12-2016

Digital Citizenship in 21st Century Education

Aimee Green Logan
Dominican University of California

Digital Citizenship in 21st Century Education

Aimee Green Logan

A culminating thesis submitted to the faculty of Dominican University of California in partial fulfillment of the requirements for the degree of Master of Science in Education

Dominican University of California

San Rafael, CA

May 2016

This thesis, written under the direction of the candidate's thesis advisor and approved by the department Chair, has been presented to and accepted by the Department of Education in partial fulfillment of the requirements for the degree of Master of Science in Education. The content and research methodologies presented in this work represent the work of the candidate alone.

Aimee Green Logan Candidate	May 17, 2017
Madalienne Peters, Ed.D. Program Chair	May 17, 2017
Suresh Appavoo, Ed.D. First Reader	May 17, 2017

Table of Contents

List of Figures

Abstract

Recent Federal Government initiatives have affected equitable public school funding, which prevents many schools from becoming compliant with the California Common Core Standards. Presently, public schools in California must adopt Common Core State standards, which require the integration of technology within the classroom, however, there are no specific standards and or guidelines within the CCCS that address how students should safely conduct themselves online. This has left students and teachers unprepared to adequately support the growing needs of students online, especially without standards addressing digital literacy. Students who go online face cyberbullying, predatory contact, identity theft and other consequences that may affect their future including the permanence of their digital footprint. Using Howard Gardner and Common Sense Media's end of unit assessment on digital citizenship and Dr. Mike Ribble's Nine Elements of Digital Citizenship, this study inquired into what a sample group of fifth grade students know about digital citizenship. Researcher examined how their knowledge relates to the California Common Core Standards (CCCS) and 21st century skills. The study found that only 32% of the sample group of 88 participants had sufficient knowledge about digital citizenship. The results of this study indicate that the majority of students within this sample are active online without proper knowledge of what digital citizenship means, which may be putting them at risk. A digital citizenship program that addresses access, commerce, communications, etiquette, law, health, wellness, rights and responsibilities, is recommended to support children online.

Acknowledgments

It is with heartfelt gratitude that I offer my thanks to Dr. Suresh Appavoo for his tireless efforts to support me throughout my process of writing my thesis. His patience, determination and dedication to ensuring my success was valiant. A special thank you to Anne Reid who provided her time and expertise in assisting me in research and formatting my thesis correctly. A thank you to my Professors at Dominican who guided and inspired me throughout my midlife transition into becoming a multiple subject elementary school teacher and obtaining my Masters in Education. Your kindness and support of me during this transformative experience was invaluable. Throughout this process, I was fortunate to work with an array of colleagues who challenged me, took me out of my comfort zone and provided companionship throughout this milestone. Your presence, commitment, and focus gave me courage. A whole hearted thank you to my Mom and Dad, my ultimate heroes, for their selfless support and their tough, unconditional love. Your belief in me gave me strength to persevere. From the bottom of my heart, I offer my sincerest gratitude and love. Thank you to my sister, Mimi O'Connell and her family for their faith, generosity and mirth. You were a guiding light. Thank you to my brother Dr. William Scott Green, your warmth and wisdom allowed me to feel safe within the storm. Your home and family became my temple of joy. To Eric Leaf, who offered me tender loving care. The one who stood faithfully by my side as I transformed. You witnessed the heartache, exhaustion and glory. Your commitment and love remained unwavering. I love you. Again, to each of you, I thank you.

Chapter 1: Introduction

The Nigerian Igbo proverb, "Ora na azu nwa" means that it takes a village to raise a child (Crowen-Fletcher, 1994). This proverb means that children benefit from a community upbringing. Each person is limited in their abilities, but there is a wealth of collective resources when a community comes together to support one another. It can be said that this attitude of tribal interconnectedness is still relevant to 21st century education and how we are raising children in a digital age. It raises questions about what our moral, global, and civic responsibilities are, to raise and educate children with a global attunement and perhaps even to a notion of universal citizenship.

The introduction of the world-wide web has changed boundaries within communities and the world as to our moral and civic responsibilities as a global community. The advantages of the world-wide web are that it has enhanced commerce, communication, advanced accessibility of knowledge, and it has brought to the forefront what it means to be digital citizens of the world. As technology advances, it has necessitated ongoing dialogue and policy changes as to how we educate our youth and implement computer technology within the classroom. One of the challenges has been ensuring equitable access to computer technology so that students have the 21st century skills necessary to be prepared for jobs of the future.

Public schools within the United States face issues of inadequate or inequitable funding and changing standards, which affects accessibility, and enhances a digital divide. Digital access and appropriate digital citizenship would allow students to safely optimize the benefits of using the world-wide web, meet varying learning styles and intelligences through online access. The

world-wide web is a vehicle that has opened up the world to those who have digital access and has necessitated a global conversation about what it means to be a digital citizen and what our ethical responsibilities are to children without proper guardianship.

> It is no longer enough for every child to have access to education and to master reading, writing, and math. The global community is now endeavoring to develop students into global citizens, capable of finding solutions for the world's greatest challenges and motivated to instill peace and justice into their communities. Educators must understand these important concepts, such as global citizenship, education for sustainable development, human rights, and the promotion of a culture of peace, that shape children's lives if they are to effectively support children in their development and prepare them for the 21st century. (Bennett, Aguaya, & Field, 2016, p. 23)

When the first personal computer was created in 1981 by IBM, Time Magazine named "The Computer" man of the year, in 1982. Time magazine stated that it is "the end result of a technological revolution that has been in the making for four decades and now, quite literally, hitting home" (Purdue University, 2017, para. 4). In 1984, Apple created the first Mac computer and in 1993, The World Wide Web opened to the general public. The World Wide Web started a global renaissance because information became so readily available and the manner in which people began to communicate changed. The idea of globally connected citizenship arose due to the immediate interconnectedness with the world at large. The advancement of computer technology also began propelling socio-political agendas and about how education should change to prepare students for 21st century skill sets. These agendas lack, "who will own this

challenge of guiding students towards a productive and safe technological society." (Hollandsworth, Dowdy, & Donovan, 2011, para 34).

President Bill Clinton took office in 1993, and during his tenure, made a commitment to bring technology into every classroom by the year 2000. It is now, 2017 and this still continues to be an agenda for each administration that has succeeded him. For over 20 years, the advancement of technology has continued to bloom, and yet the fulfillment of each administration's agenda to make technology available to all public-school classrooms, still remains unfulfilled leaving school districts ill prepared to meet 21st century skills.

After the Bush administration developed the 'No Child Left Behind' Act, and failed due to a lack of funding, the Obama administration developed 'Race to the Top', the public, K-12, education agenda. Race to the Top's agenda is based on accountability and high stakes testing (Onosko, 2011). Common Core State Standards (CCSS) were developed to support this agenda. As of August 2015, forty -two states had adopted the CCSS. (National Governors Association for Best Practices & Council of Chief State School Officers, 2010). In order for public schools to receive funding from being CCSS compliant they needed to have access to computer technology so that students can take standardized tests. A part of the vision for CCSS, was to develop 21st Century learning skills, and ensure that students were college ready.

Since, technology is considered a 21st Century skill for all K-12 students, the use of computers in the classroom is being required to support and reinforce language arts, reading, writing, speaking and listening (California Department of Education, 2016). While technology proficiency is considered a 21st Century skill, CCSS for technology have not been developed, but are expected to be publicized by the year 2019 (CDE, 2016). In 2013, California Governor Jerry

Brown's education policy, the Local Control Funding Formula (LCFF), was signed into law and implemented in California. The 2013 policy replaced old formulas for public school financing. In order for public schools to qualify for funding, they must comply with the new CCCS. In the past, California state school funding was based on categorical programs, which created a complicated and often inequitable distribution of resources, leaving schools who needed more assistance at greater risk (California Department of Education, 2015). The foundation of LCFF was to equalize funding and support schools in need. This has enabled schools in low income areas to be able to become more 21st century compliant.

In 2014, four million students in 36 states adopted CCSS and began online testing (Elkind, 2015). Schools transitioned from paper based testing to digital testing. Schools were required to provide the necessary technology for students to take online tests. While the adoption of the LCFF changed California state funding for public schools, many such schools in low income areas still lacked access to the proper funding.

In a fact sheet put out by the Public Policy Institute of California, public schools receive funding from three sources: the state (57%), property taxes and other local sources (29%), and the federal government (14%), (PPIC, Weston, 2010). Due to the inequality in how schools are funded, many public schools in lower economic areas still struggle with basic operations. Public schools, offset expenses through the Parent Teacher Association (PTA) and fundraising efforts.

Chromebooks have been universally used throughout school districts, due to their lower cost, relative ease of use, and their capability for multiple user sign-ins. This means that multiple students could have access to the Chromebook, with their own identification number. The use of

Chromebooks and the multi-class use of them has enabled many public schools to become 21st century compliant and able to meet the CCSS.

The implementation of CCSS and the necessity of technology within the classroom poses high stake risks for students because districts are operating without explicit technology standards, or a curriculum of how to teach digital citizenship. Digital citizenship involves access, commerce, communications, etiquette, law, rights and responsibilities, health and wellness and law (Ribble, 2011). A permanent digital footprint starts to accumulate the moment a person starts to use the internet." Our digital world is permanent, and with each post, students are building a digital footprint. "(Common Sense Media, 2016, para. 3). Twenty-two percent of the five to eight year old population are online daily for about 17 minutes (Hope, 2015).

The dangers that children using the internet face are electronic identity theft, cyber bullying, predatory contact, unsolicited marketing to minors, cyber-exposure to adult content, and personal information breaches. The irony is that children born in the digital age, often are more adept with online usage than their parents or teachers, but this does not mean that children have the maturity or sophistication to know how to be digital citizens (Berson, 2006).

Funding access has created an inequality for schools who receive more resources and has worked against what the funding laws are trying to create. While digital access is vital to meeting 21st Century skill sets, digital literacy is also paramount. Without proper education, online users are creating an unauthorized biography obtained through aggregated information and cookies. School districts are required to have Acceptable Use Policies (AUP), but this does not provide students with guidelines on how to use to internet, to ensure privacy issues, while they are

online. This study focuses on what students from three classrooms in the fifth grade know about Digital Citizenship as it relates to the Common Core State standards and 21st century skill sets.

Background and Need

President Bill Clinton in his State of the Union address, stated, "In our schools, every classroom in America must be connected to the information superhighway with computers and good software and well trained teachers" (State of the Union, 1996, para. 35). He proposed a two billion dollar technology literacy challenge. The plan was scheduled to unfold within five years, where every classroom in the United States would have internet access. Technology innovation was the motivation to close the digital divide. On February 8, 1996, President Clinton signed the Telecommunications bill, which provided discounted internet rates to schools. On February 15, 1996, President Clinton announced his five- year plan. The mission was to make all young person's technologically literate by the year 2000. Funding was to be determined by the number of students in each State (Department of Education, 1996).

In 2001, President George W. Bush signed the No Child Left Behind (NCLB) Act into law. This measure forced schools to report student performance. Additionally, this measure began introducing the need for classrooms to have computers and education technology. NCLB was not successful in funding all schools with the necessary technology to meet the growing demands of 21st century skill sets. What remained unaddressed in NCLB were the risks that minors would be exposed to as a result of going online. Moreover, NCLB did not provide requirements for a program such as digital citizenship, whereby teachers could use a set of

standards and best practices to educate students about the importance of online privacy and issues of cyberbullying, predatory contact, unsolicited marketing, and cyber-security.

President Barack Obama's education plan in 2008, was to bring public schools into the 21st Century, and ensure that public schools had equal access to broadband and students prepared for participating in the global economy when they graduated from high school. Technology is considered a 21st Century skill. Twenty-first century skills refer to critical thinking, problem solving, communication, collaboration, information and technology literacy, adaptation, innovation, creativity, intercultural competency and financial literacy skills ("P21", 2007). President Obama found our education systems were 20th Century and that we needed to elevate our standards, hire qualified teachers, and prepare students for the growing demands of the 21st century.

In 2009, President Barack Obama re-envisioned public education, and created "Race to the Top" program. Four billion dollars were awarded to 19 states that incorporated the new program. Standards, assessment, better technology, and turning low performing schools around were the focus of this reform agenda. CCSS were released in 2010, and States that complied were given incentives. By 2014, forty-three states including the District of Columbia complied. This funding allowed for longitudinal data systems that could access standardized tests of students and follow teacher track records with students.

The Obama education policy had been about accountability and what schools perform the best on standardized tests. In fact, the Obama administration gave out 100 million dollars in federal grants for teacher preparation programs for those that score the highest on standardized tests (Onosko, 2011). However, funding remains a national issue in public schools, with ongoing

threats supporting the privatization of public schools. What was not addressed in 'Race to the Top' was ensuring that all public schools have equitable access to technology in the classroom. Funding was distributed to schools that aligned with CCSS, which involved schools to have the technology for students to be able to take standardized tests. Chromebooks were used in school districts because they could be shared amongst multiple classes. While billions of dollars have been spent over the past eight years, Race to the Top has not funded all schools to ensure that students are meeting CCSS and are trained in 21st century skills (Onosko, 2011).

Common Core State Standards evolved through the deficiencies of No Child Left Behind. The areas of weakness were reported to be poor assessments and fears about the future viability of the United States as competition from around the world increased. CCSS was developed by governors, state school officials, educators and researchers (Polikoff, 2014). The Center on Education Policy, states that the CCSS was to be fully implemented by 2015. Twenty states in the U.S. observed that having a sufficient number of computers in schools to meet the new CCSS was a challenge. Having internet access, bandwidth, available expertise at state, district and school levels to technological problems was a major concern.

