring minors' online access, and consistent Internet safety education that is integrated with the use of 21st century online technologies.

The advent of ubiquitous Web 2.0 and mobile technologies has essentially negated the effectiveness of "lock down" Internet access policies that aim to protect students by blocking access to all potentially harmful content. These reactive policies not only undermine student safety by providing a false sense of security, but they widen the gap between students' in-school and out-of-school technology use. Students must have opportunities to apply safe and responsible online behaviors while using 21st century technologies for authentic learning activities. In order to maximize these learning opportunities, the focus of Internet safety must shift from restrictive Internet access policies to proactive Internet safety strategies that emphasize digital citizenship awareness and education. Otherwise, the in-school and out-of-school technology use gap will only widen, and efforts to integrate 21st century communication and collaboration technologies will continue to be hampered.

Appendix A

Expert Panelists and Instrument Evaluation/Revisions

Expert Panelists

Helen R. Adams, Online Instructor, School of Library and Information Studies
Mansfield University, PA,

Scott S. Floyd, M.Ed., Director of Instructional Technology
White Oak Independent School District, TX

Doug Johnson, Director of Media and Technology
Mankato Area Public Schools, MN

Melissa P. Johnston, Ph.D., Assistant Professor, School of Library and Information Science, University of Kentucky, KY

Lynn Sutton, Ph.D., Dean, Z Smith Reynolds Library
Wake Forest University, NC

Instrument Evaluation and Revisions

Original Item (IT Survey)	Average Rating (Mean)	Item Revisions Based on Expert Panel Recommendations
1) What is your job title?	3.25	No Revisions
2) Does your district participate in the E-rate program?	3.75	No Revisions
3) What Internet content filtering product does your district use?	3.25	Changed beginning of question to: "If your district filters Internet access"
4) Which of the following content categories does your district filter? (Check all that apply)? Adult/Mature, Alcohol/Tobacco, Alternative Lifestyles (LGBT), Criminal/Illegal, Cult/Occult, Blogs/Wikis, Drugs, Email/Chat/Instant Messaging, Gambling, Hate/Racism, Hacking/Proxy Avoidance, Internet Radio/TV, Intimate Apparel/Swimsuits,	4.0	Revised question to state: Please indicate the level of filtering for the following content categories. Select "filters all" if the entire content category is filtered, "filters some" if the category is partially filtered, or "filters none" if the category is not filtered.

Original Item (IT Survey)	Average Rating (Mean)	Item Revisions Based on Expert Panel Recommendations
Media downloads/file sharing, Malicious sites, Pornography/Nudity, Sex Education, Social Networking, Telephony (VOIP), Violence, Weapons		Added a comment section for additional filtered categories or explanations.
5) Who decides which content categories are blocked? District Administrators, Filtering Software (district uses the program's default/recommended settings), IT Staff, School Board, Committee of Stakeholders, Other (please specify)	4.0	Added "check all that apply," Added "media Specialists" as a choice
6) Please indicate the extent to which the following concerns influence content filtering decisions. (Rate 1-5, 1 no influence-2 substantial influence) CIPA Compliance, Preserving Bandwidth, Preventing Non-educational use, Preventing Potential Litigation (Lawsuits), Maintaining Network Security, Maintaining Student Safety, Community or Parental Opinions	3.75	Added a comment section.
7) For each statement, select the answer that corresponds with your district's Internet filtering policies and practices. (Answer choices: Yes, No, Not Sure) a) The district uses the filter's default settings. b) When appropriate, the filter is configured to block specific sub-categories instead of entire content categories. c) Filter settings can be overridden to access educational content that has been blocked unintentionally. d) When users encounter blocked content, the blocked page notification provides instructions on how to get the content unblocked.	4.0	Added a comment section.

Original Item (IT Survey)	Average Rating (Mean)	Item Revisions Based on Expert Panel Recommendations
e) Different access levels have been established for specific user groups (i.e., elementary students, secondary students, teachers, staff) f) Filter override privileges have been granted to designated on-campus staff (i.e., administrators, media specialists, technology specialists)		
8) The district has implemented an Internet safety education program that includes cyber bullying and social networking safety issues. Yes, No, Not Sure	4.0	No Revisions
9) During a typical week, please indicate how often you receive request to: Block inappropriate content (Never, Rarely, Sometimes, Frequently) Unblock educational content that has been unintentionally blocked (Never, Rarely, Sometimes, Frequently)	4.0	Inserted (or the person responsible for blocking/unblocking content) after "how often do you." Added a comment section for respondents to describe procedures for addressing blocking/unblocking requests.
10) How effectively does the filter: Block inappropriate content (Very ineffective, Somewhat ineffective, Somewhat effective, Very effective) Permit access to educational content (Very ineffective, Somewhat ineffective, Somewhat effective, Very effective)	4.0	Added a comment section.

Appendix B

IT Administrators' Survey

Introduction
Thank you for responding to the filtering/safety policy survey. Your response is vital to this research project and should take 10 minutes or less to complete.
Proceeding to the next page indicates your voluntary participation in this research study.

Background Information
1) What is your job title?
_____

2) Does your district participate in the federal E-rate program?
The E-rate program provides discounts of 20 percent to 90 percent for eligible telecommunications services, depending on economic need and location.
[ ] Yes
[ ] No
[ ] Not sure

3) If your district filters Internet access, what Internet filtering product is used?
_____

Filtered Content Categories
4) Please indicate the level of filtering for the following content categories.
Select "filters all" if the entire category is filtered, "filters some" if the category is partially filtered, or "filters none" if the category is not filtered.

	Filters all	**Filters some**	**Filters None**
Adult/Mature	( )	( )	( )
Alcohol/Tobacco	( )	( )	( )
Alternative Lifestyles (LGBT)	( )	( )	( )
Criminal/Illegal	( )	( )	( )
Cult/Occult	( )	( )	( )
Blogs/Wikis	( )	( )	( )
Drugs	( )	( )	( )
Email/Chat/Instant Messaging	( )	( )	( )
Gambling	( )	( )	( )
Hate/Racism	( )	( )	( )
Hacking/Proxy Avoidance	( )	( )	( )
Internet Radio/TV	( )	( )	( )
Intimate Apparel/Swimsuits	( )	( )	( )
Media downloads/file sharing	( )	( )	( )
Malicious sites	( )	( )	( )
Pornography/Nudity	( )	( )	( )
Sex Education	( )	( )	( )

	Filters all	Filters some	Filters None
Social Networking	( )	( )	( )
Telephony (VOIP)	( )	( )	( )
Violence	( )	( )	( )
Weapons	( )	( )	( )

Additional filtered categories/Additional comments

Content Filtering Decisions

5) Who decides which content categories are blocked? (check all that apply)

[ ] Committee of Stakeholders
[ ] District Administrators
[ ] Filtering Software (district uses the software's default/recommended settings)
[ ] IT staff
[ ] School Board
[ ] Media Specialists
[ ] Other, please specify

Content Filtering Influences

6) On a scale of 1-5, with 1 indicating no influence and 5 indicating substantial influence, how much do the following concerns influence content filtering decisions?

