Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference

Portia Pusey and William A. Sadera
Towson University

Abstract

In teacher education programs, preservice teachers learn about strategies to appropriately integrate computer-related and Internet-capable technologies into instructional settings to improve student learning. Many presume that preservice teachers have the knowledge to competently model and teach issues of safety when working with these devices as well. This study investigated the current knowledge and understandings preservice teachers have about cyberethics, cybersafety, and cybersecurity (C3) topics and their beliefs about their ability to teach them. The researchers conducted a survey with 318 preservice teachers asking them to rate their ability to model or teach 75 C3 topics. The results indicated that the respondents were not prepared to model or teach C3 topics. (Keywords: Internet safety, cyberethics, cybersecurity, cybersafety, preservice teacher education)

The Pandora's Box of Internet-capable technology has long been open for K–12 education. With its gift of greater resources for learning, communication, and collaboration comes its dangers of physical and emotional harm to its users, their data, and the organizations where they work and learn (Berkman Center for Internet & Society at Harvard University, 2008; National Center for Missing & Exploited Children & Cox Communications, 2006; National Cyber Security Alliance & Norton by Symantec, 2010). Although learning institutions have been quick to profit from the Internet's gifts, they have been slow to recognize their responsibility to educate their communities about cyberethics, cybersafety, and cybersecurity (C3).

This paper reports the results of a survey-based study designed to collect data regarding preservice teacher knowledge about, and preparedness to teach, C3 content in their future teaching. The results of this study will be the first to provide information about preservice teacher knowledge of C3 topics and an understanding about where preservice teachers stand in regard to teaching and modeling these topics in their own instruction. The results of this research will help teacher preparation programs to develop strategies for addressing these topics in their curriculum to better prepare preservice teachers to integrate C3 in their future teaching.

Review of Literature

Cyberethics, cybersafety, and cybersecurity, also known as C3, are three overlapping domains of knowledge (Pruit-Mentle, 2001). Cyberethics are the moral choices individuals make when using Internet-capable technologies and digital media. Cyberethics issues include copyright, online etiquette, hacking, and online addiction(s). Cybersafety consists of the actions individuals take to minimize the dangers they could encounter when using Internet-capable technology. Cybersafety issues include online predators and unwanted communications, viruses, and spyware. This domain also involves building an awareness of how a person's behaviors can contribute to the spread of malware and ways individuals are tricked while using Internet-capable technologies (e.g., phishing, pharming, and spoofing). Cybersecurity involves the technical interventions that protect data, identity information, and hardware from unauthorized access or harm. Cybersecurity includes antivirus software, Internet content filters, firewalls, and password protection. The examples included with each definition are a subset of all the potential topics that could be included to illustrate the C3 content; they are a collection of issues that are reflective of the domain.

Addressing these domains and solving these cyberproblems are often seen as "someone else's" responsibility. Pruit-Mentle (2008) found that cyberethics is often seen as the responsibility of parents, whereas cybersecurity is the responsibility of the information technology (IT) department. However, the authors of this study argue that C3 should be the responsibility of all, and addressing the dearth of knowledge and developing a sense of responsibility can start with teachers and teacher educators.

Laws and Professional Standards

Laws and professional educational standards regarding C3 in K–12 schools direct teacher practice. In the past 10 years, two federal laws have been passed that affect K–12 education. The Children's Internet Protection Act (CIPA) requires schools to have a clear Internet safety policy and to protect students from contact with objectionable content through the use of Internet filters. The Broadband Data Improvement Act (2008) requires appropriate online behavior to be taught in schools. The National Educational Technology Standards (NETS) also require that C3 content be taught in schools (International Society for Techonology Education, 2008). However, these requirements are general and vague in their design and recommendations.

Current Research

The most significant research in this field to date is the C3 Baseline study

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.

conducted with inservice teachers (Pruitt-Mentle, 2008). This large-scale study suggests that many schools, school systems, and districts address the laws and standards for covering C3 content by addressing only plagiarism and cyberbullying (Pruitt-Mentle, 2008). Although important, these topics represent only two of the many topics included within the C3 domains. The C3 Baseline Study provides researchers a glimpse at C3 content integration that can be used for future comparisons with inservice teachers (Pruitt-Mentle, 2008). However, at the moment, we know very little about how colleges of education are preparing preservice teachers to fulfill their obligations to professional standards and legal requirements related to C3. These vague recommendations may be the reason for the lackluster coverage of C3 content in K–12 schools.