According to the Central Intelligence Agency and Internet Live Stats (2016), in 1995, less than one percent of the population was using the internet. In 2013, 48.4% of internet users were from Asia. North and South America were clumped together, totaling 21.8% ("Internet Live Stats," 2016). In 2016, 40% of the world population is using the internet. This equates to 3,424,971,237 persons who are online today and there are 7,432,663,275 people in the world (Central Intelligence Agency, 2016). These statistics are only projected to grow, which has made the need to incorporate technology in education more urgent. Computers are being mandated for

students to be able to take online testing and meeting CCSS. Classrooms that do have technology in the classroom have begun to incorporate education apps to support student learning as well as cloud based sharing. While classrooms are trying to comply with the new CCSS and 21st century learning, classrooms are expected to have access to external websites such as Khan Academy and Edmodo. According to Education Week, Khan Academy, and Edmodo, who are leading learning management systems for teachers have been under scrutiny for privacy issue violations (Harold, 2014). They have been accused of tracking and using surveillance strategies to track student activity so that they can buy and sell the metadata to marketers.

Education Week reported that a review of each group's privacy policies yielded concerns about the use of tracking and surveillance technologies that allow third parties to gather information on students; questions about the collection, use, and sharing of massive amounts of student 'metadata'; and criticism of the growing burden on students and families, who experts maintain, are being forced to navigate an ever-shifting maze of dense vendor policies on their own (Harold, 2014, para. 4). *Inbloom*, an educational technology company received $100 million dollars in grants to create educational applications that allowed the company to spy on student's activities while they were online (Solve, 2014). They would sell the metadata to vendors and then the vendors would then market to the students. The advantages of such educational technology are that they are able to customize assignments to meet student needs. Having access to the internet allows for students to have access to the best lectures and teachers from around the world to enhance the curriculum in the classroom (Polonetsky &Tene, 2014).

The risks of students who are minors being online necessitate and reinforce their vulnerability to both intentional and unintentional disclosures of sensitive information

(Polonetsky & Tene, 2014). Therefore, there is a fundamental need to provide students with the requisite education, knowledge, and tools. This foundational knowledge will equip youth about the dangers of being online or using social media. The goal is to establish awareness and personal ownership so that they know how to protect their online identities. Data miners, use the information they mine to sell to the government and businesses for the creation of a digital dossier so businesses can find ways to manipulate your online activity (Pointas, 2014). The use of technology in the classroom, presents a threat to many students because of 'cloud' based information sharing (Valcke, Schellens, Van Keer, & Gerarts, 2007). Online activities may be creating a permanent digital footprint that can lead to unintended consequences throughout their lifetimes.

The Children's Online Privacy Protection Act of 1998 was put into effect in April of 2000 to protect the rights of children under the age of 13, from having their information mined by data marketers. This act requires that websites must adhere to a published privacy policy. The main function of this law is to protect the privacy and safety of children online, as regulated by the Federal Trade Commission (FTC), (Federal Trade Commission, 2016). Personal information as defined by the FTC includes a full name, address, email, phone number, social security number, video or photo of a person, geolocation or any combination of information (FTC, 2016). Compliance to this law requires that all businesses must seek and receive parental consent as well as disclose how they are using the personal information of a child under the age of 13.

The Children's Online Privacy Protection Act (COPPA) was passed in 1998 and was put into effect in 2000. COPPA was created by the FTC to ensure parents were involved in what personal information was being used of their children online and to protect personal information

of children under the age of 13. This act requires that online companies are transparent in their online collecting policies. Consent is required from parents if personal information is collected. Parents can deny the online company permission to sell personal information to a third party. Personal information constitutes your full name, address, screen name, phone number, social security number, geolocation, information about a family member or an identifying identity used through other online platforms (FTC, 2016). In 2014, the White House recommended that Congress:

> Modernize the privacy regulatory framework under the Family Educational Rights and Privacy Act and Children's Online Privacy Protection Act to ensure two complementary goals: protecting students against their data being shared or used inappropriately, especially when that data is gathered in an educational context, and ensuring that innovation in educational technology, including new approaches and business models, have ample opportunity to flourish. (Executive Office of the President, 2014, p.64)

The Student Online Personal Information Protection Act (SOPIPA) was revised in 2014, to prohibit student's personal information to be used for commercial purposes. Parents were concerned about the aggregation of children's data, its persistence over time, and its potential monetization by vendors. "Others worried that the data analysis would accrue for those of wealth, and deepen the digital divide for those less fortunate" (Gangadharan & Wooley, 2014, p. 948).

Google has been the leader in selling Chromebooks to schools, due to cost and accessibility of their product. Their cloud applications and sync are under investigation, due to

the failure to impose a data deletion option (Gebhart, 2017). In regard to schools and technology vendors, there is a grey area. Vendors and schools become partners and often schools will rely on vendors for their infrastructure (Leswing, 2015). Vendors under contract with schools, to gain access to student information, even if it is in aggregated forms. This fell under FERPA in 2009, when it was amended to allow school vendors to qualify as school officials. The Protection of Pupil Rights (PPRA) states that schools must disclose the use or sale of student information, except when it is in regard to developing educational products ("Family Policy Compliance", 2016).

On December 1, 2015, the Electronic Frontier Foundation filed a complaint with the FTC that Google had violated the Student Privacy Pledge (SPP). The SPP was created to protect minors online from online companies using their information to market to them. The EFF found that Google's "Sync" feature for the Chrome browser was enabled by default on Chromebooks sold to schools. This allows Google to track, store on its servers and data mine for non-advertising purposes. It records every internet site each student visits, every search term they use, the search result links they click on, videos they look for, watch on YouTube and their saved passwords. Google does not obtain permission from students or their parents, and many parents are unable to prevent Google's data collection (Electronic Frontier Foundation, 2015).

Respectively, Chromebooks are a compelling solution for schools because they are affordable and multiple users can have access. In fact, Chromebooks accounted for 78% of all laptop shipments to U.S. elementary, middle and high schools. The average cost for a Chromebook is $200, which is why 1.63 million Chromebooks were sold last quarter to U.S. schools. Schools are important to computer makers because it's one of the remaining areas where

large institutions are looking to buy new PC's in large quantities (Leswing, 2015). Allegations against Google are that they collect, maintain, and record everything a student uses online.

Google acknowledges that they use Chrome Sync in an aggregated and anonymized form (Crowley, 2015). Chrome for Education is outside the bounds of the SPP. The SPP was put into place so companies would not sell student information, would not engage in behaviorally targeted advertising, support parental access, use security standards and would be transparent about how information is being collected and used. Privacy policies would also not be changed without notification. (Crowley, 2015).

The Student Privacy Pledge was established to protect the privacy of K-12 school children from companies who might use information collected online to market to users. It serves to protect student privacy by not collecting personal information beyond what is needed in school. Companies are not to share or sell student information. They agree not to create dossiers on students or save student information longer than allotted by the school and for companies to have a strong online security system to protect online users. Companies who sign this pledge agree to protect the privacy and identity of children. For a full listing of the SPP refer to Appendix C.

While technology is being actively implemented into classrooms, computer science CCSS are still being developed. These standards are being considered to be implemented on or before July 31, 2019. This means that for three more years, schools will not have standards to follow regarding computer sciences. Additionally, these standards do not address digital literacy and digital citizenship. A full proposal for consideration for computer science content standards can be referenced in Appendix D.

While there are no standardized Common Core Technology standards that schools are implementing, each school district must implement a legal agreement called an Acceptable Use Policy (AUP), which outlines what students, teachers and administrators are allowed to do online. This policy outlines acceptable and unacceptable online behavior. Students and parents sign the policy and each district policy may differ. This does not relate to metadata being gathered by third parties or the storage of personal data.

Digital citizenship is a set of standards online that set the norm of what is appropriate and responsible behavior in reference to the use of technology (Ribble, 2011). The importance of having a set of universal standards of digital citizenship, is that it educates students about what the expectations are online and protects students from risky and unsafe situations. Having digital citizenship as an ongoing training program within a school and classroom will prepare students in meeting 21st century skill sets and meet CCSS proficiencies. Teachers and students must be trained and practice online strategies and skills so that they become aware of what their responsibilities are to themselves and community. Having digital citizenship curriculum would enable students to know how to work online and understand how to protect their identity.

Students will know what information is private, what information could be used for identity theft, what cyberbullying is, how to deal with inappropriate people online, how to use a search engine, what should a person use as a password, how to use a proper citation and what information is safe to share online (Common Sense Media, 2016). Despite all the risks associated with being a digital citizen, the advantages of educational technology in the classroom are that teachers can customize assignments to meet student needs, and the internet allows for students to

have access to the finest lectures from teachers from around the world as well as education apps which enhance the curriculum in the classroom (Sharples, Graber, Harrison, 2009).

The challenges reside with the fact that public schools are not funded equally due to the changing educational agendas with new Presidents and their administrations. Public schools continue trying to secure funding through each administration while trying to meet the growing demands of technology and ensuring that students have the 21st century skills necessary to prepare them for their futures (Guthrie & Springer, 2004).

Statement of the Problem

Since 1993, U.S. Presidents and subsequent administrations have attempted to bring technology into public schools so that classrooms would have the necessary technology to meet 21st Century skills (Guthrie & Springer, 2004). Public schools in the State of California who wanted grant funding from President Obama's 'Race to the Top' program were required to incorporate CCSS into their curriculum, which included a State Longitudinal System (SLDS), which tracks the identity of the students, and their performance.

Public schools who have implemented CCSS into their curriculum are required to use computers for assessment testing as well as meeting standards to continue to receive funding. What is not available are standards and curriculum for teachers to educate the online behavior of the students. Students who are using the internet, without guidance and knowledge of the permanence of a digital footprint are at risk. Part of the challenge is the discrepancy that digital immigrants are teaching digital natives. Students are more technologically savvy, while they lack the wisdom of common sense online (Oxley, 2010).

K-12 public school students in California, and in particular minors may be at risk online from multiple sources due to the ever-increasing requirement and usage of technology in the classroom. Electronic identity theft, cyber bullying, predatory contact, unsolicited marketing to minors, cyber-exposure to adult content, and personal information breaches including visual media are among the major threats that students who are minors face (Valcke et. al, 2007).

According to "Guardchild" (2017), every 79 seconds an online thief steals someone's identity and will use that information to open accounts. Fifty-eight percent of students between grades four through eight reported being subjected to cyberbullying. Ninety percent of children ages eight to sixteen have been exposed to pornography online. Approximately 116,000 requests for child pornography are made online daily. "Guardchild", (2017) states that 20% of children ages 10-17 were sexually solicited online.

In the State of California, CCSS have no specific technology standards woven into the curriculum to include the ethical consideration of digital citizenship. Digital citizenship would be a foundational tool to establish ethical norms online as it is unclear is how the length and permanence of one's digital footprint will affect a person's future. The problem is that minors are being required to be online in school without being fully educated about digital citizenship. This study examined what 10 to 11 year olds specifically know about digital citizenship to address what seems to be a potential gap in the research scholarship.

Statement of Purpose

This study aims to inquire into and document the knowledge, scope, and skills demonstrated by a sample group of fifth grade students regarding digital citizenship. The primary

purpose of the study is to ascertain if this sample group of fifth grade students may be at risk due to their use of the internet, particularly due to the specific technology requirements of the CCSS which are woven throughout language arts and math curricula. Selected examples of some CCSS for fifth graders that require the use of technology are referenced below:

> Reading Standards for Literature 5th Grade
>
> 5.7 Analyze how visual and multimedia elements contribute to the meaning, tone, or beauty of a text (e.g., graphic novel, multimedia presentation of fiction, folktale, myth, poem).
>
> Reading Standards for Informational Text 5th Grade
>
> 5.7 Draw on information from multiple print or digital sources, demonstrating the ability to locate an answer to a question quickly or to solve a problem efficiently.
>
> Writing Standards 5th Grade
>
> 5.6 With some guidance and support from adults, use technology, including the Internet, to produce and publish writing as well as to interact and collaborate with others; demonstrate sufficient command of keyboarding skills to type a minimum of two pages in a single sitting.
>
> Language Standards 5th Grade
>
> 5.4 c. Consult reference materials (e.g., dictionaries, glossaries, thesauruses), both print and digital, to find the pronunciation and determine or clarify the precise meaning of keywords and phrases and to identify alternate word choices in all content areas.
>
> (CCSS, 2016)

The school district in which this research was conducted is CCSS compliant, the select

standards highlighted above, address how fifth grade students are required to use technology within the classroom to meet these standards. This study attempted to ascertain if students who are being required to use technology within the classroom were at risk, due to a potentially incomplete education regarding digital citizenship.

Research Question

This study is focused on the following research question. What knowledge, scope, and quality of digital citizenship skills do a sample of fifth graders from three classrooms in one Northern California public school demonstrate?

Theoretical Rationale

The theorist, Howard Gardner who is most noteworthy for his Theory of Multiple Intelligences, also founded the *Good Play Project* and through this, identified five ethical fault lines for children while online. The five ethical fault lines he identified are namely: identity, credibility, privacy, ownership, and participation. Gardner and the Good Play Project found that cultivating digital ethics allows for best practices to be achieved while promoting digital literacy and that the risks and opportunities for youth online become a collective responsibility. Having best practices allows for youth who are immature, in need of social validations, and at risk of fragmentation of identities to apply a framework in order to develop rational thinking while still cultivating productive, innovative and ethical practices (Erikson, 1968).