	1	2	3	4	5
CIPA Compliance	( )	( )	( )	( )	( )
Preserving Bandwidth	( )	( )	( )	( )	( )
Preventing Non-educational Use	( )	( )	( )	( )	( )
Preventing Litigation (Lawsuits)	( )	( )	( )	( )	( )
Maintaining Network Security	( )	( )	( )	( )	( )
Maintaining Student Safety	( )	( )	( )	( )	( )
Community or Parental Opinions	( )	( )	( )	( )	( )

Additional Comments:

Filtering Policies

7) Please indicate whether the following filtering policies are being implemented in your school district?

	Yes	No	Not sure
a) The district uses the filter's default settings.	( )	( )	( )
b) When appropriate, the filter is configured to block specific sub-categories instead of entire content categories (i.e., filter settings block non-educational Web 2.0, but allow educational Web 2.0 tools).	( )	( )	( )
c) Filter settings can be overridden/adjusted to access educational content that has been blocked unintentionally.	( )	( )	( )
d) When users encounter blocked content, the	( )	( )	( )

	Yes	No	Not sure
blocked page notification instructs users how to get the content unblocked.			
e) Different access levels have been set for specific user groups. (i.e., elementary students, secondary students, staff)	( )	( )	( )
f) Filter override privileges have been granted for designated on-campus staff (i.e., administrators, media specialists, technology specialists).	( )	( )	( )

Additional comments:

Internet Safety Education Program

8) The district has implemented an Internet safety program that educates students about appropriate online behavior, including social networking and chat room interactions, and cyber bullying awareness and response.

[ ] Yes
[ ] No
[ ] Not sure
Additional comments:

Blocking/Unblocking Frequency

9) During a typical week, how often do you (or the person responsible for blocking/unblocking content) receive requests to:

	Never	Rarely	Sometimes	Frequently
a) Block inappropriate Internet content?	( )	( )	( )	( )
b) Unblock educational content that has been unintentionally blocked?	( )	( )	( )	( )

Briefly describe the procedure for addressing blocking/unblocking requests.

Filter Effectiveness

10) How effectively does the filter:

	Very ineffective	Somewhat ineffective	Somewhat effective	Very effective
a)Block inappropriate content	( )	( )	( )	( )
b)Permit access to educational content	( )	( )	( )	( )

Additional Comments:

Thank You!

Thank you for responding to the survey!

Appendix C

School Library Media Specialists' Survey

Introduction
Thank you for responding to the filtering/safety policy survey. Your response is vital to this research project and should take less than 10 minutes to complete. Proceeding to the next page indicates your voluntary participation in this research study.

Title/Academic Level
1) What is your:
a) Job Title?: _____
b) Academic Level (of your school) (i.e, K-5, 6-8, 9-12, etc.)?: _____

Content Blocking Decisions
2) Who decides which content categories are blocked? (check all that apply)
[ ] Committee of Stakeholders
[ ] District Administrators
[ ] Filtering Software (district uses the software's default/recommended settings)
[ ] IT staff
[ ] School Board
[ ] Media Specialists
[ ] Other, please specify
Additional Comments:

Over-blocking Content
3) If the Internet filter over-blocks, what kind of educational/instructional content does it block? (check all that apply)
[ ] Business/Finance
[ ] Controversial content (i.e, LGBT, alternative lifestyles, hate groups, cults, occult, etc.)
[ ] Educational games
[ ] Health/Sex Education
[ ] Sports and Recreation
[ ] Streaming media (i.e. Youtube, UStream.tv, Internet Radio, etc.)
[ ] Virtual Worlds
[ ] Visual images
[ ] Web 2.0 resources (i.e., Wikis, blogs, social bookmarking tools, etc.)
[ ] Other, please specify
Additional Comments:

Unblocking Time
4) If the filter unintentionally blocks educational Web content, how long does it usually take to get the content unblocked?

[ ] Content is unblocked immediately
[ ] Less than 1 hour
[ ] Several hours
[ ] 1-2 days
[ ] 3-4 days
[ ] 1-2 weeks
[ ] 3-4 weeks
[ ] More than 1 month
[ ] Content cannot be unblocked
[ ] Not sure

Over-blocking/Under-blocking Frequency
5) During a typical week, how often does the filter:

	Never	Rarely	Sometimes	Frequently
Permit access to objectionable content (under-blocking)	( )	( )	( )	( )
Prevent access to information/resources that support educational, professional, or personal growth (over-blocking)	( )	( )	( )	( )

Filter Effectiveness
6) Considering the filter's over-blocking/under-blocking efficiency, how would you rate the filter's overall effectiveness?
( ) Very ineffective
( ) Somewhat ineffective
( ) Neutral
( ) Somewhat effective
( ) Very effective
Additional Comments:

Filtering/Safety Policies and Practices
7) Have any of the following Internet filtering/safety policies or practices been implemented in your school district?

	Yes	No	Not sure
a) Input from all stakeholders is considered when content filtering decisions are made.	( )	( )	( )
b) Designated on-campus staff have filter override privileges (i.e. administrators, media specialists, technology specialists).	( )	( )	( )
c) When users encounter blocked content, the blocked page notification instructs users how to get the content unblocked.	( )	( )	( )
d) Different access levels have been	( )	( )	( )

established for specific user groups (elementary users, secondary users, staff).			
e) An Internet safety education program that educates students about appropriate online behavior (including social network and chat room interactions, and cyber bullying awareness and response) has been implemented.	( )	( )	( )

Additional Comments:

Filtering/Safety Policy Opinions

8) Please indicate the level of your agreement with the following statements about the district's/school's Internet filtering policies/practices.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
a) The Internet filter prevents instructional staff from accessing resources needed for instructional or professional activities.	( )	( )	( )	( )	( )
b) The Internet filter prevents students from accessing information/resources needed for classroom assignments.	( )	( )	( )	( )	( )
c) The Internet filter prevents users from deliberately or unintentionally accessing inappropriate content.	( )	( )	( )	( )	( )
d) Filter override procedures allow timely access to blocked resources/information.	( )	( )	( )	( )	( )
e) Filtering and safety policies facilitate easy access to online collaboration and communication tools (Web 2.0).	( )	( )	( )	( )	( )
f) Filtering and safety policies/practices (i.e. Acceptable Use policies, Cyber-safety education, monitoring, etc.) prepare	( )	( )	( )	( )	( )

students to be safe and responsible users in unfiltered environments.					