News stories and research studies indicate that malware, plagiarism, privacy, and the protection of identity data are only some of the many issues confronting today's school-age children (Berkman Center for Internet & Society at Harvard University, 2008; Lenhart, 2010; Lenhart, Ling, & Campbell, 2010; West, 2009). In a recent study, Cranmer and Selwyn (2009) noted that children ages 7–11 lack a fundamental understanding of the risks to their personal safety and data. Cranmer and Selwyn, (2009), along with several other researchers (LaRose, Rifon, & Enbody, 2008; Sharples, Graber, Harrison, & Logan, 2009), have called for positive messaging across the curriclum for all grade levels to help build a student's ability to use Internet-capable technology in more safe, secure, and ethical ways. Acording to Pruitt-Mentle (2008), this cannot be done with the current C3 knowledge and confidence level of many inservice teachers.

C3 and Preservice Teachers

The current body of research, involving preservice teachers and C3 issues, focuses predominantly on privacy and conduct issues related to social networks (e.g., Carter, Foulger, & Ewbank, 2008; Foulger, Ewbank, Kay, Popp, & Carter, 2009; Kist, 2008). Only one study in the past 5 years evaluated an instructional intervention to present C3 content to future educators (Wollard, Wickens, Powell, & Russell, 2009). However, we cannot design instructional interventions for preservice teachers without understanding their existing knowledge about C3 issues and thier ability to address C3 issues in their future teaching. Perhaps a C3 baseline study in teacher education has yet to be completed because the current population of preservice teachers has been identfied as "digital natives" (Prensky, 2001). It is often assumed that digital natives, including current preservice teachers, already know C3 because they have grown up surrounded by technology and speak technology "without an accent." Although this generation can operate the newest cell phone without reading the instruction booklet, Prensky (2001) does not speak to issues of ethics, safety, and security in his analogy of being a digital native. A baseline study of preservice teacher C3 content knowledge needs to be conducted to learn if preservice teachers are prepared and have the necessary knowledge to integrate it into their future teaching. Teacher education programs model and teach effective technology integration across the curriculum and across all grade levels. As we prepare future teachers to integrate technology into their teaching we should prepare them to integrate C3 content as well. Educators have a long history of including important safety and security topics in the classroom that affect students outside of the classroom; "Stop, drop, and roll" and "Look both ways before crossing the street" are now second nature, thanks to educators' efforts. C3 will never become second nature without training preservice teachers to integrate and model interventions that will help today's students overcome the vulnerabilities and dangers they confront when using Internet-capable technologies inside and outside the classroom.

Method

This survey-based research makes an important distinction in C3 knowledge that is essential for future teachers and teacher educators. Awareness of C3 content is not adequate for a teaching professional; this study asked whether preservice teachers are prepared to model or teach C3 content in their classrooms. Knowing what C3 content knowledge preservice teachers are prepared to model or teach will enable preservice teacher preparation programs to improve curricula to integrate essential C3 content. The purpose of this research was to investigate preservice teacher C3 knowledge and identify what C3 topics preservice teachers report that they currently know well enough to model or teach.

Setting and Sample

Participants were solicted for this research from a Mid-Atlantic university college of education undergraduate introductory technology integration course. This technology integration course is required for preservice teachers in all but one major (early childhood majors have the option to take their own version). The majority of students in this course are undergraduate students in their sophomore and junior year of study. The course, titled Integrating Instructional Technology, is designed to introduce preservice teacher candidates to the various forms of electronic and digital technology and to provide opportunities for engagement and reflection on the role these technology tools can play in a teaching/learning environment. Through this course, the students become skilled in using the many digital tools found in today's schools. In addition, the course exposes students to basic learning theory and assists them in determining appropriate applications of these theories and techniques in educational settings. The course is designed to help preservice teachers meet both state and national technology standards for teachers (e.g., ISTE's NETS•T). Topics covered in the course include, but are not limited to Web 2.0 (i.e., blogs and wikis), online learning, multimedia, digital storytelling, Universal Design for Learning (UDL), instructional theory, and technology integration strategies. At the time of this study, copyright was a standard topic

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.