Dr. Howard Gardner and the Good Play Project out of Harvard University collaborated with Common Sense Media to use Howard Gardner's theory of digital ethics to create a literacy curriculum on digital citizenship, based on digital image, digital footprint, digital literacy, digital privacy, digital relationships and privacy, cyberbullying, internet safety, copyright and creative copy. Common Sense Media looks at digital citizenship curriculum based on privacy and security, which focuses on keeping information safe.

The second component is one's digital footprint and reputation, which addresses the permanence of online activity and how self-reflection can help students gain perspective on what they are posting online. The third is self- image and identity, which address virtual lives compared to their actual lives. It addresses the complications of presenting varying personas and how that can affect someone's sense of self- worth. The fourth is relationships and communications and this relates to how a person can use "interpersonal and intrapersonal skills to build and strengthen positive online communication and communities" (Common Sense Media, 2016, p. 2).

The fifth addresses cyberbullying and drama and students address both positive and negative situations and learn what it means to build supportive community online. The sixth is credit and copyright, which addresses user's responsibilities to the creators or intellectual property. The seventh is information literacy, which addresses how a person finds information online and are able to evaluate reputable sources. The eighth is internet safety, which involves the joy of connecting with others online, which knowing how to protect yourself and your identity online. Online users learn what inappropriate contacts might look like, vs reputable.

Dr. Mike Ribble is a leader in digital citizenship who has written two books, *Raising Digital Children* and *Digital Citizenship in Schools* and is an active member of the International Society for Technology in Education (ISTE). He has created the Nine Elements of Digital Citizenship (Ribble, 2011). The first element is one of digital access and ensuring that all persons have equal access to participate electronically to ensure that there will not be a digital divide due to privilege. The second is digital commerce, which includes illegal downloading or making purchases that are in conflict with the laws or regulations of other countries.

The third is digital communication, and this refers to how one addresses communicating appropriately online. The fourth is digital literacy, which has to do with being a perpetual learner and continually learning new technology. The fifth is digital law, which involves hacking, stealing others work online, downloading illegal music, creating viruses or sending spam (Ribble, 2011). The sixth is digital etiquette, which is how a person engages in appropriate online behavior. The seventh is in regard to digital rights and responsibilities, which include privacy and freedom of speech. The eighth is digital health and wellness, which address the psychological and physical ramifications of being online. Being aware of repetitive online motions, sounds, ergonomics etc.

Psychologically, people can become addicted to being online. Digital citizenship addresses ways to protect one's self online. The ninth principle is one of digital security, which is about online protection and safety. The emphasis is that we protect ourselves online with virus protection and protect ourselves from other people or places having access to our private information. Ribble's Nine Elements of Digital Citizenship can also be categorized under the labels of *Respect*, *Educate*, and *Protect*. Respect would incorporate digital access, etiquette, and

digital law. Educate would incorporate digital communication, literacy, and commerce. Protect would cover digital rights and responsibilities, digital safety and security, and health and wellness.

Respect:

- Digital access**:** Advocating for equal digital rights and access is where digital citizenship starts.
- Digital etiquette: Rules and policies aren't enough — we need to teach everyone about appropriate conduct online.
- Digital law: It's critical that users understand it's a crime to steal or damage another's digital work, identity or property.

Educate:

- Digital communication: With so many communication options available, users need to learn how to make appropriate decisions.
- Digital literacy: We need to teach students how to learn in a digital society.
- Digital commerce: As users make more purchases online, they must understand how to be effective consumers in a digital economy.

Protect:

- Digital rights and responsibilities: We must inform people of their basic digital rights to privacy, freedom of speech, etc.
- Digital safety and security: Digital citizens need to know how to protect their information from outside forces that might cause harm.

- Digital health and wellness: From physical issues, such as repetitive stress syndrome, to psychological issues, such as internet addiction, users should understand the health risks of technology. (Ribble, 2011, p.18)

Ribble (2011), also proposed that these nine principles of digital citizenship can be organized into three tiers for students in kindergarten through eighth grade. He believed that digital citizenship should begin as early as kindergarten or when a child starts becoming involved with technology. In kindergarten through second grade, the focus is on how to respect yourself online and others online as well as being introduced to what digital etiquette, digital literacy and educating yourself and others. The second category is for third through fifth graders and the focus is on respect for self and other, digital access, educate and connect with others, digital communications, protecting self and others online and digital safety. The third tier is for sixth to eighth graders which focuses on respecting yourself and others online, digital law, educating yourself and others, digital commerce, protecting self and others online and digital health and welfare (Ribble, 2011).

Assumptions

This study assumed that minors are using technology as an educational requirement in the classroom as the CCSS mandates. The study assumed that this sample of fifth grade students from one school in Northern California reflected the average demographics and characteristics of a California State fifth grade public school classroom. Lastly, this study assumed that digital citizenship was not being taught in the classroom.

Summary

Since the advent of Apple's computer in 1984, and access to the World Wide Web in 1993, a technological renaissance has emerged. While information, communication, and commerce have flourished, there have subsequently emerged pitfalls and perilous dangers to online usage. There is a reshaping of what citizenship means and the necessity to address global citizenship and digital ethics. It has forced political administrations to look at education in new ways, and ask how we as a nation are preparing our youth to meet 21st century skill sets and ensuring that the upcoming generation will be prepared for the future job market. Additionally, political administrations continue to look at how schools are funded to ensure that schools have equitable access to technology. President Bill Clinton, President George W. Bush and President Barack Obama have all allocated funding to ensure that classrooms are 21st century compliant by having computer access, but none have been wholly successful in fulfilling this mission. Most recently, CCSS was created under Barack Obama's administration, which focused on accountability through online standardized testing. A computer is required for students to be compliant with CCSS and to take the standardized tests. Educators have been using computers without specific technology state standards or via a curriculum of digital citizenship. Students are at risk for electronic identity theft, cyber-bullying, predatory contact, unsolicited marketing to minors, cyber-exposure to adult content, and personal information breaches including visual media. Businesses continue find savvy ways to use aggregated and longitudinal data of online users to market or build dossiers of online users. Schools struggle to manage their infrastructure while incorporating new educational technologies in the classroom. These concerns continue to warrant and justify new online policies and regulations.

Chapter 2: Review of the Literature

Introduction

This chapter examines the scholarship and research literature on digital citizenship and its impact on education. Information was gathered from academic library searches using online resources. Research information is organized in the following categories: Historical Context, Review of the Academic Research, Statistical Information, and Internet Sources.

Historical Context

Citizenship, is derived from the Latin word city. Citizenship, used to pertain to what city a person was from, not a country. Citizenship is comprised of three main elements or dimensions (Cohen, Kymlicka, Norman & Carens, 2000). The first component refers to legal status, referring to political, civil and social rights. The second refers to citizens and their participation in political parties, and the third refers to citizenship as how citizens become involved in a political party. The "psychological" dimension of citizenship (Cohen et al, 2000, p. 166), refers to the subjective sense of belonging. When enough people have an interest or sense of belonging, communities are strengthened.

Global citizenship in turn refers to a person who identifies with being a part of an "emerging world community and whose actions contribute to building this community's values and practices" (Cohen et al, 2000, p.166). Global citizenship also refers to the globalization of the world and what our collective responsibilities are. Since World War II, global policies have supported this notion of global citizenship, through treatise, legal statutes, international

agreements and technical standards. (Israel, 2012). In the 1940's, scholar Nobert Weiner (1954), coined the term Cybernetics, which is now referred to as information ethics. He was responsible for building computers during the Second World War. In one of his studies he examined the metaphysical components of technology through the lens of knowledge, freedom, security, opportunities, health and happiness. He believed that all societies should hold principals of justice. Human beings are intelligent, creative and have the ability to adapt (Weiner, 1954, pp. 57-58).

The purpose of life was for humans to expand upon this quality of being informational beings. Weiner believed that the universe, world and all inhabitants are a combination of matter-energy combination. In order for humans to flourish they need to be free to engage in creative, flexible action. His great principles are, the Principle of Freedom, the Principle of Equality, the Principle of Benevolence. Humans need to be able to actualize their human potential, equality and good will. His methodology was not intended to create a new branch of ethics. He made it clear that computers and technology would remake society. He states," it would affect every walk of life, and would be a multi-faceted, on -going process requiring decades of effort. Informational technology has placed human beings in the presence of another social potentiality of unheard-of importance for good and for evil" (Weiner, 1948, p.27).

In 1976, Walter Maner developed "computer ethics." In 1985, Deborah Johnson (1985) published a book called Computer Ethics. She states that computers "pose new versions of standard moral problems and dilemmas, exacerbating the old problems, and forcing us to apply ordinary moral norms in unchartered norms." (Johnson, 1985 p. 1). Global laws, global cyber-business and global education are new ethical dilemmas that affect how over 200 countries are

engaged online and what each country's rights and responsibilities are. In 1999, Luciano Floridi wrote the, "Flourishing Ethics" theory. His theory combined Aristotle and Wiener. Information ethics treats everything as "informational" objects or processes. He coined information ethics theory (FIE). FIE holds that everything in the info-sphere should be ethically respected (Floridi, 1999).

Michael Fredrick Hauben (1997), internet theorist and author, founded a term called Netizen, stemming from citizens of the net. In the 1990's Hauben coined the term Netizens which was referring to cyber citizens and our responsibilities we now have to a community online. He believed that we are now citizens of the world due to global connectivity. His philosophy is that we are world citizens because of the internet and netizens is a term implying universal social membership. Global connectivity is an e-democracy. Ultimately, he saw the collaborative nature of the internet, extensions of a global citizenship that has emerged from the world wide web. It was his belief that we could build a more democratic, human society and solve socio-political problems while improving the state of the world through, netizenship (Hauben, 1997). He coined Netizen in regard to computers, society, democracy, democratization and decision making.

Karen Mossberger, Caroline Tolbert and Ramona McNeal (2007) coined the term digital citizenship in reference to the state of having access to the internet that provides equal opportunities for online participation, a digital democracy, human rights, and technology skill. Digital citizenship referring to access and those that have access can use the internet for information, communication, politics, and economics. Their belief is that digital citizenship benefits the lives of others, opposed to people who do not have access. This limits a person's

ability to make sound decisions due to limited access to information and knowledge. They found that those who do not have access to the internet have limited economic opportunity and this creates financial inequalities. A digital divide also creates issues with civic responsibilities, such as the political process. In the internet age, their recommendation is for governments to empower citizens with digital access because it enhances communities. Social inclusion is a noble pursuit because it promotes the welfare for a society to prevail, (Mossberger, Tolbert and McNeil, 2007).

The International Society for Technology in Education (ISTE) can be attributed with creating the term digital citizenship as it was coined when they update their 2016 technology standards in education. ISTE identified that standards needed to be created to protect students while they are online. They define digital citizen as the following:

> Students recognize the rights responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal ethical. Students: Cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world. Engage in positive, safe, legal and ethical behavior when using technology, including social interactions online or when using networked devices. Demonstrate an understanding of and respect the rights and obligations of using and sharing intellectual property. Manage their personal data to maintain digital privacy and security and are aware of data-collection technology use to track their navigation online (ISTE Standards, 2016).

Review of the Academic Research

The internet has revolutionized the world we live in, but has also brought with it very serious social issues. The internet connects the world and makes everything accessible and available at our fingertips (Oxley, 2010). The danger is that it has created issues with identity, privacy, child safety, bullying and illegal behaviors. Digital citizenship is needed as a guide to help children and adults manage and navigate the internet in an agreeable set of rules. If children are exposed and practice digital citizenship it will prepare children to respond effectively when confronted with inappropriate opportunities. Oxley's, (2010) research found that most students did not care about their online presence or would simply forget to protect their online identity. She reinforced the necessity to protect youth when online. According to the National Center for Missing and Exploited Children, one in five children is solicited for sex and one in 17 children are threatened on the internet. It is estimated that 4,000,000 children are on the internet daily (Wolak, Mitchell, Finkelhor, 2006).

Children need to have an environment where they can practice online situations about security and privacy, without harmful ramifications, (Berson, 2006). Developmentally, children do not understand risk until mid-childhood. Parental involvement is important because computer technology is streamlined and online activities are more unforgiving. Children would benefit from virtual online experiences where they could see the effects of their online behavior, without actually having to experience them.

Marc Prensky's theory of Digital Natives and Immigrants (2001) examined the changes in education, regarding the use of technology. He addressed how students from Grades K-college are the first generations to grow up with computer technology. They have spent their entire lives

surrounded by digital music players, video cams, cell phones, and all other toys and tools of the digital age. “Today’s average college graduates spend less than 5,000 hours of their lives reading, but over 10,000 hours playing video games (not to mention 20,000 hours watching TV). Computer games, email, the Internet, cell phones, instant messaging are integral parts of their lives”, (Pensky, 2001, p. 45). His theory is that due to the amount of time used on the internet, the way students learn is also changing. The thinking patterns of students now are different from those of previous generations. Digital immigrants refer to people who have not grown up with technology. Like immigrants to a country, some people may struggle to become adept at new ways of learning and will retain their “digital immigrant accent”. He suggests that the biggest problem facing education today are outdated teachers trying to teach a new generation of digital natives who speak another language. The goal being to teach legacy and future content to meet the growing needs of students (Pensky, 2001).