Additional Comments:

Thank You!
I am seeking 4-5 survey respondents to participate in a brief follow-up telephone interview. If you are willing to be interviewed, please email me at tyler@nova.edu or call me at 803-699-6479 (H) or 803-553-3276 (M).

Thank you for taking the survey, your input is vital to this research study.

Appendix D

Interview Protocol

An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K-12 Public Schools

Interview with_____ Date: _____ Time: _____
Phone: _____

Hello. I want to thank you for your willingness to participate in this research study on Internet filtering and safety policy implementation. The research goal is to determine how Internet use policies influence teaching and learning.

This interview will take 20-25 minutes. If at any time you wish to end your participation, just let me know. If you do not wish to have the information you have provided included in the study, I will destroy it when this conversation is terminated, along with my notes. Let's begin.

Question Set 1-- Stakeholder Involvement in Policy decisions (RQ1)
How are stakeholders (teachers, media specialists, students, parents, etc.) involved in filtering and safety policy decisions? (i.e., do they have input in content blocking decisions, developing AUPs, or establishing filter unblocking practices/procedures?)

_____
_____
_____
_____
_____

If stakeholder involvement is minimal or nonexistent:
Would the district's safety/filtering policies be more effective if stakeholders were more involved in filtering and safety policy decisions? _____Why or Why not?

_____
_____
_____

If stakeholder involvement is significant:

Does stakeholder involvement have a positive influence on access to online resources and on student online safety? _____ Why or Why not?

_____
_____
_____
_____

Question Set 2 -- Unblocking/blocking procedures and practices: (RQ1, RQ2)
Please describe your district's unblocking procedures/practices that have been established to allow access to content the filter blocks unintentionally.

_____
_____

_____
_____
_____
_____

Do you believe these unblocking procedures/practices facilitate or impede access to information?

Facilitate	**Impede**
What specific practices enhance information access?	**What specific practices impede or delay access information?**
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Question Set 3 – Influence of over-blocking and under-blocking on teaching/learning: (RQ2)

In your view, has filter under-blocking (allowing access to inappropriate content) had an adverse influence on learning or student safety?

Yes	**No**
Can you give specific examples of when under-blocking had an adverse influence on instruction or student safety?	Go to next question.
_____	
_____	
_____	
_____	
_____	

How frequently do students circumvent the filter to gain access to blocked content?

_____
_____

Has over-blocking (preventing access to educational resources) adversely influenced student or teacher access to educational resources?

Yes	**No**
Can you give some examples of when over-blocking prevented students from information needed for assignments or teachers from resources need for instruction or professional development?	Go to Question Set 4
_____	
_____	
_____	

What strategies do students/teachers use to gain access to blocked content when it is needed for instruction or classroom assignments?

Question Set 4 – Internet safety education programs (RQ3)

What Internet safety education program(s) has your district implemented to educate students about responsible online behavior? (If there are no programs in place, go to question set 5)

In your view, are these Internet safety education programs effective in preparing students to safely and responsibly navigate the Internet in filtered and unfiltered settings?

Yes

What makes your Internet safety education program effective?

No

What makes the Internet safety education program ineffective?

How can the Internet safety program(s) and policies be improved to increase overall effectiveness?

Question Set 5 – Web 2.0 safety and access issues: (RQ3, RQ4)

In your view, do the district's filtering and safety policies restrict access to Web 2.0 tools that foster online communication and collaboration? (i.e., wikis, blogs, Google docs)

Yes

What safety concerns prompt policymakers to restrict Web 2.0 access?

No

What specific policies/practices have been implemented to facilitate access

In what ways do these policies restrict access to online communication and collaboration tools? to Web 2.0 tools?

_____
_____
_____
_____
_____

How does restricted access to Web 2.0 tools limit attainment of 21st century information literacy and technology standards?

_____
_____
_____
_____

Conclusion

Is there anything else you would like to share regarding Internet filtering/safety policy implementation and how it affects the SLMS's mission to provide information in the least restrictive and most timely manner?

_____
_____
_____

Appendix E

Protocol for Analyses of Artifacts (AUPs)

Research Question: How are school districts addressing Web 2.0 safety issues?

Beginning July 1, 2012, E-rate applicants are required to update their Internet safety policy (AUP) to reflect the requirements of the 2008 Protecting Children in the 21st Century Act. To address Web 2.0 safety issues, school districts must certify that their Internet safety policies have been updated to provide for educating minors about appropriate online behavior including interacting with other individuals on social networking Web sites and in chat rooms and cyber bullying awareness and response.

School District Name:

The AUP was last updated on:	Date:
Has the AUP been updated to provide for educating minors about appropriate online behavior including interacting with other individuals on social networking Web sites and in chat rooms and cyber bullying awareness and response?	Yes ☐ No ☐
	Comments -- including references to educating minors, social networks, cyber bullying, etc. _____ _____ _____ _____ _____

Appendix F

Letter to Expert Panelists

Hello,

My name is Mary Tyler and I am a Ph.D. student at Nova Southeastern University's Graduate School of Computer and Information Sciences. My dissertation research focuses on Internet filtering and safety policy implementation in South Carolina's public schools, and its influence on information access and instruction. I have read your contributions to the knowledge base in this domain and am seeking your assistance. Would you be willing to serve on my dissertation expert panel as a subject matter expert? The expert panel's role is to assist in validating the data collection instruments for the proposed research. These instruments have been designed to answer the following research questions:

- How are filtering and safety policies being implemented in public schools?
- What issues do school library media specialists encounter as they facilitate information access on filtered computers?
- How are school districts addressing Web 2.0 safety issues?
- In what ways do filtering policies impede access to information and/or resources necessary for achieving 21st century technology and information literacy standards?

Expert panelists are asked to rate each item for relevance to the research questions, assess the comprehensiveness of the instruments (do they adequately cover the topic?), and provide comments regarding content, wording, format, and clarity? If you are willing to participate, please click on the links below to access the evaluation instruments.

IT Survey evaluation:
http://edu.surveygizmo.com/s3/784410/IT-Administrators-Survey-Evaluation

School library media specialists survey evaluation:
http://edu.surveygizmo.com/s3/784286/Media-Specialists-Survey-Evaluation

If you have any questions regarding this study, you may contact me at tyler@nova.edu. Thank you in advance for your time and expertise.