Table 1. Participant Demographics

Demographic	*n*
Gender	
Male	69
Female	249
Age	
18–22	261
23–28	37
29–33	8
34+	12
Major	
Early Childhood Education	15
Elementary/Middle Education	135
Secondary Academic Areas	108
Special Education	41
Other	19
Who owns the computer you use most frequently?	
Me	287
My parents and I	18
School	7
Other	5
Length of Computer Ownership (years)	
0–1	60
2–3	132
4–5	71
6–7	21
8–9	10
10+	24

found on course outlines, but no other C3 topics were formally covered.

Seventeen sections of the course were asked to complete the C3 Awareness and Instructional Preparedness Instrument in a series of semesters between 2008 and 2010. To maximize the response rate, the researcher attended each of the 17 sections of the course to administer the survey. The researcher assured the participants that they would be anonymous, that they were not required to participate, and that their decision regarding participation would not affect their course grades.

The sample resulted in 318 completed surveys (69 males, 249 females) with a 100% response rate (see Table 1). The mean age of the participants was 22 years old (ranging from 18 to 56). The selected majors for this group are proportionately representative of the university's college of education (except for early childhood majors, who have the option to enroll in a different course): 4.7% (15) early childhood education, 42.7% (135) elementary education, 34.2% (108) secondary academic areas, and 13.0% (41) special education (see Table 1). Ninety percent of the participants reported that they had owned their own computers for a mean of 3.88 years; 94% of these students also said they maintain their own computers. Twelve of the participants indicated that they have taken a computer security course.

Instrumentation

The researchers designed the C3 Awareness and Instructional Preparedness Instrument and used it over the course of 2 years to gather data for this study. They developed the C3 Awareness and Instructional Preparedness Instrument to assess preservice teachers' self-reported ability to model or teach 75 C3 topics in their classrooms. They developed and pilot-tested the online survey instrument in 2008 with a similar sample and determined that it was reliable (Phi = .246, p = .000, χ^2 = 40.593, df = 1, α = .997). The researchers have used this survey repeatedly during this time without changing it; the reliability of the instrument has been consistent with the pilot data. The C3 Awareness and Instructional Preparedness Instrument has 98 questions and requires approximately 20 minutes to complete. The instrument consists of three sections, including: Background Information, C3 Knowledge, Awareness and Instructional Preparedness.

Background Information. The Background Information section asked students their age, gender, student standing (freshman, sophomore, etc.), and major. Additionally, this section was designed to collect data about the participants' experiences and the number of computer courses they have taken. This section asked participants about the ownership, length of ownership, and maintenance of the computer the participants used most often. Finally, this section asked participants to describe any computer-related courses, including computer security, they have taken.

C3 Knowledge. The C3 Knowledge section included a 10-item test of factual C3 knowledge using a multiple-choice format. This section of the instrument measured the preservice teachers' knowledge about the following topics: virus scanning software updates, e-mail attachments, proxy servers, pop-up ads, portable data storage devices, firewalls, the Children's Internet Protection Act (2000), the Children's Online Privacy Protection Act of 1998, the Family Education Rights and Privacy act of 1974, and passwords. Following is an example of a C3 Knowledge section question regarding e-mail attachments:

It is fine to open an e-mail attachment without first scanning it for viruses:

☐ When it comes from a reliable source
☐ When it comes from a bank or other commercial institution
☐ When the subject line contains personal information about you
☐ All of the above
☐ None of the above
☐ I don't know

In this example, "None of the above" is the correct answer. The purpose of this section was to gather reliable data about the participants' C3 knowledge. "I don't know" was included as the last choice for each of the C3 Knowledge items to ensure accuracy of knowledge and keep respondents from guessing. The researchers informally shared the instrument with

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.

experts to ensure accuracy of the statements and responses.

Awareness and Instructional Preparedness. The Awareness and Instructional Preparedness section asked participants to rate their ability to model or teach 75 C3 topics. The researchers initially developed the list of C3 topics through a review of the literature. Once the list of C3 topics was compiled, it was subjected to a content validity review by three experts. The experts included a member of the computer science faculty at the researchers' institution, a member of a national organization focused on promoting knowledge and awareness of C3, and an expert from the National Center for Missing and Exploited Children's online C3 awareness division.