Dr. Howard Gardner, a developmental psychologist and professor at Harvard is most noted for his theory of multiple intelligences, which was a paradigm shift on how intelligence was defined and understood in the past. He challenged Piaget’s cognitive development theory and demonstrated that a child can be in varying developmental stages. He provided evidence that developmental stages were not static. Gardner found the people have eight varying intelligences, namely: linguistic, logical-mathematical, musical, body-kinesthetic, spatial, interpersonal, intrapersonal, and naturalist intelligence, (Gardner, 1983). Gardner viewed intelligence “as the capacity to solve problems or to fashion products that are valued in one or more cultural setting” (Gardner & Hatch, 1989, p. 7).

These intelligences rarely operate solely on their own. In the field of education, this has enabled educators to examine how to teach children with variety of learning styles. Gardner looks to see "how morality and intelligence can work together", (Gardner, 1999, p. 4). He also feels that knowledge is not the same as morality. In relationship to education, digital literacy, and children, this theory presents the idea that if a person understands who they are, and how they learn, they will have a greater understanding of what they are capable of. "The performance of understanding that matters are the ones we carry out as human beings in an imperfect world which we can affect for good or ill" (Gardner, 1999, pp.180-181).This theme of morality and consciousness has carried on with the Good Play Project, Ground Zero and the Common Sense Media. His focus is on digital ethics and what it means for youth to engage online. This addresses how youth can benefit from digital media, but learn how to protect themselves so that they can engage as ethical and responsible citizens.

Gardner (2014), focused on an ethical fault line with youth and that the five components that put youth at risk are identity, privacy, ownership, authorship, credibility and participation. The theory behind his digital citizenship curriculum in collaboration with Common Sense Media is used to establish and cultivate best practices for children online, to generate awareness, develop a global citizenship mentality with ethical and moral consideration, while maximizing the intellectual capacities that the internet provides and is capable of reaching the eight multiple intelligences.

In 2000, Marc Prensky coined the term "digital natives", referring to the first generation of people who have spent their lives using the internet. Persons who have not grown up with access to technology are called digital immigrants (Pensky, 2001). Children have an ease with

the use of technology, but they do not have the maturity and are not savvy when to comes to communicating and online ethics, (Young, 2014).

Children need to be taught and guided about socially appropriate and inappropriate behaviors. Most children are naïve about the consequences of sharing too much private information or the tone of the emails that they may project. One way teachers and parents can protect children when they are online is to be aware of privacy settings and that public domain documents are open to third party use (Berson, 2006). In schools, teachers have legal authority to monitor children's online usage. Developmentally, children do not understand risk until mid-childhood, which is why it is important to guide and monitor children online. Digital natives have become desensitized to loss of privacy and adults are not prepared to know how to meet the growing digital demands of children growing up today. This is also called the online disinhibition effect, which means that when people are online they might be more inclined to self- disclose (Syler, 2004).

Digital citizenship is a global movement intended to provide online users with protocols concerning appropriate and inappropriate online behavior. Digital footprints start the moment a person begins using the internet and social media sites. For many children being born, the imprint begins prior to their birth, when parents post information about their birth on social media sites. Children born into the digital age will have extensive digital footprints. Teaching children how to manage their online identity, is protecting their online reputation (Orth and Chen 2013).

Children are becoming increasingly more vulnerable to the loss of privacy and falling prey to online predators. These predators may not be a living person, but how cookies, data mining and

track users are manipulating and evaluating your private information. (Berson, 2006). The Children's Online Privacy Protection Act of 1998 (COPPA) and the Elementary and Secondary Education Act of 2001 prohibit companies form using information about minors who are under the age of 13. At the age of 13 a teenager is deemed mature enough to make critical choices online. These acts were established in regard to the 14th amendment of equal protection under the law, the first amendment of freedom of expression, the 4th amendment which protects search and seizures and the 5th amendment. Cyberspace preys on weakness (Berson, 2006). It capitalizes on those who do not understand how companies mine for information through surveys, online forms, quizzes and registration forms.

Teaching digital citizenship is creating good citizens who exercise sound judgement. Children know a lot about technology, but do not have the maturity to navigate safely (Kivunja, 2014). Parental involvement is important and the consistency of online and offline behavior should be consistent. Parents are looking for guidance on how to create policies for their children in the home. There is a sense of disempowerment amongst parents, because their children know more about technology than they do. In a 21st century school model, schools will guide students and the models used in schools will be communicated with parents (Palfrey, Gasser, 2008). The National Cyber Security Alliance advises parents to stay positively engaged in their children's lives online and to use your time together online as a learning experience with teachable moments. Having a positive attitude is effective ("National Cyber Security Alliance", 2017).

School districts require and an AUP, before staff or students are granted access to the internet or server. This policy outlines acceptable and unacceptable behavior while online. This agreement addresses how the student may use the computer and what they are or not allowed to

view. Often students will be required to take a computer responsibility online assessment or class prior to being able to use the internet (Common Sense Media, 2016) The AUP will also clearly define what is deemed as unacceptable behavior. This agreement is usually signed by the parent and student. AUP's are not considered sufficient, because technology is constantly changing and students are not always knowledgeable about what is appropriate and inappropriate behavior online. Digital Citizenship requires strategies that are discussed and used daily for reinforcement (Ribble, 2011).

Tony Wagner (2003), author, speaker and expert in residence at Harvard University is known for his Theory of Change. He combats the theory that if schools raise the stakes with standardized testing, performances will improve with students. His hypothesis is that this is a fatally flawed mentality, because it does not take into account what a model school looks like and there is no general consensus as to what exceptional teaching is. Schools required to take online standardized testing are not taking into account where the school ranked in mastering academic competencies. Policy makers are setting up public schools for failure, due to their lack of understanding of public schools. Students are dropping out of high school because they are unable to pass the standardized test. His understanding is that this is creating a widening gap amongst students and their education of the have and have nots (Wagner, 2003).

Common Core State Standards require public schools to take online standardized testing, which require technology within the classroom. Most schools are getting tablets in elementary schools because various classes can share the tablets, but the infrastructure surrounding how students and teachers are supported and using technology is not equal. Wagner (2003), has looked at models of how Denmark has addressed public education and in turn developed these

seven survival skills for the 21st century, which are in alignment with CCSS and the vision of 21st century skill sets. His hypothesis is that we need students to develop the following skills of critical thinking, problem solving, collaboration across networks and leading by influence, agility and adaptability, initiative and entrepreneurship, effective oral and written communication, and finally, assessing and analyzing information.

Jason Ohler (2010), professor emeritus, speaker, writer, teacher, researcher and digital humanist, wrote Digital Community: Digital Citizen. He addresses how citizenship continually needs to evolve. He believes that citizenship is a virtuous behavior, but requires education. People need to be taught and need to practice. "We need a whole-school approach to behavior that sets the entirety of being digitally active within an overall ethical and behavior context-character education for the digital age." (Ohler, 2010, p.145.)

Karen Mossberger (2008), associate professor and author holds the belief that the internet can be used for demographic participation and economic welfare. That humans have a need and capacity for belonging and the internet gives the potential for political and economic engagement in society in an information age. Both address how preparing students to cultivate these skill sets are important components to creating future leaders who will be prepared for the responsibilities that lie ahead of them.

Teachers need to learn how to have exemplarily online behavior (Hassel, Hassel, 2011). Technology has become interwoven into the classroom and children while often more technologically savvy, lack the common sense or have the maturity to distinguish what is appropriate or inappropriate behavior (Sook-Jung &Young-Gil, 2007). Harte (2011) addresses the gaps teachers have with digital citizenship, and that they too fall victim of the permanence of

a digital footprint. Teachers have been fired for careless behavior online or making poor online choices through emails or social media sites.

Harte (2011) looks at E-professionalism and ethics around electronic communication with teachers. Every time we are online we are creating a digital footprint, so teachers need to take this into account with emails that are free of errors and are sent to the intended recipient (Richardson, 2008). When these areas are compromised they undermine their professionalism. Teachers should take advantage of using technology in the classroom to enhance lessons and meet varying learning styles. When engaging in social networking, be mindful of your professional image (Richardson, 2008). Use necessary privacy settings and to limit access to persons outside their peer group to ensure that outsiders do not misinterpret your content.

According to Harte (2011) rules of trust and respect apply online. The National Association for the Education of Young Children (NAEYC) Code of Ethical Conduct is recommended resource for teachers online. Teachers have a harder time gauging the risks of online behavior. Teachers need to be both diligent and dedicated to demonstrating what professionalism means in the classroom and online (Fodeman, Monroe, 2012). The premise of NAEYC is to be responsible to children by doing no harm, to be responsible to families, co-workers, employers and community. The recommended practices are to have online users pause prior to posting. Reflect on what you are posting. Use privacy settings, be proactive about student expectations and then engage professionally online. Maintaining healthy boundaries is important online, with parents and students.

The K-12 professional community must also develop procedures for children using technology within the classroom. “These opportunities will consist of effective digital citizenship

curriculum, peer mentor programs, effective role models, educational faculty/staff awareness, enhanced awareness of risks, and most importantly a proactive vs reactive approach." (Hollandsworth, Dowdy and Donovan, 2011, p. 39). A teachable moment allows for a more organic process with children within the classroom.

Digital citizenship can be compared to citizenship in that all citizens have the basic rights: privacy, free speech, and creative work rights (Hollandsworth et al., (2011). The village concept of raising children in the digital age comes into play because the community is responsible for ensuring that the students know what is considered legal and illegal behavior online. Additionally, that when there are rights, responsibilities follow with it. Engaging in legal, ethical behavior starts with the community, with teachers, parents, guardians and then must be modeled and taught to children (Gardner, Davis, 2013).

The challenge remains that adults who were not brought up in the digital age have a more challenging time keeping up with the latest technologies. Technology is not going away, and educating students to thrive within a digital society is the responsibility of adults advocating for children's rights and responsibilities. From the perspective of the Good Play Project, more scaffolding is required to create digital citizens.

The Presidents of State Library Media and Educational Technology Association participated in a ten question digital citizenship survey. There were over 500 participants that responded to this survey. Over eight percent of the teachers from this participant sample indicated that they were very aware of digital citizenship and how to teach students about these issues, (Hollandsworth, et al., (2011). There was a direct correlation between what was addressed in state standards and the percentage of teachers who taught that skill. This survey also found

that information about plagiarism was taught by teachers, and 44% agreed that these skills were addressed in state standards. Ergonomics had a 33% rate of being taught and 14% of the sample that agreed that these skills were addressed in state standards.

Missouri, Virginia, Kentucky, Arkansas, Georgia, Tennessee, New Hampshire and Kentucky were the States that were found to be at the forefront of Digital Citizenship education (Hollandsworth, et al., (2011). Kentucky has implemented Dr. Mike Ribble's nine elements of digital citizenship, also outlined through the International Society for Technology (ISTE). They address digital etiquette, digital communications, digital literacy, digital access, digital commerce, digital law, digital rights and responsibilities, digital health and wellness and digital security. Within their educational policies they outline how to engage with electronic email, confidentiality, internet activity and use of technology. This is different than an AUP, in that it serves as an educational tool for teachers and students. The remaining states have not adopted Information Literacy Standards and Common Core curriculum does not address digital citizenship. Standardized test scores outweigh the implementation of digital citizenship curriculum, even though technology is required in the classroom through CCSS, (Hollandsworth et. al., 2011)

According to Ribble (2016), reflecting on what it means to be a good ethical person is the first step in developing awareness. Students need role models within their lives to demonstrate what it means to have good online and offline behavior. Digital citizenship should be integrated within the classroom and curriculum and not taught on one occasion within the classroom. Ribble found the challenge of teaching digital citizenship is changing their attitudes and this is the most effective when it relates to students on a personal level. When children are 12 years old,

their behavioral patterns online are set (Ribble, 2016). Ribble recommends starting in K-1st grade and building on topics each consecutive year.

A school media specialist who would work with each grade would be an ideal solution for schools looking to integrate digital citizenship within their school and classroom. This lead person at the school would either establish digital citizenship practices or implement established ones. They would educate administrators, teachers, students, parents, library specialists, technology coordinators and community members (Hollandsworth, et al., 2011). They would remain engaged and evaluate the program regularly, receive feedback, be proactive, and allow for a collaborative approach.

Information and communications (ICT) is vital to human and sustainable development. There are 7 billion people on earth and 6 billion have access to a mobile phone, while only 4.5 billion have access to a toilet (Tan & Park, 2014). The Asia-Pacific (AP) region has had significant issues related to digital citizenship. In a survey through Microsoft amongst 25 countries in 2012, China, Singapore and India has the highest rates of cyberbullying ("Microsoft's Global Youth Online Behavioral Survey," 2012). Countries throughout the world are looking into best practices to address these growing concerns. UNESCO Bangkok is taking the initiative of "Fostering Digital Citizenship through Safe and Responsible Use of ICT". This is being addressed through policy, research, advocacy, education and support. The ICT region has an estimated population of 4.07 billion, 57% of the world population.

Australia's Cybersmart program, Singapore's Cyber-Wellness Program, Malaysia's Cyber Safe Program, and Click Wisely campaign, the Republic of Korea have content regulations and educate children, teachers, and students about digital citizenship

("UNESCOBKK", 2014). Most of these programs focus on safety and protection, but the greater vision is how to empower online users so that they can participate fully as technological citizens. Australia's program incorporates interactive games, lesson plans, outreach, parent forums and the collaboration with Peer Support Australia. They also cross reference with other government programs. The Australian Government allotted 10 million dollars in the 2014-2015 budget ("Australian Government", 2014) to fund online safety programs.