Mary Tyler
tyler@nova.edu
(803) 553-3276

Appendix G

Letter to School Districts Requesting Authorization to Conduct Research

January 24, 2012

Dear Superintendent and School Board Members,

I am a retired educator and Nova Southeastern University doctoral student in the Graduate School of Computer and Information Sciences department. The goal of my dissertation research is to investigate Internet filtering and safety policy implementation in South Carolina's public schools and its influence on teaching and learning. This investigation requires surveying a sampling of technology directors and media specialists in the state. Therefore, I am requesting permission to invite your district's technology director and media specialists to participate in the survey.

The media specialists and IT surveys, which are attached, will consist of about ten items asking about your district's Internet filtering policies and practices, the effectiveness of your filtering software and safety policies (AUPs), how Internet filtering/safety policies influence teaching and learning, and how Web 2.0 safety issues are being addressed.

The surveys will be completely anonymous and can be accessed via SurveyGizmo's Website. Survey participants will be sent a Web link to access the surveys. At no time will participants' or school districts' names be used in this research.

The research results will provide district policymakers and stakeholders with research-based data to inform Internet access policy decisions, and prescribe practices that optimize access to the most recent online educational resources. Thank you in advance for supporting and advancing this research study.

Sincerely,

Mary E. Tyler-Vicks
Doctoral Candidate, Nova Southeastern University

Please mail your approval in the enclosed self-addressed stamped envelope or fax it to the above toll-free fax number.
_____School District _____grants permission _____ does not grant permission for media specialists and the technology director to be sent invitations to participate in the proposed research study.
_____ and/or _____
Superintendent's Signature School Board Chairman's Signature

Appendix H

IRB Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Mary Tyler

From: Ling Wang, Ph.D.
Institutional Review Board

Date: April 12, 2012

Re: *An Examination of Internet Filtering and Safety Trends and Issues in South Carolina's K-12 Public Schools*

IRB Approval Number: wang04151204

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

Appendix I

Media Specialists' Survey Invitation Email

Dear Colleague,

I am requesting your participation in a research study about Internet filtering and safety policies in South Carolina's public schools. This research is being conducted as part of a doctoral dissertation at Nova Southeastern University in Fort Lauderdale, Florida. The purpose of the study is to determine how these policies affect information access and instruction in South Carolina's public schools. The results of this study will provide stakeholders and policymakers with useful data for evaluating and improving existing Internet use policies.

I am seeking your input because media specialists facilitate information access and are keenly aware of the issues users encounter when they search for information on filtered computing devices. You also play a critical role in educating users about safe and responsible Internet use.

Below is a secure link to the online survey. Your responses will be anonymous and your name will not be attached to any results. The survey is user-friendly and should take no more than 10-15 minutes. Completing the survey indicates your voluntary participation in this research study.
http://edu.surveygizmo.com/s3/940684/Media-Specialists-Survey

I appreciate your willingness to participate in the survey. If you have any questions please feel free to contact me.

Mary Tyler,
Principal Investigator,
Graduate School of Computer and Information Sciences
Fort Lauderdale, Florida 33314
Contact Information:
tyler@nova.edu

Appendix J

IT Administrators' Survey Invitation Email

Dear Colleague,

I am requesting your participation in a research study about Internet filtering and safety policies in South Carolina's public schools. This research is being conducted as part of a doctoral dissertation at Nova Southeastern University in Fort Lauderdale, Florida. The purpose of the study is to determine how filtering and safety policies affect information access and instruction in South Carolina's public schools. The results of this study will provide stakeholders and policymakers with useful data for evaluating and improving existing Internet use policies.

I am seeking your input because IT administrators play a critical role in establishing and implementing filtering and safety policies. You are also knowledgeable of the technical considerations of filtering software selection and configuration.

Below is a link to the online survey. Your responses will be anonymous and your name will not be attached to any results. The survey is user-friendly and you should be able to complete it within 15 minutes. Completing the survey indicates your voluntary participation in this research study.
http://edu.surveygizmo.com/s3/958372/IT-Survey

I appreciate your willingness to participate and value your input. If you have any questions before or after completing the survey please feel free to contact me.

Mary Tyler,
Principal Investigator,
Graduate School of Computer and Information Sciences
Fort Lauderdale, Florida 33314
Contact Information:
tyler@nova.edu

Appendix K

Interview Consent Form

NOVA SOUTHEASTERN UNIVERSITY

Consent Form for Participation in the Research Study Entitled An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K-12 Public Schools

Funding Source: None

IRB protocol #: 04151204

Principal investigator(s)
Mary E. Tyler
422 Ridge Trail Dr.
Columbia, SC 29229
803-699-6479
803-553-3276

Co-investigator/Committee Chair
Steven Zink, Ph.D.
Nova Southeastern University,
3301 College Avenue
DeSantis Building, #4108
Fort Lauderdale, FL 33314
(954) 262-2020 or 800-541-6682

For questions/concerns about your research rights, contact:
Institutional Review Board
Nova Southeastern University
Office of Grants and Contracts
(954) 262-5369/Toll Free: 866-499-0790
IRB@nsu.nova.edu

Description of the Study:
What is the study about?
You are being asked to take part in a research study about Internet filtering and safety policies in South Carolina's public schools. The purpose of the study is to examine filtering and safety policy practices and procedures to determine how they may be influencing information access and instruction. The study utilizes multiple surveys and interviews to collect data.

Why are you asking me?
You are being asked to participate in the interview phase of the study because you responded to the initial media specialists' survey and you agreed to take part in the post-survey telephone interview.

What will I be doing if I agree to be in the study?

If you participate in the interview phase of the study, you will be interviewed about your district's filtering and safety policy practices/procedures. The interview will also address your convictions and concerns about how Internet use policies influence end users' access to information and resources.

Audio/Video Recording
Is there any audio recording?
Interviews **will not be** audio recorded. The researcher will take extensive notes during the interviews.

Risks/Benefits to the Participant:
What are the dangers to me?
All studies have some risks, whether direct or indirect. However, the present research involves no more than minimal risks as it seeks to investigate your district's Internet filtering/safety policies and your perception of how these policies may be affecting teaching, learning, and students' online safety. The procedures or activities in this study may have unknown or unforeseeable risks. If you have any concerns about the risks or the benefits of participating in this study, you can contact Mary E. Tyler, Dr. Steven Zink, or the IRB office at the numbers indicated above.

Are there any benefits to me for taking part in this research study?
There are no direct benefits, but the proposed study will arm school district stakeholders with the data and information necessary to guide filtering and safety policy decisions. The study will also prescribe filtering practices that may lead to improved Internet filtering and safety policies.

Costs and Payments to the Participant:
Will I get paid for being in the study?
No payments will be made to participants in this study.

Will it cost me anything?
There are no costs to you for participating in this study.