Each of the experts received the initial list and was asked to review it to ensure it included the most current and important C3 topics for students as well as educators. Only one addition was made to the initial list. The final list of 75 C3 topics included the 10 topics from the C3 Knowledge section as well as other current topics, such as spyware, cookies, defamation, copyright, key loggers, phishing, proxies, spoofing, and webcams.

The researchers presented the 75 items to the participants in a table format and then asked the preservice teachers to rate their ability to model or teach the C3 topic using the following 4-point Likert-type scale choices:

1: I have never heard anything about this.
2: I have heard about this but, I am not sure what it means.
3: I know about this, but I could not model or teach it to others.
4: I know about this, and I could model or teach it to others.

This scale had only four levels, as research has suggested that respondents should be presented with fewer than seven categories (Miller, 1956). The scale was designed to use the minimum number of choices that would still present a clear-cut differentiation between the responses. The terms model and teach were used as part of this scale to emphasize a deeper understanding of the topic, and that this knowledge can be shared and put into practice. Moreover, the terms model and teach were used in tandem, because espousing good practice involves ownership of the material beyond the ability to teach about it. The analysis of the pilot study data indicated that this four-level scale provided adequate precision about a participant's level of knowledge or skill. The Cronbach's alpha reliability coefficient for this section of the instrument was .999

The researchers conducted further analysis to confirm reliability between the self-reported C3 Knowledge and the Awareness and Instructional Preparedness data by recoding the data and calculating a Phi value. The researchers conducted this reliability analysis using the data from the 10 C3 Knowledge items and the corresponding 10 Awareness and Instructional Preparedness items. First, they recoded data from both sections into binary format., coding data from the C3 Knowledge items as "1" for a correctly answered question or "0" for an incorrectly answered question. Second, the researchers recoded correlating Awareness and Instructional Preparedness items based on participants' self-reported knowledge, coding responses as "0" for if the respondent was unsure or had no knowledge of the technology or issue and "1" if the respondent had some knowledge or belief in his or her ability to teach it. The researchers then correlated the recoded data for these 10 paired items using Phi. The researchers assumed that if a sample of 10 items from the Awareness and Instructional Preparedness data can be verified as reliable, then the self-reported data for all 75 C3 topics from this section will be inferred to be reliable. The Phi analysis indicated a high correlation between the C3 Knowledge and the Awareness and Instructional Preparedness data (Phi = .293, $p = .000$, $\chi^2 = 295.69$, $df = 1$).

Results

Awareness and Instructional Preparedness

To address the focus of this research and specifically identify the preservice teachers' C3 knowledge and self-reported ability to model or teach these topics, the researchers used descriptive analysis to aggregate and determine means from the responses for the Awareness and Instructional Preparedness section. Based on the means, two thresholds were operationally defined. Means greater than 3.5 indicated C3 content that preservice teachers felt they were "prepared to teach." Means less than 2.5 indicated that C3 content preservice teachers felt they were "not prepared to teach". The latter was further stratified to include "never heard anything about this" and "I have heard about this but, I am not sure what it means." Table 2 (p. 86) presents the means for all 75 topics.

The results of the descriptive analyses indicated that preservice teachers reported weak knowledge of the 75 topics included in this instrument, as only 20% (15) of the topics had a mean greater than 3. Moreover, participants reported they could model and teach only .05% (4) of the 75 C3 topics. In contrast, preservice teachers reported no or uncertain knowledge of 56% (42) of the 75 C3 topics; these topics include the four federal laws that regulate student rights, school policy, and the types of data the teachers must protect.

Prepared to teach. Four C3 topics received high means (greater than 3.5) indicating that participants believed they could model or teach this content. These topics included activities that are frequently associated with this generation, such as attachments (e-mail), text messaging, cell phones, and plagiarism. Current research (Jones, 2009; Lenhart, Purcell, Smith, & Zickuhr, 2010) notes that these technologies are commonplace in this generation. Plagiarism, although different, is a topic that is commonly addressed in educational settings (Pruitt-Mentle, 2008; Pruitt-Mentle & Pusey, 2010).