On the flip side, China has tight restrictive and censorship laws. Online gaming is an issue in China amongst children. China was the first to declare that internet addiction was a clinical disorder. In India, the National Cyber Safety and Security standards were established through the National Cyber Defense Research Center as has the Cyber Safe India Alliance. Indonesia, has the highest Muslim population, and has the largest censorship of online material. The government supports the "Digital Citizenship and Safety of Children and Adolescents in Indonesia" study. New Zealand strongly backs netsafe.org. In Europe, they have a network of 31 national awareness centers that use Insafe ("UNESCOBKK", 2014).

The European Commission's Better Internet for Kids Program is one of the most comprehensive and extensive in the field of digital media literacy (Tan & Park, 2014) UNICEF's Voices of Youth Citizens Program looks at digital literacy, behavior, and habits on children online. What persists amongst countries not engaged in digital literacy is that the digital divide continues to grow within countries, parental involvement is limited, and educators do not have the skill sets to meet these growing demands.

According to a study by Microsoft in 25 countries among 7,600 children ages 8-17 found that despite children wanting to talk with parents about risks, only 29% of kids say their

> parents have talked to them about protecting themselves online… only 17 percent having communicated a clear set of rules for negative behaviors online, and only 5% of parents engaged with their children's school about online bullying." ("Microsoft's Global Youth Online Behavioral Survey, 2012, p.1)

Internationally, tablets are being introduced to children under the age of nine, which posed physical health injuries due repetitive strain injuries, musculoskeletal, obesity, visual strain and computer radiation exposure. Another issue addressed is that children are being exposed to harmful contents like gratuitous violence and sexual content online. Lastly, commercial content, that contain gender and cultural stereotypes could possibly have an undesirable impact on children's emotional, intellectual, social and behavioral development. "This is attributed to their underdeveloped ability to discern, self -regulate, and ability for impulse control", (UNESCBBK, 2014, p. 64).

Children are at risk due to privacy and personal information being disclosed. Children up to the age of 5 poses the greatest risks online because that is the most vulnerable developmental time. Children using the internet during those ages pose risk of having social challenges. Globally, counties are addressing the growing pains of technology and how to create standards and policies to protect the rights and needs of citizens. Principles that can be agreed upon by the United Nations Convention on the Rights of Children, but vary with each country's defining government structure and priorities in making global access and citizenship accessible.

Statistical Information

statistics on identity theft and marketing opportunities for businesses.

- 10.2% of children have had their Social Security number used by someone else, compared to .2% for adults. (Power, 2011).
- Children under 12 influence $500 billion dollars in purchases a year. (Campbell & Davis-Packard, 2000).

statistics on internet safety and cyberbullying.

- One in 17 children are solicited for sex online. (Missing Children Statistics, 2016).
- Approximately 116,000 child pornography requests are made daily on the internet. (Guardchild Social Media Statistics, 2017).
- 90% of children ages 8-16 have seen online pornography. (Guardchild Social Media Statistics, 2017).
- 65% of 8-14 year olds have been involved in a cyber bully incident. (Guardchild Social Media Statistics, 2017).

Summary

Technology is remaking society, be it for good or evil. Presently, 200 countries are engaged online, which poses the need to define what people's rights and responsibilities are ("UNESCBBK", 2014). Having access to technology is an underlying issue to what is considered a digital divide. Additionally, countries who do not implement digital citizenship see a greater digital divide ("UNESCBBK", 2014). Children who were born into the digital age are digital natives and tend to have greater knowledge about technology than their parents and teachers, (Pensky, 2001). Children are leading the way for many adults who are digital

immigrants. Research suggests that parents and teachers are not taking the initiative to have those discussions with children. Children may be more comfortable online, but they lack the maturity to discern between what is appropriate and inappropriate online behavior. Children do not understand the gravity of a permanent, digital footprint. Children are falling victim to cyberbullying, predatory contact, sexual content, unsolicited marketing, identity theft, and the storage of their personal data online. Countries that have implemented digital citizenship and seen less online dangers, many have incorporated Dr. Mike Ribble's digital citizenship curriculum. In the United States ISTE standards for technology have been created, but are not mandated. Teachers can play an influential role with children online in the classroom, by modeling exemplary online behavior. Their online behavior is professional and they take the time for teaching moments when using technology within the classroom. Technology companies that have educational apps and i-cloud, have access to be a part of the school network and have access to student information. Chrome sync application saves students aggregated information and cookies are often embedded in websites. AUP's are not sufficient protection for students while they are online.

Chapter 3: Method

Research Approach

This study utilized a quantitative action research methodology with a single end of unit survey that allowed for the researcher to tabulate simple statistical data in order to analyze the trends and draw inferences (Creswell, 2014). The population studied was three fifth grade classrooms, consisting of a sample of 88 participants from one public elementary school in Northern California. Researcher did not use stratification. The end of unit survey instrument used for quantitative data collection is in the public domain, and was developed by Dr. Howard Gardner and the Good Play Project at the Harvard Graduate School of Education in collaboration with Common Sense Media, who created the online digital citizenship for assessment for fifth graders (Common Sense Media, 2016). This instrument assessment involved 13 multiple choice items and two short answer questions that questioned participants about their knowledge, scope and quality of digital citizenship skills. The end of unit assessment instrument included digital citizenship topics of privacy and security, digital footprints and reputation, self- image and identity, relationships and communications, cyberbullying, credit and copyright, information literacy, and internet safety. The 13 multiple choice items and the two short answered questions were analyzed based on the supplied correct answers and responses provided by the Good Play Project and Common Sense Media on components of digital citizenship.

Ethical Standards

This study adheres to the ethical standards for protection of human subjects of the American Psychological Association (2010). Additionally, a research proposal was submitted and reviewed by the Dominican University of California Institutional Review Board for the Protection of Human Subjects (IRBPHS), approved and assigned number 10404. Participant names were not recorded or included and the name of the school was not used on any documents to preserve complete confidentiality. Students were not identified individually, and the quantitative data collected was only used in aggregated form for the entire sample of participants. All participants were advised of their rights and of their prerogative to not participate in the end of unit survey at any time. Participants were assured of the confidential nature of this study and informed that all information obtained would be destroyed within one year of the completion of this study. To maintain confidentiality, the researcher was be the only person who had access to the data and all information, documents pertaining to this study was stored in a locked file cabinet in the researcher's home office. Digital data were stored on the researcher's personal computer, secured by a password. Prior to data collection, permission was solicited and received from the Principal at the school site, and then from the respective teachers responsible for the three classrooms of the participants. A sample copy of the consent letter for obtaining permission is included in Appendix A.

Sample and Site

The participants for this study were 88 students from three fifth grade general education classrooms in one public school, in Northern California. This site was selected based on its size

as well as being a school that has implemented the California State Common Core Standards. The researcher approached three public school districts and selected one school in one district based on their interest in technology and digital citizenship. Researcher received written consent to provide an end of unit assessment to their three, fifth grade classes. Participants were not random and were all from the same school. Each of the fifth grade classes within the school consisted of 30 students, and a possible 90 students served as the sample for this study.

Access and Permissions

Researcher obtained written permission from the school Principal prior to conducting the study. Additionally, the teachers of record for each classroom received a written explanation of the study, which was followed up with a face to face meeting to discuss the logistics of how the assessment would be would be conducted with the voluntary participants within the classroom. A sample copy of the consent/permission letter is included in Appendix A.

Data Gathering Procedures

The end of unit assessment was administered to three fifth grade classrooms, totaling 88 voluntary participants. The assessment was provided in hard copy. After the researcher introduced herself, described what the focus of the study was to participants and reiterated that it was a confidential study and that students were not to put their names on their assessments to protect their identities. All participants voluntarily agreed to complete the end of unit assessment. The researcher went into each classroom at 10 a.m., 15 minutes prior to recess to administer the end of unit assessment and collect the responses on three separate days. The respective

classroom teachers remained in the classroom for the duration. Participants were advised that this was a multiple-choice unit assessment. Researcher advised participants to read the questions carefully and to fill out the assessment to the best of their ability. There were 15 questions in total, and that the multiple questions that had more than one correct answer. There were two short answer responses and two questions that required students to move answers into the appropriate categories. Students were advised to write the correct answer in the allocated area, where it states correct answer. Eighty eight of the possible 90 participants completed their assessments during the allotted time. Two students from two different classrooms were absent and did not complete the assessment. Once the assessments were completed participant responses were grouped from each of the three classrooms and labeled using the letters A, B, or C. Respectively, they were placed into large manila envelopes with their class letter on it. No further personal information was collected.

Data Analysis Approach

Researcher input questions and responses from the 15 items, found in Common Sense end of unit assessment into an excel spreadsheet and then compared it to the responses of the participants. Then researcher used percentages to measure how participants answered the questions in comparison to the provided answers from Common Sense Media. There were 88 participants, total. In each of the three fifth grades there were 30 participants per class, but during the assessment one student was absent in two of the three classes. Initially, the data was organized by each class and then combined as a whole for all three classes in total into one table.

Researcher examined how participants responded to the questions and then was able to comparatively analyze the data after calculating and tabulating the percentages of responses aligned to the eight components of digital citizenship identified by Howard Gardner/Good Play and Common Sense Media. The data was organized as the percentages of responses into the respective categories of self-image, digital footprint and reputation, information literacy, privacy and security, relationships and communication, cyberbullying, internet safety and creative credit and copyright. The responses were also organized using percentages to align with the Nine Elements of Digital citizenship (Ribble, 2011), as a cross-comparison to the previous tabulation to arrive at the findings. The data provided insight into the knowledge base of 88 fifth grade participants in one school about what they actually know about digital citizenship.

Chapter 4: Findings, Analysis and Discussion

Introduction

Data from 88 participants were compiled, tabulated, and analyzed in aggregate using calculated percentages. Data was imputed into charts to reflecting percentages of digital citizenship competency, and then compared for analysis with the digital citizenship curriculum answer key from Howard Gardner and Common Sense Media. A second analysis for the data was completed using Ribble's (2011), Nine Elements of Digital Citizenship as a cross-comparison.

Findings

The data suggested that 90% of the participants could identify online responsibilities, however none (0%) could identify what their responsibilities were to the larger community. Fifteen percent (15%) knew what being a responsible digital citizen means. Forty percent (40%) knew what information is private and what information is personal. Twenty two percent (22%) knew what information an identity thief could steal. Eighteen percent (18%) knew what personal information is okay to share online. Ninety three percent (93%) of the participants knew about cyberbullying. Eighty eight percent (88%) of the participants could identify the best way to respond to a mean message online. Seventy five percent (75%) of the participants could identify hurtful messages online. Seventy three percent (73%) of the participants could identify what a keyword in a search engine is. Fifty nine percent (59%) of the participants were able to do a search online, given certain topics. Less than one percent (0.25%) of the participants indicated

that they could do a search for information using key words. One percent (1%) of the participants knew when it was okay to use someone's work. Less than one percent (0.07%) of the participants knew what information was needed to provide a proper citation for an online article. Forty four percent (44%) of the participants knew what the first step was when using another person's work online.

Figure 1Common Sense End of Unit Assessment

Common Sense End of Unit Assessment

t

Questions	Correct Answer	T.P.	A	B	C	D	A, D	B, C	A, C	A, B	A,B, C	MIS	Y	N	% C.R.
Which sentence about your online responsibilities is true?	B	88	1	79		3	3	2							**90%**
What responsibilities do you have to your larger community online?	A,D	88	37	11	11	2		6	8			13			**0%**
What does being a responsible digital citizen mean to you?	Short Answer	88											16	72	**15%**
What information is private? What information is personal?	Private C,D Personal A,B	88											35	53	**40%**
What information could an identity thief use to steal your identity?	A,B	88	56	10	1					19		2			**22%**
What personal information is okay to share online without risking your privacy?	Short Answer	88											16	72	**18%**
To _____ someone means to use technology to upset someone on purpose.	C	88	3	2	82	1									**93%**

Common Sense End of Unit Assessment

Questions	Correct Answer	T.P.	A	B	C	D	A,D	B,C	A,C	A,B	C,D	A,B, C	A,C D	A,D, F	MiS	Y	N	% C.R.
Which would be the best way to respond to a mean message you got online?	D	88	5	2	2	77									2			**88%**
What messages are most likely meant to be hurtful?	A,D	88	12			21	55											**75%**
What are the search words you type into a search engine called?	A	88	64	13	4					3					4			**73%**
You want to search on the internet to find fun things for kids your age to do during the summer. What are the three best keywords for this topic?	A,D,F	88	6			1	4							52	25			**59%**
Which keywords would work best to search information about "Healthy Eating"? Which keywords would work best to search for information about the "Most Popular Songs"?	H.E: A,D M.P.S: B,C	88														22	66	**.25%**
When is it okay to use someone else's work?	A,D	88	3		1	77	5								2			**1%**
Which information is needed to provide a proper citation for an online article?	A,C,D	88	21		4	45	12			2	2				2			**1%**
What is the first step you need to do to use another person's work responsibly?	B	88	1	39	27	1		9							11			**44%**

T.P., refers to the total participants and percentage (%) of C.R. refers to percentage of participants who answered correctly. The chart addresses each of the 15 questions within the survey, the correct responses according to Common Sense Media, total participants, total participant responses as a whole group, and the percentages of participants who answered correctly. Full listing of questions, multiple choice options, correct answer and responses are listed in Appendix F.