Confidentiality and Privacy:
How will you keep my information private?
Every effort will be made to keep participants' information entirely confidential. No risk of exposure of sensitive information due to the research process is anticipated and data collected during the interviews will be handled and stored securely to protect participants' privacy. Interview data will be retained in a secure digital file for 36 months from the conclusion of the study. No personally identifiable information will be revealed in the final report. That is, all information obtained in this study is strictly confidential unless disclosure is required by law.

Research records identifying you may be examined by the principal investigator's dissertation chair, the Nova Southeastern University Institutional Review Board, and other regulatory Agencies.

Participants Right to Withdraw from the Study:
What if I want to leave the study?
You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or loss of benefits to which you are entitled. If you choose to withdraw, any information collected about you before the date you leave the study will be kept in the research records for 36 months from the conclusion of the study, but you may request that it not be used.

Other Considerations:
If significant new information relating to the study becomes available, which may relate to your willingness to continue to participate, this information will be provided to you by the investigator.

Voluntary Consent:

By signing below, you indicate that

- this study has been explained to you
- you have read this document or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact them in the event of a research-related injury
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you are entitled to a copy of this form after you have read and signed it
- you voluntarily agree to participate in the study entitled "An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K-12 Public Schools."

Participant's Signature: _____ Date: _____

Participant's Name: _____ Date: _____

Signature of Person Obtaining Consent: _____

Date: _____

References

Adams, H. R. (2010, September/October). Intellectual freedom online: The new battleground for minors' First Amendment rights. *Knowledge Quest, 39*(1), 10-15. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a6bc6ad4ad1109d2821d4de3f6db5fb16d2ad9cacc8bec632&fmt=P

Adams, H. R. (2012). Don't filter me: One success in the fight over filtering in schools. *School Librarian's Workshop, 32*(5), 16-17. Retrieved from http://web.ebscohost.com.ezproxylocal.library.nova.edu/ehost/pdfviewer/pdfviewer?vid=4&hid=17&sid=b27dabe7-78db-4a78-96dd-51c6f5285d12%40sessionmgr12

Ahn, J., Bivona, L.K., & DiScala, J. (2011, October). Social media access in K-12 schools: Intractable policy controversies in an evolving world. *Proceedings of the American Society for Information Science and Technology, 48*, 1-10. doi: 10.1002/meet.2011.14504801044

Alexander, K. & Alexander, M. D. (2012). *American public school law* (8th ed.). Belmont, CA: Wadsworth, Cengage Learning

American Association of School Librarians (AASL). (2007). *AASL standards for the 21st-century learner*. Retrieved from http://www.ala.org/ala/mgrps/divs/aasl/guidelinesandstandards/learningstandards/AASL_LearningStandards.pdf

American Association of School Librarians (AASL). (2012). Filtering in schools: AASL executive summary. Retrieved from http://www.ala.org/aasl/researchandstatistics/slcsurvey/filtering-schools

American Library Association (ALA). (2013a). *Access for children and young adults to nonprint materials: An interpretation of the Library Bill of Rights*. Retrieved from http://www.ala.org/ala/issuesadvocacy/intfreedom/librarybill/interpretations/accesschildren.cfm

American Library Association (ALA). (2013b). *Library bill of rights*. Retrieved from http://www.ala.org/ala/issuesadvocacy/intfreedom/librarybill/index.cfm

American Library Association (ALA). (2013c). *Code of ethics of the American Library Association.* Retrieved from http://www.ala.org/advocacy/proethics/codeofethics/codeethics

American Library Association (ALA) v. United States, 201 F.2d 401 (U. S. District Court for the Eastern District of Pennsylvania 2002).

Associated Press (2012, April 4). Mo. District Settles Web-Filtering Suit. *Education Week, 31*(27), 4. Retrieved from http://go.galegroup.com.ezproxylocal.library.nova.edu/ps/i.do?id=GALE%7CA286517601&v=2.1&u=novaseu_main&it=r&p=AONE&sw=w

Banday, M.T., & Shah, N.A. (2010). A concise study of Web filtering. *Sprouts: Working Papers on Information Systems,10*(31). Retrieved from http://sprouts.aisnet.org/10-31

Baule, S. M. (2010, March/April). Revisiting filtering. *Library Media Connection, 28*(5), 48-49. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/results/external_link_maincontentframe.jhtml?_DARGS=/hww/results/results_common.jhtml.43

Bertino, E., Ferrari, E., & Prego, A. (2010). A general framework for Web content filtering. *World Wide Web, 13*(3), 215-249. doi: 10.1007/s11280-009-0073-5

Board of Education, Island Trees Union Free School District No. 26 v. Pico, 457 U.S. 853 (1982).

Booth, A. (2011). Barriers and facilitators to evidence-based library and information practice: An international perspective. *Perspectives in International Librarianship*, 1, 1-15. doi: 10.5339/pil.2011.1

Bosco, J. & Krueger, K. (2011, July 10). Moving from 'acceptable' to 'responsible' use in a Web 2.0 world. *Education Week, 30*(17). Retrieved from http://www.edweek.org/ew/articles/2011/07/20/37bosco.h30.html

Brooks-Young, S. (2010). *Teaching with the tools kids really use*. Thousand Oaks, CA: Corwin.

Bush, L. & Hall, J. (2011). Transforming teaching with technology: Using Web 2.0 tools to enhance on-line communication, collaboration, and creativity. In M. Koehler & P. Mishra (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference,2011* (pp. 3887-3890). http://www.editlib.org/p/36937

Chen, T., & Wang, V. (2010). Web filtering and censoring. *Computer, 43*(3), 94-97. doi 10.1109/MC.2010.84

Children's Internet Protection Act (CIPA), 47 U.S.C. § 254 (2000).

Child Online Protection Act of 1998, 47 U.S.C. § 231 (1998).

Chmara, T. (2010, September/October). Minors' First Amendment rights: CIPA & school libraries. *Knowledge Quest, 39*(1), 17-21. Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=2184630971&sid=2&Fmt=3&clientId=17038&RQT=309&VName=PQD

Chou, C., Sinha, A.P., Zhao, H. (2010). Commercial Internet filters: Perils and opportunities. *Decisions Support Systems, 48*(4), 521-530. Retrieved from http://dx.doi.org.ezproxylocal.library.nova.edu/10.1016/j.dss.2009.11.002

Cohen, L., Manion, L., & Morrison, K. (2011). *Research methods in education* (7th ed.). London: Taylor & Francis.

Collins, A., & Halverson, R. (2009). *Rethinking education in the age of technology: The digital revolution and schooling in America*. New York: Teachers College Press.