Unprepared to teach. At the other end of the knowledge continuum are C3 topics that the participants rated with a mean less than 1.5. These are C3 topics participants indicated they have "never heard anything about." Nine topics that received this low rating: tricklers, zombies, sniffing, script kiddies, the Health

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.

Table 2. Preservice Teacher Self-Rating of Ability to Teach C3 Topics

Topic	*n*	*M*	*SD*	95% CI	Topic	*n*	*M*	*SD*	95% CI
Cell phones	317	3.76	0.65	[3.69, 3.83]	Pirating	315	2.33	1.11	[2.21, 2.45]
Text messaging	316	3.70	0.73	[3.62, 3.78]	Ports	313	2.13	1.02	[2.02, 2.25]
Attachment (e-mail)	314	3.55	0.73	[3.47, 3.63]	Defamation	315	2.06	1.12	[1.94, 2.18]
Plagiarism	316	3.51	0.78	[3.42, 3.59]	Hijack	314	2.01	0.89	[2.01, 2.20]
Password	316	3.41	0.81	[3.32, 3.50]	Acceptable use policies	316	2.00	0.94	[1.89, 2.10]
Posting videos and pictures	314	3.35	0.79	[3.27, 3.44]	Adware	316	1.98	0.89	[1.88, 2.07]
Online games	317	3.27	0.81	[3.19, 3.36]	Encryption	316	1.90	0.85	[1.81, 2.00]
Wireless devices	315	3.19	0.86	[3.10, 3.29]	Child-safe portals	310	1.89	0.9	[1.79, 1.99]
E-mail (not encrypted)	317	3.14	0.96	[3.04, 3.25]	Phishing	316	1.88	0.97	[1.77, 1.99]
Social networking	317	3.13	1	[3.02, 3.24]	End user license agreement	317	1.86	0.89	[1.76, 1.95]
Pop-up ads	313	3.12	0.83	[3.03, 3.21]	Walls	314	1.82	0.91	[1.71, 1.92]
Copyrights	317	3.11	0.83	[3.02, 3.20]	Tracking cookies	314	1.80	0.89	[1.7, 1.89]
Webcams	315	3.11	0.86	[3.02, 3.21]	Digital certificates	313	1.69	.859	[1.60,1.79]
Privacy	316	3.09	0.83	[3.00, 3.18]	Denial of service	317	1.69	0.86	[1.6, 1.79]
Portable data storage devices	313	3.03	1.02	[2.92, 3.15]	Social engineering	317	1.67	0.91	[1.56, 1.77]
Blogs	318	2.97	0.87	[2.87, 3.06]	Profile audit	316	1.67	0.89	[1.57, 1.77]
Cyberbullying	318	2.93	1.03	[2.82, 3.05]	Archived documents	317	1.66	0.81	[1.57, 1.75]
Spam	317	2.90	0.84	[2.80, 2.99]	Disposal of technology	317	1.66	0.85	[1.57, 1.76]
Identity theft	315	2.90	0.8	[2.81, 2.99]	Children's Internet Protection Act	318	1.65	0.79	[1.56, 1.74]
Software updates	316	2.89	0.86	[2.79, 2.98]	Proxies	316	1.65	0.8	[1.56, 1.74]
Internet predator	314	2.79	0.95	[2.57, 2.71]	Cached Web sites	317	1.62	0.85	[1.52, 1.71]
Spyware	315	2.78	0.92	[2.37, 2.58]	Patches	317	1.61	0.92	[1.51, 1.72]
Copy machines with hard drives	318	2.74	0.93	[2.64, 2.84]	Key logger	315	1.58	0.86	[1.49, 1.68]
American Disabilities Act	317	2.67	1	[2.56, 2.79]	Exploit	315	1.57	0.77	[1.49, 1.66]
Digital altering of images	317	2.66	.999	[2.55,2.77]	Spoofing	316	1.56	0.85	[1.46, 1.65]
Secure sites	316	2.64	0.97	[2.53, 2.75]	"Fair Use" exemption	315	1.55	0.85	[1.46, 1.65]
Spam filters	317	2.63	0.93	[2.53, 2.73]	The Children's Online Privacy Protection Act 1998	315	1.51	0.72	[1.43, 1.59]
Online identities	316	2.62	0.99	[2.51, 2.73]	Family Educational Rights and Privacy Act 1974	314	1.5	0.76	[1.47, 1.63]
Hate groups	313	2.61	1.01	[2.50, 2.72]	Back doors	316	1.49	0.8	[1.4, 1.58]
Security setting	316	2.61	0.99	[2.50, 2.72]	Bypassing filters	318	1.46	0.74	[1.38, 1.54]
Gambling (online)	317	2.60	0.86	[2.50, 2.69]	Bot	318	1.45	0.85	[1.36, 1.55]
Hacking	316	2.53	0.86	[2.43, 2.62]	"Sticky" Web sites	314	1.43	0.75	[1.34, 1.51]
File sharing	314	2.52	0.98	[2.41, 2.63]	Health Insurance Privacy Act 1996	313	1.39	0.68	[1.32, 1.47]
Firewalls	316	2.50	0.81	[2.41, 2.59]	Script kiddies	313	1.32	0.66	[1.24, 1.39]
Internet filters	314	2.49	0.95	[2.57,2.71]	Sniffing	315	1.30	0.67	[1.23, 1.38]
Permissions	316	2.47	1.03	[2.35, 2.58]	Zombie	317	1.29	0.63	[1.22, 1.36]
Malware: virus, worm, trojan	315	2.43	0.94	[2.33, 2.54]	Trickler	316	1.23	0.55	[1.17, 1.29]
Cookies	318	2.34	0.86	[2.24, 2.43]					
Overall mean		2.30							