Chart 2

Figure 2Percentages of Correct Responses From 88 Participants to 15 Questions From End of Unit Assessment From Common Sense Media

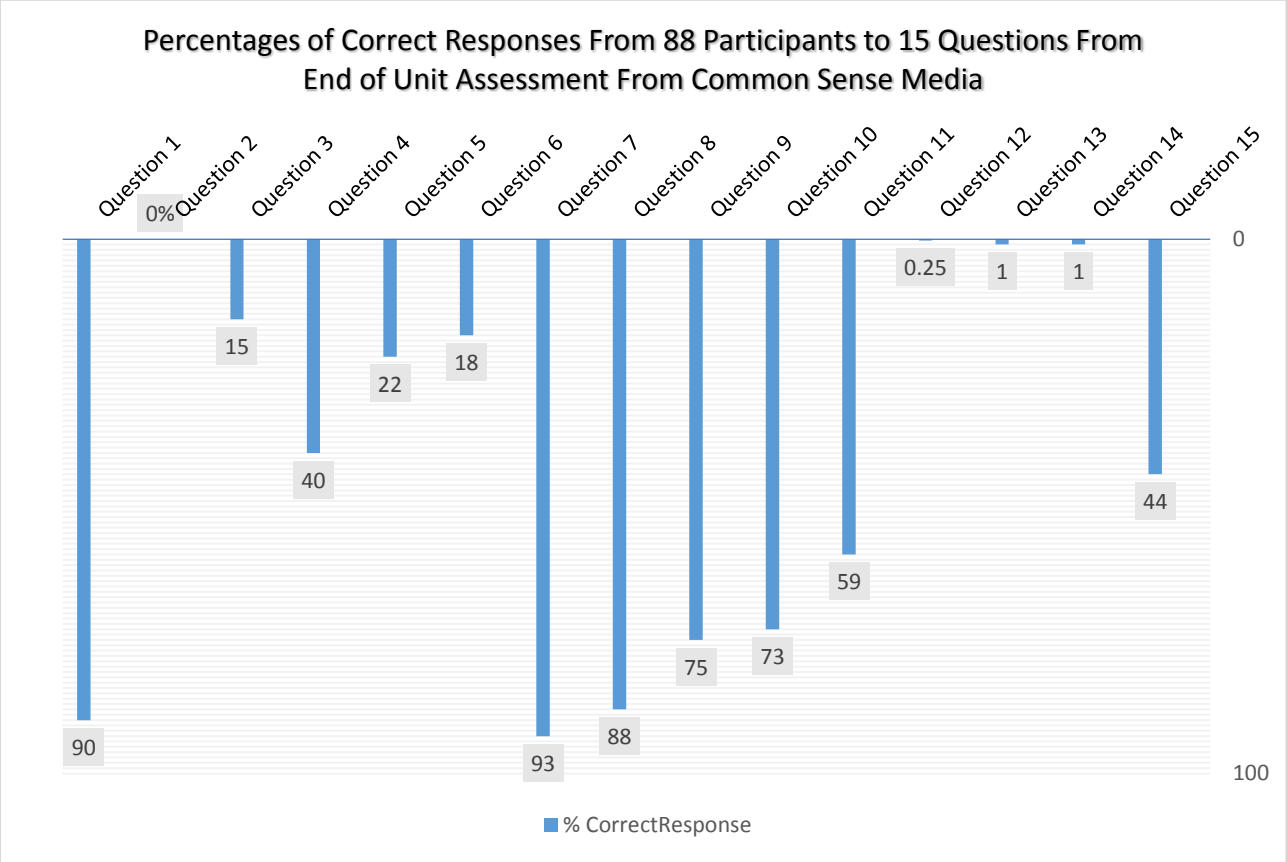


Chart 2 depicts the percentages of the 88 participants who answered the end of unit assessment correctly. A full listing of data from the responses to the 15 item end of unit assessment, unit one from Common Sense Media by questions, correct answers, and percentages by item is presented below:

1) Which sentence about your online responsibilities is true.

Answer: B

- 90% of participants answered this question correctly.

2) What responsibilities do you have to your larger community online?

Answers: A and D

- 0% of participants answered this question in full, correctly. 42% answered with A and 20% answered D.

3) What does being a responsible digital citizen mean to you?

Response Provided by Common Sense Media: Being a responsible digital citizen means that I protect myself, my family and friends, and other people online. It also means that I respect the feelings and work of other people online.

- 15% responded according to the response provided. 55% of participants provide little to no information to this question.

4) Which information is private? Which information is personal?

Answer: Private information is your phone number and street address. Personal information is favorite food and dogs name.

- 40% of participants were able to determine what information was private and what information was personal. 32% of participants were able to determine 2 out of the 4 correct responses.

5) What information could an identifying thief use to steal your identity?

Answer: A and B

- 22% of participants were able to answer this question correctly, with both answers. 64% responded to the question with the answer of a, which was partially correct. 11% responded with b.

6) What personal information is okay to share online without risking your privacy?

Response per Assessment Answer: I could share some information about my hobbies, favorite band and their latest song, favorite color, favorite food or favorite animal.

- 18% of participants responded by answer given by end of unit assessment. 25% responded with a limited answer. 35% of participants left no information or, inaccurate information.

7) To _____ someone means to use technology to upset someone on purpose.

Answer: C

- 93% of all the participants were able to answer this question correctly.

8) Which would be the best way to respond to a mean message online?

Answer: D

- 88% of participants were able to answer this question correctly.

9) What messages are most likely meant to be hurtful?

Answer: A and D

- 75% of participants answered this question correctly. 25% of participants answered the question with D. 14% of participants answered the question with A and received partial credit.

10) What are the search words that you type into a search engine called?

Answer: A

- 73% of participants were able to identify the correct answer.

11) You want to search on the internet to find fun things for kids your age to do during the summer. What are the three best keywords for this topic?

Answer: A, D, F

- 59% of participants were able to answer this question with all 3 answers. 41% of the students answered in some variation of this answer to include answers that were incorrect.

12) Which keywords would work best to search for information about "Healthy Eating"? Which key-words would work best to search information about the "Most Popular Songs"?

Answer: Healthy Eating: Nutrition and Recipes

Most Popular Songs: Hits and Music

- .25% of participants answered this question correctly. 49% of participants were able to answer the question with a partially correct response. They added one search word to each keyword.

13) When is it okay to use someone else's work?

Answer: A and D

- 1% of participants answered this question correctly with both answers. 88% of participants answered this question with the answer of D and .03% of participants answered with an A.

14) Which information is needed to provide a proper citation for an online article?

Answer: A, C, D

- .07 % of participants were able to answer this question with 100% accuracy. 73% of participants were able to respond with one correct answer out of 3.

15) What is the first step you need to do to use another person's work responsibly?

Answer: B

- 44% of participants were able to answer this question correctly. 31% of participants thought that answer C was correct.

Figure 3 Good Play and Common Sense Media Eight Components of Digital Citizenship

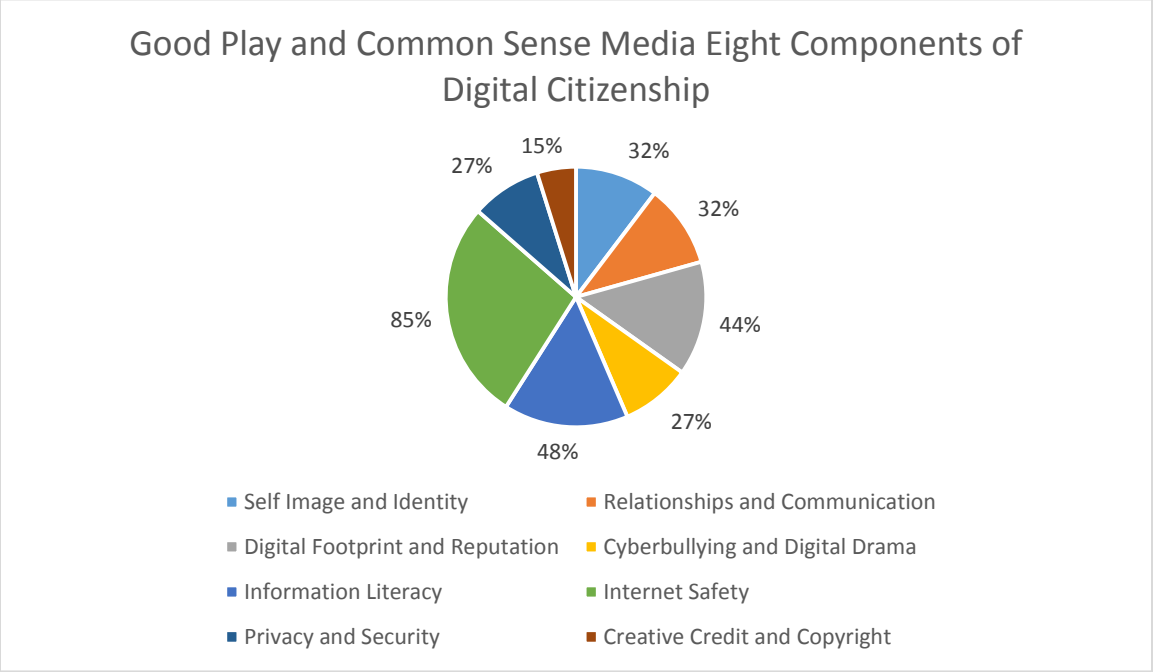
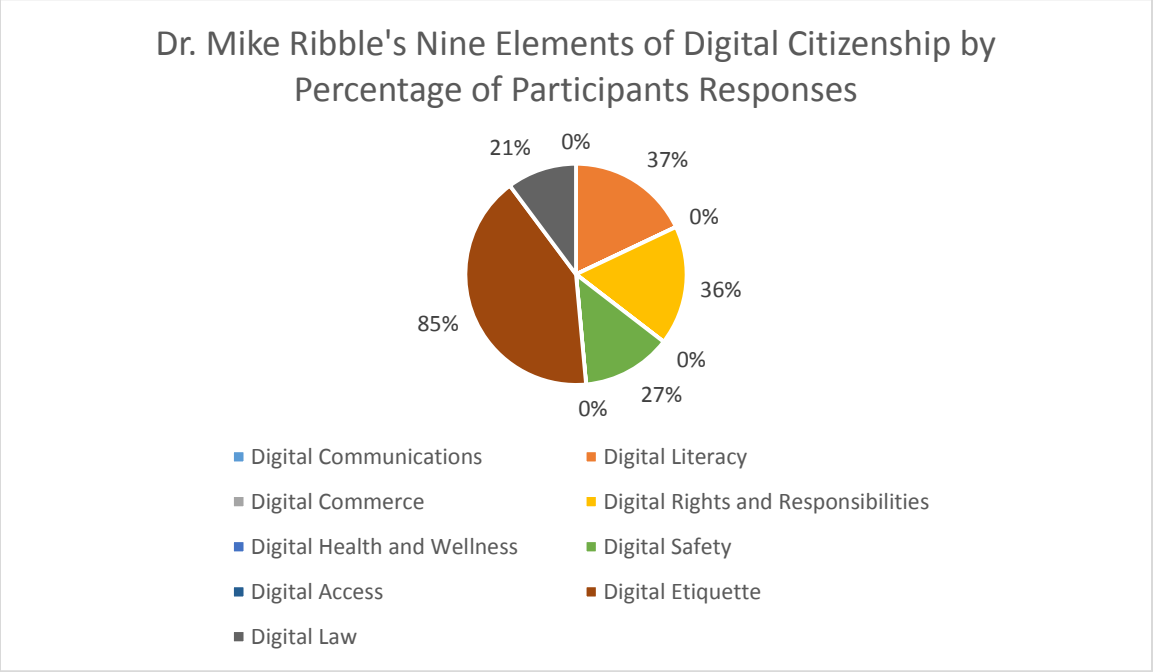


Figure 4 Dr. Mike Ribble's Nine Elements of Digital Citizenship by Percentage of Participants Responses



Themes

The first section of the end of unit assessment is self-image and identity. This component addresses avatars, profile pictures and the manner in which people communicate online. Self-image and identity is identified in all 15 questions of the end of unit assessment as it represents how a person is presenting themselves online. This study found that participants had an average of 32% in terms of an understanding of their digital image. The second was digital footprint and reputation. All 15 questions addressed digital footprint and reputation, since being online suggests a permanent footprint. Participants had an average of 32% in terms of their understanding of their digital footprint and reputation. The third was information literacy which was specifically addressed in questions 10, 11, and 12. Participants had an average of 44% understanding of what digital literacy means. The fourth was privacy and settings, which was

addressed in questions four, five, and six. Participants had an average percentage of 27% in terms of their understanding of privacy and settings. The fifth was relationships and communications, which was addressed in questions one, two, three, and eight. Participants had an average of 48% understanding of their relationships and communications online. The sixth was cyberbullying and digital drama, which was addressed in questions seven, eight and nine. Participants had an average of 85% of understanding cyberbullying and digital drama. The seventh was internet safety that was addressed in questions four, five, and six. Participants had an average of 27% of understanding about internet safety. The eighth was creative credit and copyright. This was addressed in questions 13, 14, and 15. Participants had an average of 15% of understanding what creative credit and copyright means.