Communications Decency Act of 1996, 47 U.S.C. § 223 (1996).

Consortium for School Networking (CoSN). (2011). *Acceptable use policies in a Web 2.0 era: A guide for school districts.* Retrieved from http://www.cosn.org/Initiatives/ParticipatoryLearning/Web20MobileAUPGuide/tabid/8139/Default.aspx

Cramer, M., & Hayes, G.R. (2010, July/September). Acceptable use of technology in schools: Risks, policies, and promises. *Pervasive Computing, 9*(3), 37-44. doi 10.1109/MPRV.2010.42

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Los Angeles: Sage Publications.

Creswell, J., & Plano Clark, V.L. (2007). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage Publications.

Deleting Online Predators Act, H.R. 5319, 109th Cong. (2006), http://www.govtrack.us/congress/bill.xpd?bill=h109-5319

Devaney, L. (2013, January). Survey: School web filtering can impede learning. *eSchool News, 16*(1), 13.

Endicott-Popovsky, B. (2009, December). Seeking a balance: Online safety for our children. *Teacher Librarian, 37*(2), 29-34. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a11572fffa46aad42ba0d0bc7e4e0f96819ba8cda9548a10b&fmt=P

Enex Testlab. (2011, July). *Content filtering technologies overview*. Retrieved from http://www.cso.com.au/article/393605/content_filtering_technologies_overview/

E-rate Central. (2012). *Internet safety policies and CIPA: An E-rate primer for schools and libraries*. Retrieved from http://www.eratecentral.com/CIPA/cipa_policy_primer.pdf

Essex, D. (2009, Spring). From deleting online predators to educating Internet users: Congress and Internet safety: A legislative analysis. *Young Adult Library Services, 7*(3), 36-45. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a11572fffa46aad42d82c82bc7500b267b2f402807e352bb0&fmt=H

Federal Communications Commission. (2011). Consumer guide: Children Internet Protection Act (CIPA). Retrieved from http://www.fcc.gov/guides/childrens-internet-protection-act

Finsness, L. S. (2008). *The implications of Internet filters in secondary schools* (Doctoral dissertation, University of Minnesota). Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=1564026751&sid=3&Fmt=2&clientId=17038&RQT=309&VName=PQD

Fowler, F. J. (2009). *Applied social research methods: Survey research methods* (4th ed.). Los Angeles: Sage.

Fuchs, L. (2012). *The impact of filtered Internet access on student learning in public schools.* (Doctoral dissertation, Walden University). Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/pqdtft/docview/955172752/fulltextPDF/13A4F9F6629EEC78D6/1?accountid=6579

Gay, L. R., Mills, G. E., & Airasian, P. W. (2011). *Educational research: Competencies for analysis and applications* (10th ed.). Columbus, OH: Merrill.

Gossett, D. & Shorter, J. D. (2011). Effectiveness of Internet content filtering. *Journal of Information Technology Impact, 11*(2), 145-152.

Gros, L., & Hancock, R. (2011, March). The evolution of digital statutory law: An overview for educational technology leaders. *Society for Information Technology & Teacher Education International Conference* (pp. 2961-2968). Chesapeake: VA.

Hall, R. T., & Carter, E. (2006). Examining the constitutionality of Internet filtering in public schools: A US perspective. *Education and the Law, 18*(4), 227-245. doi:10.1080/09539960601035906

Hall, W. (2011). The ever-evolving Web: The Power of Networks. *International Journal of Communication, 5*,551-664. Retrieved from http://ijoc.org/ojs/index.php/ijoc/article/view/1120

Harris, F. J. (2009a, January/February). Ethics from Web 1.0 to Web 2.0: Standing outside the box. *Knowledge Quest, 37*(3), 56-61. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a807214e88588c3dd2144d21b0b058bd71d7f0cfe08ae48e9&fmt=P

Harris, F. J. (2009b). Challenges to teaching evaluation of online information: A view from LM_NET. *School Library Media Research, 12*. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a05e5d81d61e777748097c05dcb66e6bc1b9baec7a85ca1ae&fmt=P

Hidalgo, J. M., Garcia, F. C., Sanz, E. P., & Rodiguez, M. D. (2009). Web content filtering. In M. Zelkowitz (Ed.), *Advances in computers* (Vol. 76, pp. 257-306). Burlington, MA: Academic Press.

Holcomb, L., Brady, K., & Smith, B. (2010, March). Ning in Education: Can non-commercial, education-based social networking sites really address the privacy and safety concerns of educators? *Society for Information Technology & Teacher Education International Conference* (Vol. 2010, No. 1, pp. 528-531).

Holt, L., & Galligan, M. (2012, March). Is it time to recreate the E-rate program? *Federal Communications Law Journal, 64*(2), 275-379.

Holzhauer, J. L. (2009). *Filtering of the Internet and its effect on K-12 public school classroom instruction* (Doctoral dissertation, Northcentral University, Prescott, Arizona). Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=1793220611&sid=2&Fmt=2&clientId=17038&RQT=309&VName=PQD

Hoover, B. J. (2009, Winter). The First Amendment implications of Facebook, MySpace, and other online activity of students in high school. *Southern California Interdisciplinary Law Journal, 18*(2), 309-328. Retrieved from http://www.lexisnexis.com.ezproxylocal.library.nova.edu/us/lnacademic/results/docview

Hope, A. (2012). The shackled school Internet: Zemiological solutions to the problem of overblocking. *Learning, Media and Technology*, 1-14. Retrieved from http://dx.doi.org/10.1080/17439884.2012.670646

Houghton-Jan, S. (2010, November/December). Internet filtering. *Library Technology Reports, 46*(8), 25-45. Retrieved from http://find.galegroup.com.ezproxylocal.library.nova.edu/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T002&prodId=AONE&docId=A244158909&source=gale&srcprod=AONE&userGroupName=novaseu_main&version=1.0

Hua, V. (2011). Redefining the security wall: With the proliferation of Web 2.0 apps and mobile devices, Internet security requires more than a simple firewall. *T H E Journal (Technological Horizons in Education), 38*(7), 36-38.

International Society for Technology in Education (ISTE). (2007). *The ISTE national educational technology standards (NET*S) and performance indicators for students*. Retrieved December, 10, 2012, from http://www.iste.org/standards/nets-for-students/nets-student-standards-2007.aspx

Internet. (2011). In D. Batten (Ed.*) Gale encyclopedia of American law* (3rd ed., Vol. 5, pp. 489-494). Detroit, MI: Gale Cengage Learning.