Note: Self-ratings were based on a 4-point Likert-type scale: 1 = I have never heard anything about this; 2 = I have heard about this, but I am not sure what it means; 3 = I know about this, but I could not model or teach it to others; 4 = I know about this, and I could model or teach it to others.

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.

Insurance Portability and Accountability Act of 1996, "sticky" websites, bots, bypassing filters, and back doors. The list is much longer when including items that received a self-reported mean score of 2.5 or less for items in the Awareness and Instructional Preparedness section. This mean score signifies that the preservice teachers "have heard about this but, are not sure what it means." Forty-two C3 topics had a mean of 2.5 or less.

These results indicate that preservice teachers have limited knowledge of C3 content and a poor self-reported ability to model and teach this content to their future students. Participants reported that they had no knowledge or limited knowledge of 60% of the 75 topics presented in the survey. Conversely, they reported that they could model or teach only 4%. These results indicate that the preservice teachers surveyed are not prepared to teach C3 content in their classrooms.

Limitations

The greatest limitation of this research is that C3 content knowledge is constantly changing. Therefore, some of the C3 topics assessed during the survey years of 2008–10 may not present the same level of danger to today's students. For example, one could argue that Internet browsers have improved blocking of pop-up advertising, and this may no longer need to be included. Similarly, some C3 content, such as the vulnerabilities to privacy and identity due to increased adoption of smartphones, has recently become a pressing issue to security experts. It is important to review the literature on C3 prior to replicating this study in future years to assure that the content being assessed represents the most important and current issues of the time.

Discussion

As 90% of the participants in this research state they own computers and the U.S. national average of computer ownership is 76%, it is essential that we all have a strong understanding and knowledge of C3-related issues (Smith, 2010). Every computer owner is the administrator of his or her own computing environment and is vulnerable to the dangers that good C3 knowledge can help prevent. Therefore, computer owners must know more than how the computer and the various programs function; they need to know how to keep themselves and their data safe from harm. Moreover, the safety and stability of the information and communications technology infrastructure depends on the good C3 practice of every citizen (Cyberspace Policy Review, 2009). Teacher education programs must prepare their preservice teachers to model and teach C3 topics and safe computing practices so that future generations will know how to behave ethically as well as to keep themselves safe and secure online.

Most of the preservice teachers in this study, as well as the majority of current preservice teachers, were born during or after a time of nearly ubiquitous access to Internet-capable technologies. These individuals have been classified by Prensky (2001) as digital natives. When Prensky (2001) described these individuals as digital natives, he was referring to their technology experience and capabilities. It is certain that growing up with diverse digital tools and toys has given this generation the ability to use almost any technology without first reading an instruction manual. But his analogy does not translate when considering C3 content. In fact, calling this generation digital natives is premature, based on the findings of this study.