Data were also compared and analyzed based on Ribble and his Nine Elements of Digital Citizenship (2011). Digital literacy was addressed through questions 10, 11, and 12. Participants had an average of 37% of an understanding of digital literacy. Digital etiquette was addressed in questions seven, eight, and nine. Participants had an average of 85% of an understanding of Digital etiquette. Digital rights and responsibilities, which include privacy and freedom of speech were addressed through questions one, two, three, and four. Participants had an average of 36% of understanding about digital rights and responsibilities. Digital security, which addressed online protection and safety, was addressed via questions four, five, and six. Participants had an average of 27% of a comprehension rate for digital security. Digital law, which addresses the crime of stealing another's work, was considered in questions 13, 14, and 15. Participants had an average of 21% of a comprehension rate regarding Digital law.

Digital health and wellness, which addresses the psychological and physical ramifications of being online including repetitive online motions or sound ergonomics was not analyzed as a part of this study. Nor, did it address how psychologically, people can become addicted to being online.

Ribble and his Nine Elements of Digital Citizenship (2011) also considers digital access and ensuring that all persons have equal access to participate electronically. It must be noted that in this study, the assessment was not distributed electronically, due to the fact that one set of 30 Chromebooks were shared with three classrooms. Therefore the participants did not have the digital access to be able to take the end of unit assessment electronically. In addition, the end of unit assessment for unit one did not address digital commerce, which included illegal downloading or making purchases that are in conflict with other countries laws or regulations. Digital communication and how one communicates and discerns applications online additionally were also not addressed as a part of this study.

Chapter 5: Discussion, Analysis and Conclusions

Summary of Major Findings

From this sample of participants this study found that further education on digital citizenship is needed at the fifth grade level. The data indicated that from this sample of participants, 68% of the overall participants had little to no understanding of digital citizenship as measured by this end of unit assessment. When broken down by the eight components of digital citizenship presented by Common Sense Media, there was further insight into which areas participants had knowledge in, and which areas participants would benefit from further guidance and instruction.

The sections that present the highest vulnerability amongst these 88 participants are in the area of copyright and creative credit, where they had an average of 15% comprehension. The second area was with privacy and internet safety where participants had an average of 27% understanding. The third was digital image and footprint, where the average percentage was 32% understanding. Digital literacy has an average of 44% understanding. Relationships and communications had an average of 48% understanding. Finally, cyber-bullying had an average percentage of 85% understanding.

From this research, researcher found that among these 88 participants, they had most knowledge of cyber-bullying. Participants in this research demonstrated that further education and guidance is needed with regard to copyright and creative credit, internet safety, privacy, digital image, digital footprint, digital literacy and digital relationships and communications.

A comparison using Ribble's Nine Elements of Digital Citizenship to the end of unit assessment, indicated that there was an 23% overall level of comprehension of digital citizenship, which include the four sections not addressed in the end of unit assessment; digital communication, digital commerce, digital health and wellness as it pertains to physical and psychological issues, and digital access. The data indicated that areas where more education are needed are in digital literacy, digital rights and responsibilities, digital safety and security, and digital law. Digital literacy had 37% competency. Digital rights and responsibilities had 36% competency. Digital Safety and security had 27% competency. Digital law had 21% competency. The area where participants demonstrated greater competency was with digital etiquette as it applied to online conduct.

It has to be noted that this group of fifth grade participants within this school have limited online access and no district mandated or required digital citizenship curriculum. Therefore, one of the key questions that this study raised was about how policy and funding might be affecting the development of digital citizenship due to inequitable digital access and a digital divide. In 2014, Proposition 30 and Local Control Funding Formula (LCFF), ensured that most districts would receive more funding. LCFF was supposed to benefit low income districts, with a 50 to 75 percent increase per student (Pace, 2014). While LCFF is not supposed to be fully implemented until 2020, in 2016 a lack of funding and digital access are still a threat to public schools. Additionally, we may witness further changes to education policy, which could affect how public schools are funded in the future.

This study concluded that further digital citizenship education is warranted to protect the safety and well-being of at least this sample of 88 participants while they might be online. If this

sample is representative of the online knowledge base of fifth graders, then electronic identity theft, cyber bullying, predatory contact, unsolicited marketing to minors, cyber-exposure to adult content, and personal information breaches including visual media remain major threats that students who are minors face. This study demonstrates that while technology has become a requirement within the classroom, these fifth grade participants do not have the foundation to protect themselves while online.

Limitations/Gaps in the Research

The limitations to this research were that the researcher conducted this end of unit assessment for three fifth grade classes and the findings were limited to the responses of these 88 participants. Additionally, this end of unit assessment was one of three assessments, which means that the 15 questions in this unit one assessment do not address all eight components of digital citizenship in depth and the evidence derived from this research is incomplete, and may not be indicative of the knowledge base of digital citizenship for all fifth graders. Therefore this study is not generalizable to other fifth grade populations.

This study was conducted in a middle class public school in Northern California. Variables that possibly could change the outcome of the research would be public schools that have greater funding to support technology in the classroom and education about digital citizenship. Public schools with limited funding could also offset the findings, due to lack of technology within the classroom and teachers who are not trained to teach digital citizenship.

Lastly, findings might be different within a private school or charter school setting, where Common Core State Standards nor other mandates for education govern how they will be

funded. Student access to technology and teachers who are trained to guide student's online activity are also factors that contribute to gaps in student knowledge of digital citizenship.

Implications for Future Research

Evidence from my research indicated that there is a correlation between funding and how schools can be adequately equipped in meeting 21st century skills, which include modern technology within the classroom, training of teachers, and staff to keep up with the mercurial nature of technology and how to implement digital citizenship. Additionally, schools having the infrastructure, bandwidth and up to date AUP's for schools.

Overall Significance of the Study

The significance of this study is primarily that it demonstrates that there is initial evidence to support the need for further guidance and education about how students conduct themselves online. This is especially pertinent to one's digital footprint and reputation, digital literacy, privacy, relationships and communication, internet safety, credit and copy.

Overall, this sample group was from a middle class public school district, which is CCSS compliant, adheres to federal mandates to ensure access to funding, has a strong parental involvement, and yet within these three fifth grade classes they have to share a set of 30 Chromebooks, and do not have a digital citizenship curriculum to support online usage to meet the demands of the CCSS. Not only is having access to technology a necessity to prepare students to be 21st century competent, but it is equally imperative to provide education and training about how to use technology properly, effectively, and constructively.

Without proper funding for schools to have up to date technology, digital access, and curriculum to teach digital citizenship, students remain at risk whilst using technology. Funding is directly related to how public schools run and operate, and presently, there still remains an inequality. Schools with more funding have more access to technology and resources to educate students about the importance of what it means to be a digital citizen. Schools with more resources have worked against what the funding laws are trying to create.

A digital footprint is permanent and the repercussions of our online behaviors have not had sufficient time to mature and materialize as to what the long- term ramifications will be. This study also indicates that without sufficient privacy laws to protect children under the age of 18, instead of the current age of 13, information obtained while online will be used as a form of exploitation and therefore is of crucial significance to consider in future educational research regarding digital citizenship.

For the past 20 years, political agendas have attempted and failed to make technology accessible to all public schools. Consequently, a greater digital divide has emerged. Public schools are required to use technology to meet CCSS standards, but are doing so without adequate guidance and support. It is the researcher's understanding that the Nigerian proverb, "ora na azu nwa"; (it takes a village to raise a child), is pertinent to this study as it is a collective responsibility to champion the rights of children as digital citizens. Ensuring that they have digital access and education to prepare them to meet 21st century skills will create a platform for future generations to engage, contribute and participate as virtuous, ethical digital citizens who can build a productive, innovative, social heritage for human life.

About the Author

Aimee Green Logan is an elementary school teacher in Northern California. She received her Multiple Subjects Teaching Credential from Dominican University while obtaining her M.S. in Education. She has an M.A. in Psychology from Southwestern College and a degree in Ayurvedic Medicine from the California College of Ayurveda. She obtained her BA from the University of San Francisco where she majored in Interpersonal Communications and Psychology. She is a lifelong learner, philanthropist, naturalist, and child welfare advocate. Her pastime is working as an apiarist in her garden.

She is attempting to sit on the technology board for the California Department of Education as they build technology standards for the Common Core as well as at the school in which she teaches. She is interested in supporting laws and regulations that continue to protect and support the welfare of minors online. Based on this study, she would like to bring digital citizenship into her own classroom and be able to apply some of the strategies that she has learned through the conduct of this research study. In the future, the author hopes to pursue doctoral work, and eventually publish a book.

References

Australian Government. (2014). Department of communications. Retrieved from http://www.communications.gov.au/funding_and_programs/cyber_safety

Bennett, L.B., Aguagya, R.C., & Field, S. L. (2016). At home in the world: Supporting children in human rights, global citizenship, and digital citizenship. *Childhood Education, 92*(3), 189-199.

Bennett, L.B., Aguagya, R.C., & Field, S. L. (2016). At home in the world: Supporting children in human rights, global citizenship, and digital citizenship. *Childhood Education, 92*(3), 189-199.

Berson, L.R., & Berson, M. J. (2006). Children and their digital dossiers: Lessons in privacy rights in the digital age. *International Journal of Social Education, 21*(Spr-Sum), 135-145.

Campbell, K., & Davis-Packard, K. (September 18, 2000). How ads get kids to say I want it! Retrieved from http://www.christianmonitor.com

Carens, J. H. (2000). *Culture, citizenship, and community. A contextual exploration of justice as evenhandedness*. Oxford, England: Oxford University Press.

Citizen [def.1]

citizenship [def. 2]. (http://merriam-webster.com/dictionary/citations.).

Cohen, J. (1999). "Changing paradigms of citizenship and the exclusiveness of the demos". *International Sociology, 14*(3), 245-268.

Common core state standards initiative. (2017). Retrieved from http://www.corestandards.org

Crowen-Fletcher, J. (1994). *It takes a village* (1st ed.). New York, NY: Scholastic Inc.

Creswell, J. W. (2014). In Markanich M. (Ed.), *Research designs* (4th ed.). California: Sage Publications.

Crowley, B. (2015). Is Google Illegally Spying on Your Students? New FTC Complaint Says It Is. Retrieved from http://www.edlawinsights.com/2015/12/08/is-google-illegally-spying-on-your-students-new-ftc-says-it-is

Cyberbullying. (2012). Retrieved from https://www.nemours.org/content/dam/nemours/wwwv2/filebox/service/par

Department of Education, W. D. (1996). Getting america's students ready for the 21st century: Meeting the technology literacy challenge. A report to the nation on technology and education. Retrieved from http://www.eric.gov

Digital citizenship. (2017). Retrieved from http://www.commonsensemedia.org

Electronic Frontier Foundation. (2015). Google deceptively tracks students' internet browsing, EFF says in FTC complaint. Retrieved from http://www.eff.org/press/releases/google-deceptively-tracks-students-internt-browsing

Elkind, P. (2015, 12/23). Business gets schooled. *Fortune,* Retrieved from http://www.fortune.com/common-core-standards/

Executive Office of the President. (2014). *Big data: Seizing opportunities, preserving values.* (Government). Washington DC: The White House.

Family Policy Compliance Office. (2016). Protection of pupil rights amendment. Retrieved from http://www.familypolicy.ed.gov/ppr

Federal Trade Commission. (2016). Protecting america's consumers. Retrieved from

https://www.ftc.gov/policy

Finch, K. (2014). COPPA in the classroom. Retrieved from http://iap.org/news/a/coppa-in-the-classroom

Floridi, L. (1999). "Informational ethics: On the theoretical foundation of computer ethics". *Ethics and Informational Technology*, *1.1*, 37-56.

Fodeman, D., Monroe, M. (2012). Safe practices for life online a guide for middle and high school.

Gangadharan, S. P., & Wooley, S. (2014). Data driven discrimination. Retrieved from http://www.slate.com/articles/technology/future_tense_/2014/06/big_data_can_perpetuate_poverty_and_inequlaity.html.

Gardner, H., & Hatch, T. (1989). Multiple intelligences go to school: Educational implications of the theory of multiple intelligences. *Educational Researcher*, *18*(8), 4-9.

Gardner, H. (1993). *Frames of mind: The theory of multiple intelligences* (6th ed.). New York, NY: BasicBooks.

Gardner, H., & Davis, K. (2013). *The app generation: How today's youth NAvigate identity, intimacy, and imagination in a digital world.* (1st ed.). New Haven, CT: Yale University Press.

Gebhart, G. (2017). Spying on students: School-issued devices and student privacy. Retrieved from http://www.eff.org/wp/school-issued-devices-and-student-privacy

Good Play Project- Project Zero. (2016). Retrieved from http://pz.harvard.edu/projects/the-good-play-project

Guardchild. (2017). Internet statistics. Retrieved from https://www.guardchild.com/statistics/

Guthrie, J., & Springer, M. (2004). "A nation at risk" revisited: Did "wrong" reasoning result in "right" results? at what cost? *Peabody Journal of Education, 79*(1), 2016-7-35. doi:http:www.jstor.org/stable/1493062

Harte, H. A. (2011). E-professionalism for early care and education providers. *Dimensions of Early Childhood, 39*(3), 3-9.

Hassel, B. C., & Hassel, E. A. (2011). Teachers in the age of digital instruction., 1-10.

Hauben, M., & Hauben, R. (1997). *Netizens* IEEE Computer Society Press.

Herold, B. (2014). Prominent ed-tech players- data-privacy policies attract scrutiny. Retrieved from http://www.edweek.org/ew/articles/2014/04/16/28privacy_ep.h33.html.