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006, February). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods, 18*(1), 3-20. doi:10.1177/1525822X05282260

Jaeger, P. T., & Yan, Z. (2009, March). One law with two outcomes: Comparing the implementation of CIPA in public libraries and schools. *Information Technology and Libraries, 28*(1), 6-14. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509af65e0df43927e4963c95142b6acdb75f6cebedf9d84092de&fmt=H

Jansen, B. A. (2010, September/October). Internet filtering 2.0: Checking intellectual freedom and participative practices at the schoolhouse door. *Knowledge Quest, 39*(1), 46-53. Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=2184630911&sid=3&Fmt=3&clientId=17038&RQT=309&VName=PQD

Jeon, W., Lee, Y., & Won, D. (2011). In M.J. Smith & G. Salvendy (Eds.) Human interface and the management of information. *Interacting with Information Symposium on Human Interface 2011, Held as Part of HCI International 2011: Orlando, FL, July 9-14, 2011* (pp. 548-557, Proceedings, Part I). New York: Springer Heidelberg.

Johnson, D. (2012). Power Up!: Filtering fallacies. *Educational Leadership, 70*(4), 86-87.

King, A. V. (2010, April). Constitutionality of cyberbullying laws: Keeping the online playground safe for both teens and free speech. *Vanderbilt Law Review, 63*(3), 845-884. Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=2043375811&sid=1&Fmt=4&clientId=17038&RQT=309&VName=PQD

Koumartzis, N., & Veglis, A. (2012). Internet regulation, a new approach: Outline of a system formed to be controlled by the Internet users. *Computer Technology and Application, 3*(1), 16-23. Retrieved from http://web.ebscohost.com.ezproxylocal.library.nova.edu/ehost/pdfviewer/pdfviewer?sid=e5142521-e1e6-4ffd-8b8a-0636c34b47fd%40sessionmgr15&vid=4&hid=14

Leberknight, C. S., Chiang, M., & Wong, F. M. (2012). A taxonomy of censors and anti-censors: Part I-impacts of internet censorship. *International Journal of E-Politics (IJEP), 3*(2), 52-64. doi:10.4018/jep.2012040104

Lefever, S., Dal, M., & Matthiasdottir, A. (2007, July). Online data collection in academic research: Advantages and limitations. *British Journal of Educational Technology, 38*(4), 574-582. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a1e7ee0da2ac7111d296049bb53a2ece2fb5257b099540b57&fmt=P

Lemke, C., Coughlin, E., Garcia, L., Reifsnerder, D., & Baas, J. (2009). *Leadership for Web 2.0 in education: Promise and reality*. Retrieved from Consortium for School Networking website: http://www.cosn.org/Initiatives/Web20LeadershipPolicy/LeadershipWeb20Report/tabid/5359/Default.aspx

Loertscher, D. V. (2009, June). Access to technology in transition. *Teacher Librarian, 36*(5), 46-48. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a11572fffa46aad427f4924e2e3d895b301d8333e5eb1baef&fmt=P

Losh, E., & Jenkins, H. (2012, September/October). Can public education coexist with participatory culture? *Knowledge Quest, 41*(1), 17-21. Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1076399985?accountid=6579

Losinski, R. (2009). Patrolling Web 2.0. In R. J. Stein (Ed.), *The Reference Shelf: Vol. 81. Internet safety* (pp. 96-98). New York: H.W. Wilson Company.

Macleod-Ball, M. (2011) Student speech online: Too young to exercise the right to free speech? *I/S: A Journal of Law and Policy for the Information Society, 7*(1), 102-132.

Manzo, K. K. (2009, September 5). Filtering fixes: District leaders make changes to offer greater online access to students. *Education Week, 29*(3), 23-25. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a11572fffa46aad4228c3dcabefeb923948b32d33970eb4b6&fmt=P

Manzo, K. K. (2010, February). Digital innovation outpaces E-rate policies. *Education Week, 29*(20), 1, 16. Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/202697324?accountid=6579

Marie, K. L., & Weston, J. (2009). Survey says: Online survey tools for library assessment. *Library Media Connection, 28*(2), 50-53. Retrieved from http://web.ebscohost.com.ezproxylocal.library.nova.edu/ehost/pdfviewer/pdfviewer?sid=b13b2feb-79c8-408e-bcff-5b73400375f3%40sessionmgr4&vid=9&hid=15

Maycock, A. (2011). Issues and trends in intellectual freedom for teachers and librarians: Where we've come from and where we're heading. *Teacher Librarian, 39*(1), 8-12.

Menuey, B. P. (2009, January). CIPA: A brief history. *Computers in the Schools, 26*(1), 40-47. doi:10.1080/07380560802688265

Miller, N. C., Thompson, N. L., & Franz, D. P. (2009, September). Proactive strategies to safeguard young adolescents in the cyberage. *Middle School Journal, 41*(1), 28-33. Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=1862973141&sid=1&Fmt=3&clientId=17038&RQT=309&VName=PQD

Moyle, K. (2012). Filtering children's access to the Internet at school. *In L. Morris & C. Tsolakidis (Eds.) International Conference on Information Communication Technologies in Education proceedings: Rhodes Island, Greece, July 5-7, 2012* (pp. 403-412). Retrieved from http://www.icicte.org/Proceedings2012/Papers/10-3-Moyle.pdf

Nantais, M., & Cockerline, G. (2010). Internet filtering in schools: Protection or censorship? *Journal of Curriculum and Pedagogy, 7*(2), 51-53. Retrieved from http://dx.doi.org/10.1080/15505170.2010.10471340

National Conference of State Legislatures. (2013). *Children and the Internet: Laws relating to filtering, blocking and usage policies in schools and libraries*. Retrieved from http://www.ncsl.org/issues-research/telecom/state-internet-filtering-laws.aspx

National Cyber Security Alliance, Educational Technology Policy, Research and Outreach, Microsoft Corporation, & Zogby International. (2010, February). *Cyberethics, cybersafety and cybersecurity curriculum in the United States*. Retrieved from http://staysafeonline.mediaroom.com/file.php/107/Full+Survey+Results+2010+State+of+K-12+Cyberethics%2C+Cybersafety%2C

Neighborhood Children's Internet Protection Act (NCIPA), 47 U.S.C. § 254, http://www.gpo.gov/fdsys/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf

Nicoletti, P. (2009). Content filtering. In J. R. Vacca (Ed.), *Computer and information security handbook* (pp. 723-744). Burlington, MA: Morgan Kaufmann Publishers.