This study reveals that, despite their young demographic and access to technology, the preservice teachers surveyed do not possess adequate C3 knowledge nor the ability to teach their future students to keep themselves and their data safe from harm. This is in conflict to the digital native analogy, as natives would know what clues in the environment indicate they are safe and protected. However, the participants in this study—the "natives"—reported that they are unaware of the clues in digital environments that can indicate threats to themselves, their students, and the environments where they work and learn.

It appears that knowledge of good C3 practice is not innate and is not openly passed from one person to another. This study demonstrates the need for C3 content to be taught and modeled in preservice teacher education programs. Moreover the need to address the lack of knowledge about C3 issues must also become part of a regular discussion in schools and public forums. One might argue that school is not the proper place to teach these topics. In fact, a recent survey indicated that inservice teachers place the responsibility for C3 in the realm of parents, library media specialists, and the IT department (Pruitt-Mentle, 2008). Just as we teach our children about safety on the street, strangers, and fire, it is the responsibility of everyone, including educators, to teach K–12 children how to protect themselves in the digital world as well.

Beyond the protected school's computing environment is the unprotected environment of home computers and libraries where kids do their homework and play. The preservice teachers in this study reported that they know little about the dangers that their students face when they are using technology in less-sheltered environments. Teacher preparation programs must address this knowledge deficit so that our future teacher population can model and teach this content to K–12 students and integrate C3 throughout the curriculum. This study demonstrates that preservice teachers need to acquire the C3 knowledge and skill to protect themselves and their data first. Colleges of education need to include this technical information in their curricula before helping preservice teachers integrate C3 into their teaching. The results of this study have been used to guide the implementation of a learning unit into preservice teacher education, which develops preservice teacher C3 knowledge and skills before it contextualizes the C3 content for K–12 students. Further research should be completed to determine the best methods to integrate this content into preservice teacher education and professional development for inservice teachers. Until C3 becomes second nature to every citizen, including both digital natives and immigrants, we will be mere tourists who are subject to the dangers that only locals know about.

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.

Author Notes

Portia Pusey is the assistant director at Educational Technology Policy, Research, and Outreach (ETPRO), which is the lead organization for CyberWatch K12. She is also studying to earn her doctorate of education degree in the instructional technology doctoral program at Towson University. Her research interests include STEM career pipeline development, extended learning opportunity models, and cyberethics, effective cybersafety , and cybersecurity awareness education. E-mail: ppusey@edtechpolicy.org

William A. Sadera is an associate professor of instructional technology in the College of Education in the Department of Educational Technology and Literacy at Towson University. He teaches courses in instructional technology and serves as the director of the instructional technology doctoral program. He publishes regularly and presents at scholarly and practitioner-oriented conferences. His research interests include inservice and preservice teacher technology preparation, effective integration of classroom technology, and online learning. Please send correspondence to William Sadera, College of Education, Towson University, 8000 York Rd, Towson, MD 21252. E-mail: bsadera@towson.edu

References

Berkman Center for Internet & Society at Harvard University. (2008, December 31). *Enhancing child safety & online technologies.* Retrieved from Internet Safety Technical Task Force at http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf

Broadband Data Improvement Act, P. L. No. 110-385 (2008).

Brush, T., Glazewski, K., & Khe, F. H. (2008). Development of an instrument to measure preservice teachers' technology skills, technology beliefs, and technology barriers. *Computers in the Schools , 25*(1/2), 112–128.

Carter, H., Foulger, T., & Ewbank, A. D. (2008). Have you googled your teacher lately? *Phi Delta Kappan , 89*(9), 681–685.

Children's Internet Protection Act , Pub. L. No. 106-554. (2000).

Cranmer, S., & Selwyn, N. P. (2009). Exploring primary pupils' experiences and understandings of 'e-safety.' *Educational Informational Technology, 14*, 127–142.

Cyberspace Policy Review. (2009, March 7). Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Endicott-Popovsky, B. (2009). Seeking a balance: Online safety for our children. *Teacher Librarian, 37*(2), 29–34.

Foulger, T. S., Ewbank, A. D., Kay, A., Popp, S. O., & Carter, H. L. (2009). Moral spaces in MySpace: Preservice teachres' perspectives about ethical issues in social networking. *Journal of Research on Technology in Education, 42*(1), 1–28.