Hollandsworth, L., Dowdy, L., & Donovan, J. (2011). Digital citizenship in K-12: It takes a village. *Techtrends, 55*(4), 37-46.

Hope, A. (2015). Schoolchildren, governmentality and national E-safety policy discourse. *Discourse: Studies in the Cultural Politics of Education, 36*(3), 343-353.

Internet live stats. (2016). Retrieved from http://www.internetlivestats.com/internet-users/

Israel, C. R. (2012). What does it mean to be a global citizen? *Kosmos Journal,* (Spring/Summer), 79.

ISTE standards for students. (2017). Retrieved from http://www.iste.org/standards/standards/for-students

Johnson, G. J. (1985). *Computer ethics*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

Kivunja, C. (2014). Perspectives of how digital natives learn. *International Journal of Higher Education, Volume 3*(1), 94-95-105.

Kymlicka, W. (2000). *"Citizenship in culturally diverse societies: Issues, contexts, concepts", in*

a citizenship in diverse societies. Oxford, England: Oxford Press.

Mossberger, K., Tolbert, C., & McNeal, R. (2008). Excerpts from digital citizenship: The internet, society, and participation. *First Monday, 13*(2) doi:10.5210/fm.v13i2.2131

Leswing, K. (2015, Why google is winning the race for american schools. *Fortune*,

Microsoft. (2012). Youth Spark. Retrieved from https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/program

National Cyber Security Alliance. I want to stay safe online. Retrieved from https://www.staysafeonline.org

Ohler, B. J. (2010). In Stollenwerk D., Bartlett A. D., Greenberg K., Stapleton V. and Dunham A. (Eds.), *Digital community, digital citizen*. Thousand Oaks, California: Sage Publications.

Onosko, J. (2011). Race to the top leaves children and future citizens behind. *Democracy & Education, 19*(2), 1-11.

Orth, D., Chen, E. (2013). The strategy for Digital Citizenship. *Independent School, 72*(4), 56-63.

Palfrey, J. G., Gasser, U. (2008). *Born digital : Understanding the first generation of digital natives*. New York: Basic Books.

Pointras, L., Bonnefor, M., & Wilutzky, D. (Producers), & Pointas, L. (Director). (2014). *Citizenfour*. [Video/DVD] Radius-TWC.

Policy Analysis for California Education. (2014). Retrieved from http://www.edpolicyinca/projects/lcffrc

Polikoff, M. (2014). Common core state standards assessments

challenges and opportunities. Retrieved from http://www.americanprogress.org/wp-content/uploads/2014/04/CCCAAssessment

Pointras, L., Bonnefor, M., & Wilutzky, D. (Producers), & Pointas, L. (Director). (2014). *Citizenfour.* [Video/DVD] Radius-TWC.

Policy Analysis for California Education. (2014). Retrieved from http://www.edpolicyinca/projects/lcffrc

Polonetsy, J., & Tene, O. (2015). Who is reading whom now: Privacy in education from books to MOOCs. *Vand, J ENT.& TECH. L., 17*(4), 9/05/16-927-989.

Power, R. (2011). *Child identity theft*

new evidence indicates identity thieves are targeting children for used social security numbers. ().Carnegie Mellon CyLab.

Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon, 9*(5), 2-6.

Ribble, M., (2011). Digital citizenship in schools.

Richardson, W. (2008). Footprints in the digital age. *Educational Leadership, 66*(3), 16-19.

Rouse, M. (2014,). Definition

digital divide. Retrieved from http://www.whatis.techtarget.com/definition/digital-divide

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. doi:10.1111/j.1365-2729.2008.00304.x

Skyler, J. (2004). The online disinhibition effect. *Cyberpsychology & Psychology, 7*(3), 321-326.

Solove, D. (2014, April 28). Why did inBloom die? A Hard Lesson About Education Privacy. Retrieved from https://www.safecloud.org/2014/4/28/why-did-inbloom-die-a-hard-

lesson-about-education-privacy

Sook-Jung, L., & Young-Gil, G. (2007). Children's internet USe in a family context: Influence on family relationships and parental mediation. *Cyberpsychology & Psychology, 10*(5) doi:10.1089/cpb.2007.9975

Tan, M. M., & Park, J. (2014). *Fostering digital citizenship through safe and responsible use of ICT*. Bangkok, Thailand: UNESCO Bangkok.

The Partnership For 21st Century Skills. (2008). 21st century skills. education & competitiveness. Retrieved from http://www.p21.org/storagedocuments/21st_century_skills_education_and_competitiveness

UNESCOBKK. (2014). Fostering digital citizenship through safe and responsible use of ICT. Retrieved from http://unescobkk.org/fileadmin/user_upload/ict/SRU-ICT/SRU-ICT_mappingreport_2014.pdf

Valcke, M., Schellens, T., Van Keer, H., & Gerarts, M. (2007). Primary school children's safe and unsafe use of the internet at home and at school: An exploratory study. *Computers in Human Behavior, 23*(6), 2838-2850. doi:http://dx.doi.org/10.1016/j.chb.2006.05.008

Visser, M. (2012,). Digital literacy definition. Retrieved from http://www.connect.ala.org/node/181197

Wagner, T. (2003). Reinventing america's schools. Retrieved from http://www.tonywagner.com/227

Weiner, N. (1948). *Cybernetics: Or control and communication in the animal and the machine*. Boston, MA: Technology Press.

Weiner, N. (1954). *The human use of human beings cybernetics and society*. United States: Da Capo Press.

Weston, M. (2010). *Funding california schools: The revenue limit system.* (). California: Public Policy Institute of California.

Wojniak, J., & Majorek, M. (2016). Children and ICT european initiatives and policies on protecting children online. *Universal Journal of Educational Research, 4*(1), 131-136.

Wolak, J., Mitchell, K. & Finkelhor, D. (2006). Online victimization of youth: Five years later. Retrieved from Http:missingkids.com/en/_US/publications/NC167.pdf

World Summit on the information society. (2003). Declaration of principles. Retrieved from http://www.itu.int/net/wsis/docs/geneva/official/dop.html

Appendix A Sample Letter of Permission to Principal and Teacher of Record

Dear ,

This letter confirms that you have been provided with a brief description of my MA thesis research project, which concerns factors related to digital citizenship, and the quality of knowledge 5th graders have. This letter confirms that you give your consent for me to visit your school to provide an end of unit assessment designed by Common Sense, by Dr. Howard Gardner from the Harvard School of Education to your 5th grade classes. This project is an important part of my graduate requirements for my MA in Education, and is being supervised by Dr. Suresh Appavoo, Professor of Education at Dominican University of California. As we discussed, I will make every effort to ensure that my data collection does not interfere with your regularly scheduled classes and workshops, and that your students are treated with the utmost discretion and sensitivity.

Please note that researcher will not publish or identify the name of the school or the names of the students to ensure confidentiality. If you have further concerns you may contact my research supervisor, Dr. Suresh Appavoo, at (415) 457-4440 or the Institutional Review Board for the Protection of Human Participants at Dominican University of California by calling (415) 482-3547. If my request to visit your establishment to conduct this research meets with your approval, please sign and date this letter below and return it to me in the enclosed self-addressed, stamped envelope as soon as possible. Please feel free to contact me if you have any questions about this project. Thank you very much for your time and cooperation.

Sincerely,

Aimee Logan
Address

I agree with the above request

Signature _____ Date_____
]

Appendix B Mike Ribble's Nine Elements of Digital Citizenship based on Respect, Educate and Protect

Respect:

- Digital access**:** Advocating for equal digital rights and access is where digital citizenship starts.
- Digital etiquette: Rules and policies aren't enough — we need to teach everyone about appropriate conduct online.
- Digital law: It's critical that users understand it's a crime to steal or damage another's digital work, identity or property.

Educate:

- Digital communication: With so many communication options available, users need to learn how to make appropriate decisions.
- Digital literacy: We need to teach students how to learn in a digital society.
- Digital commerce: As users make more purchases online, they must understand how to be effective consumers in a digital economy.

Protect:

- Digital rights and responsibilities: We must inform people of their basic digital rights to privacy, freedom of speech, etc.
- Digital safety and security: Digital citizens need to know how to protect their information from outside forces that might cause harm.
- Digital health and wellness: From physical issues, such as repetitive stress syndrome, to psychological issues, such as internet addiction, users should understand the health risks of technology.

(Ribble, 2011)

Appendix C Student Privacy Pledge

We Commit To:

- Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- Not sell student personal information.
- Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.

1. Not build a personal profile of a student other than for supporting authorized educational/ school purposes or as authorized by the parent/student.
2. Not make material changes to school service provider consumer privacy policies
3. without first providing prominent notice to the account holder(s) (i.e., educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements.
4. Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.

- Not to collect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution/agency, teacher or the parent/student.

- Disclose clearly in contracts or privacy policies, including in a manner easy for parents and teachers to understand, what types of student personal information we collect, if any, and the purposes for which the information we maintain is used or shared with third parties.
- Support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent.
- Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.
- Require that our vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information.
- Allow a successor entity to maintain the student personal information, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

This pledge shall be effective as of January 1, 2015.

Appendix D Section 60605.4 is added to the Education Code, to read: 60605.4.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1.

Section 60605.4 is added to the Education Code, to read: 60605.4.

On or before July 31, 2019, the Instructional Quality Commission shall consider recommending to the state board computer science content standards for kindergarten and grades 1 to 12, inclusive, pursuant to recommendations developed by a group of computer science experts. The Instructional Quality Commission shall consider existing computer science content standards, which include, but are not limited to, the national K–12 computer science content standards developed by the Computer Science Teachers Association, and consider content standards that include, but are not necessarily limited to, standards for teaching coding. For the purposes of this section, "coding" is the process of converting a program design into an accurate and detailed representation of that program in a suitable language.

(1) The Superintendent, in consultation with the state board, shall consider convening the group of experts referenced in subdivision (a), and shall ensure that the members of the group include, but are not necessarily limited to, all of the following.

Appendix E Common Sense End of Unit One Assessment and Answer Guide

15 Question End of Unit Assessment from Unit One Common Sense Media

1) Which sentence about your online responsibilities is true.

a. I should post photos of others without permission
b. I should respect myself and others when I am online
c. I should choose a username that shows my private information

Answer: B

2) What responsibilities do you have to your larger community online?

a. Stand up to cyberbullying
b. Protecting my passwords
c. Not giving out my phone number
d. Giving credit for information I find online

Answers: A and D

3) What does being a responsible digital citizen mean to you?

Response Provided End of Unit Assessment: Being a responsible digital citizen means that I protect myself, my family and friends, and other people online. It also means that I respect the feelings and work of other people online.

4) Which information is private? Which information is personal?

a. My favorite food
b. My dog's name

c. My phone number

d. My street address

Answer: Private information is your phone number and street address. Personal information is favorite food and dog's name.

5) What information could an identifying thief use to steal your identity?

a. Credit card number

b. My street address

c. My favorite class

Answer: A and B

6) What personal information is okay to share online without risking your privacy?

Response per Assessment Answer: I could share some information about my hobbies, favorite band and their latest song, favorite color, favorite food or favorite animal.

7) To _____ someone means to use technology to upset someone on purpose.

a. Greet

b. Email

c. Cyberbully

d. Misunderstand

Answer: C

8) Which would be the best way to respond to a mean message online?

a. Argue with the sender face-to-face

b. Share the message with your friends

c. Send a mean message back to the sender

d. Talk to a parent or family member about the message

Answer: D

9) What messages are most likely meant to be hurtful?

a. No one wants to go to your party
b. You always tell the funniest jokes
c. Way to go! You're a star!
d. I think your hair looks dumb

Answer: A and D

10) What are the search words that you type into a search engine called?

a. Keywords
b. Results
c. Addresses

Answer: A

11) You want to search on the internet to find fun things for kids your age to do during the summer. What are the three best keywords for this topic?

a. Kids
b. Hot
c. Sun
d. Summer
e. Seasons
f. Activities

Answer: A, D, F

12) Which keywords would work best to search for information about “Healthy Eating”? Which key-words would work best to search information about the “Most Popular Songs”?

a. Nutrition
b. Hits
c. Music
d. Recipes

Common Sense Answer: Healthy Eating: Nutrition and Recipes

Most Popular Songs: Hits and Music

13) When is it okay to use someone else’s work?

a. I provide a citation for the work
b. I copy someone else's work without permission
c. I put my own name on it
d. I get permission from the creator and give proper credit

Answer: A and D

14) Which information is needed to provide a proper citation for an online article?

a. Author’s name
b. City and author’s birth
c. Publication date or date you read article online
d. Title of article and website

Answer: A, C, D

15) What is the first step you need to do to use another person’s work responsibly?

a. Credit yourself for the work

b. Find out who created the work

c. Give credit only when you know who the creator is

d. Use it without the creator's knowledge if it is free

Answer: B

Appendix F Website Resources in Digital Citizenship

- www.edutopia.org/cyberbullying-internet-digital-citizenship-resources
- www.ikeepsafe.org/educators/more/c3-matrix/
- www.edweb.et/digtialcitizenship
- www.ciconline.org/digitalcitizenship/inctrl
- www.commonsensemedia.org/educators/educate-families
- www.connectsafely.org/wp-content/uploads/securityguide.pdf
- www.childnet.com
- www.commonsense.org/
- www.edutopia.org/social-media-education-resources
- www.ncpc.org/topics/internet-safety
- www.safetynet.aap/org/
- www.staysafeonline.org/