Online Safety and Technology Working Group. (2010, June 4). *Youth safety on a living Internet: Report of the Online Safety and Technology Working Group*. Retrieved from National Telecommunications and Information Administration website: http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_070610.pdf

Ott, J., Beard, M., Blue, D., Cleugh, C., Greenfield, D. Lee, T., ...Stager, G. (2010). *Examining Internet filtering policies and practices to increase student technological learning opportunities.* Retrieved from the Education News Website: http://www.educationnews.org/ed_reports/95634.html

Partnership for 21st Century Learning. (2011). *Framework for 21st century learning*. Retrieved from http://www.p21.org/overview/skills-framework/264

Pierce, D. (2010, February 26). *Study: Too few schools are teaching cyber safety*. Retrieved from eSchool News website: http://www.eschoolnews.com/2010/02/26/study-too-few-schools-are-teaching-cyber-safety/

Pierce, M. (2012). Equal measure: Shielding students and enabling access. *T H E Journal (Technological Horizons in Education), 39*(2), 36-40. Retrieved from http://go.galegroup.com.ezproxylocal.library.nova.edu/ps/i.do?id=GALE%7CA284937282&v=2.1&u=novaseu_main&it=r&p=AONE&sw=w

Protecting Children in the 21st Century Act**,** Pub. L. No. 110-385, Tit. II, 122 Stat. 4096 (2008), *codified at* 47 C.F.R. §§54.520(c)(1)(i), 54.520(c)(2)(i).

Quillen, I. (2010, October 20). Web 2.0 fuels content filtering debate. *Education Week's Digital Directions, 4*(1), 20-21. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a6bc6ad4ad1109d2844f79742e396decd4993bd121a91da19&fmt=P

Quillen, I. (2011, August 24). ACLU files first school suit over LGBT Website filtering. *Education Week, 31*(1), 4. Retrieved from http://go.galegroup.com.ezproxylocal.library.nova.edu/ps/i.do?id=GALE%7CA266147510&v=2.1&u=novaseu_main&it=r&p=AONE&sw=w

Ramaswami, R. (2010). Nothing to LOL about. *T.H.E. Journal*, 37(6), 24-30. Retrieved from http://web.ebscohost.com.ezproxylocal.library.nova.edu/ehost/pdfviewer/pdfviewer?vid=3&hid=28&sid=7e6132ef-d737-4b32-baf7-3c12e17f5d35%40sessionmgr114

Rea, L. M., & Parker, R. A. (2005). *Designing and conducting survey research: A comprehensive guide*. San Francisco: Jossey Bass.

Robinson, L. K., Brown, A.H., & Green, T. D. (2010) *Security vs. access: Balancing safety and productivity in the digital school*. Eugene, OR: International Society for Technology in Education.

Rodgers, D. J. (2012). *The social media dilemma in education: Policy design, implementation and effects* (Doctoral dissertation, University of Southern California). Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1151845695?accountid=6579

Selamat, A., Zhi Sam, L., Maarof, M., & Shamsuddin, S. (2011). Improved Web page identification method using neural networks. *International Journal of Computational Intelligence & Applications, 10*(1), 87-114. doi:10.1142/S1469026811003008

Shearer, K. M. (2010). Blogging and Internet filters in schools. *Community and Junior College Libraries, 16*(4), 259-263. doi: 10.1080/02763915.2010.526913

Simkins, M., & Schultz, R. (2010, January/February). Using Web 2.0 tools at school. *Leadership, 39*(3), 12-38. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a6bc6ad4ad1109d28934ff70f47df46fd1626ceff23cc0c85&fmt=H

Spurlin, C. J., & Garry, P. M. (2009). Does filtering stop the flow of valuable information?: A case study of the Children's Internet Protection Act (CIPA) in South Dakota. *South Dakota Law Review, 54*(1), 90-96. Retrieved from http://vnweb.hwwilsonweb.com.ezproxylocal.library.nova.edu/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e5912177bf56e509a807214e88588c3dd90d539fc9452d963d70483e086f855eb&fmt=P

Staino, R. (2009, August 17). TN school district dumps filters that blocks LGBT sites. *School Library Journal*. Retrieved from http://www.schoollibraryjournal.com/article/CA6676896.html

Supreme Court rejection nixes COPA. (2009, March). *American Libraries, 40*(3), 18-19. Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=1650602161&sid=2&Fmt=3&clientId=17038&RQT=309&VName=PQD

Sutton, L. (2012). Internet filtering software and its effects. In M. J. Bates (Ed.), *Understanding information retrieval systems: Management, types and standards* (pp. 537-544). Boca Raton, FL: CRC Press, Taylor & Francis Group.

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Thousand Oaks, CA: Sage.

Thomas, T., & Stoddard, D. (2012). *Network security first-step* (2nd ed.). Indianapolis, IN: Cisco Press.

Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969).

Tseng, V. (2012). The uses of research in policy and practice. *Social Policy Report, 26*(2), 1-24. Retrieved from http://www.wtgrantfoundation.org/resources/studying-the-use-of-research-evidence

United States v. American Library Association, 123 U.S. 2297 (2003).

U.S. Constitution. amend. I.

U.S. Department of Education. (2010, November). *Learning powered by technology: National educational technology plan (NETP)*. Retrieved from http://www.ed.gov/sites/default/files/netp2010.pdf

U.S. Department of Education, National Center for Educational Statistics. (2012). *Digest of Educational Statistics 2011* (NCES Publication No. 2012-001). Retrieved from http://nces.ed.gov/pubs2012/2012001.pdf

Varadharajan, V. & Cohen, F. (2010). Internet filtering: Issues and challenges. *IEEE Security and Privacy, 8*(40), 62-65. doi: 10.1109/MSP.2010.131

Willard, N. (2010a, May/June). Security in a Web 2.0-based educational environment. *Multimedia & Internet@Schools, 17*(3), 8-11. Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/323808358?accountid=6579

Willard, N. (2010b, September/October). Teach them to swim. *Knowledge Quest, 39*(1), 54-61. Retrieved from http://proquest.umi.com.ezproxylocal.library.nova.edu/pqdweb?did=2184630911&sid=3&Fmt=3&clientId=17038&RQT=309&VName=PQD

Williams, A., & Protheroe, N. (2008). *How to conduct survey research: A guide for schools*. Alexandria, VA: Educational Research Service.

Yan, Z. (2010). Do high school students benefit from the children's internet protection act? In R. Zheng, J. Burrow-Sanchez, & C. Drew (Eds.), *Adolescent Online Social Communication and Behavior: Relationship Formation on the Internet* (pp. 103-119). Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-926-7.ch007

Ye, J. (2007). Overcoming challenges to conducting online surveys. In *Handbook of research on electronic surveys and measurements* (pp. 82-87). Retrieved from http://www.igi-global.com.ezproxylocal.library.nova.edu/gateway/contentowned/chapter.aspx?titleid=20219

Zwang, J. (2011, July/August). Filtering software to meet ACLU's concerns. *eSchool News, 14*(7), 21.