International Society for Techonology Education. (2008). *National educational technology standards for teachers.* Retrieved from International Society for Technology in Education at http://www.iste.org/standards/nets-for-teachers/nets-for-teachers-2008.aspx

i-SAFE. (1998–2009). *i-SAFE curriculum effectiveness.* Retrieved from i-SAFE at http://www.isafe.org/channels/sub.php?ch=op&sub_id=media_curriculum_effectiveness

Jones, S. (2009, January 29). *Generations online 2009.* Retrieved from Pew/Internet & American Life Project at http://www.pewInternet.org/Reports/2009/Generations-Online-in-2009.aspx

Kileen, E. (2009). Internet safety. *Teacher Librarian, 37*(2), 74–74.

Kist, W. (2008). "I gave up MySpace for Len"": New teachers and social networking sites. *Journal of Adolescent & Adult Literacy, 52*(3), 245–247.

LaRose, R., Rifon, N., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3).

Lazarinis, F. (2010). Online risks obstructing safe Internet access for students. *Electronic Library*, 157–170.

Lei, J. (2009). Digital Natives as preservice teachers: What technology preparation is needed. *Journal of Computing in Teacher Education, 25*(3), 87–97.

Lenhart, A. (2010, November 9). *Teens and mobile phones: Exploring safety issues as mobile phones become the communication hubs for American teens.* Retrieved from Pew Internet & American Life Project at http://www.pewInternet.org/Presentations/2010/Nov/fosi.aspx

Lenhart, A., Ling, R., & Campbell, S. (2010, October 23). *Teens, adults & sexting: Data on sending and receipt of sexually suggestive nude or nearly nude images by American adolescents and adults.* Retrieved from Pew Internet & American Life Project at http://www.pewInternet.org/Presentations/2010/Oct/Teens-Adults-and-Sexting.aspx

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010, February 10). *Social media and young adults.* Retrieved from Pew Internet & American Life Project at http://www.pewInternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx

Miller, G. A. (1956). The magical number 7, plus or minus 2: Some limits on our capacity for processing information. *Psychological Review, 63*(2), 81–97.

National Center for Missing & Exploited Children & Cox Communications. (2006, May 11). *New study reveals 14% of teens have had face-to-face meetings with people they've met on the Internet.* Retrieved from National Center for Missing and Exploited Children at http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2383

National Cyber Security Alliance & Norton by Symantec. (2010, October). *2010 NCSA/ Norton by Symantec online safety study.* Retrieved from StaySafeOnline.org at http://staysafeonline.mediaroom.com/index.php?s=67&item=57

Prensky, M. (2001, October). Digital Natives, digital imigrants. *On the Horizon, 9*(5), 1–6.

Pruitt-Mentle, D. (2000). T*he C3 framework: Cyberethics, cybersafety, and cybersecurity implications for the educational setting.* Retreived from http://knowwheretheygo.org/static/content/MATRIX.pdf

Pruitt-Mentle, D. (2008). *2008 National cybersafety, cybersecurity, cyberethics baseline study.* Retrieved from Stay Safe Online at http://staysafeonline.mediaroom.com/index.php?s=67item=44

Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-safety and Web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning, 25*(1), 70–84.

Smith, A. (2010). *Americans and their gadgets.* Retrieved from Pew Research Center's Interent & American Life project at http://pewinternet.org/~/media/Files/Reports/2010/PIP-Americans%20and%20their%20Gadgets.pdf

West, H. (2009, October 1). *Is online privacy a generational issue?* Retrieved from Pew Internet & American Life at http://www.pewInternet.org/Media-Mentions/2009/Is-Online-Privacy-a-Generational-Issue.aspx

Wollard, J., Wickens, C., Powell, K., & Russell, T. (2009). Evaluation of e-safety materials for initial teacher traning: Can "Jenny's Story" make a difference? *Technolgy, Pedagogy, & Education, 18*(2), 187–200.

Copyright © 2011–12, ISTE (International Society for Technology in Education), 800.336.5191 (U.S. & Canada) or 541.302.3777 (Int'l), iste@iste.org, iste.org. All rights reserved.