Reconceptualizing Digital Citizenship:

Six Facets of the Internet that K-12 Educators Must Ensure Students Understand

Lauren Elizabeth LePage Harrelson

Eastern Connecticut State University

In an undergraduate journalism course on media law, my professor, Kevin Kemper, often remarked that the World Wide Web is the new Wild West. Governments are still grappling with how to manage the Internet and to what extent to moderate it. Today teachers also find themselves wondering to what extent they must teach digital skills since most children are exposed to the Internet from an incredibly young age. Indeed, today's youth must be taught that the web truly is the Wild West, which means it can be exciting and vast, but it can also be quite dangerous and misleading. They can be led astray by mirages (falsified information, phishing e-mails), they can be robbed of their identity or spied on (viruses, spyware), and much more. Worse, their parents are also victims because the Internet is still unfamiliar territory for many. Since children's parents often cannot guide them, teachers must lead the way. As an educator, I will challenge and rename the concept of "digital citizenship," then explain how and why I believe educators should teach particular Internet knowledge within K-12 classrooms.

Ribble (2011) is largely credited with defining the concept of digital citizenship within school curriculums. He breaks his model down into nine facets, some of which I support while others I believe to be mislabeled, misconstrued, unnecessary, or wrongly categorized. The term digital citizenship itself seems to suggest that we are all citizens in a shared community, which would mean we have a shared sense of values or political beliefs. Communities form around some common ground. For instance, a citizen of the United States presumably believes in or at least supports our democracy. A citizen is assumed to know our history and our laws. In this context, then, it does not make sense for us to consider ourselves "digital citizens," as Ribble (2011) suggests. Rather, we are all diverse people around the globe using the Internet as a tool for varying purposes. We are all individuals gallivanting around the online Wild West. We may not be citizens, but as individuals in this shared space, we should all keep a set of facts about the

Internet in mind. This would make us "knowledgeable Internet users" rather than "digital citizens." Our goal as educators should be "to empower students to make smart, responsible, and respectful decisions when using media" (Orth & Chen, 2013, p. 58). To do this, we will need to create "mini-lessons at the point of need" (Moreillon, 2013, p. 27) so that we can fit internet skills in our already over-packed curriculum.

The digital trail. The most important concept for students and adults alike to fully understand is the digital trail. We should regularly remind ourselves and our students that someone is always watching anything we do on the Internet. Thus, true privacy does not exist. We should always be mindful of the digital trail we are leaving behind us, since it will affect our individual futures and our safety. Many people have a false sense of security online and on their digital devices. They believe, for example, that their photos and status updates on Facebook are private because they have limited the access to a specific group of people. However, anyone in that group could easily do a screenshot of a photo or status update, then post it on the web for all to see. They could also e-mail that screenshot to an employer, a news organization, or any other potentially interested party. If Facebook experiences a technical error (and it has done so numerous times), a person's "wall" or other private details could suddenly be exposed to the world. Something similar actually happened in 2010 with their Facebook chat feature. Social media sites are not alone with these problems: E-mails can also be compromised. Anyone can forward a message to another person (or screenshot it). Moreover a judge could subpoena e-mail records in many court cases. All of these dilemmas are easy to demonstrate for students by simply doing screenshots in front of them. This shows them how quick and easy it is. We could also help students understand by addressing current events that relate to these breaches of privacy. This is particularly important for students in middle school and beyond.

We haven't even looked at the concept of tracking yet, which is done frequently across the Internet. "Cookies" in our browsers track our clicks and record data for companies. Marketers use this information to improve their advertisements and ultimately their sales. Several search engines collect data when we are signed in or simply by tracking our IP address. The end result is that "America's youth need to know that the trail they leave online — the sites they visit, the photos they share, the purchases they make — promises to follow them for a long time to come" (Gardner, 2013). Unfortunately, many students and adults seem unmoved by these invasions of privacy. "Only about half of all consumers have concerns about their data and privacy: This may be good for marketers, but it's also indicative of just how tough it will be to get young people to care about protecting themselves online" (as cited in Gardner, 2013).

Many students and adults also mistakenly believe that they can quickly and easily erase their digital trail by deleting content on the web. They believe that when they have clicked on "delete" or "remove," the content has truly vanished. This is far from the truth. Ribble (2011) points out that "even after the information is deleted it continues to 'live on' in cyberspace" (p. 23). In fact, servers often retain that data. There are also web sites that simply crawl the web, creating and storing cache versions of sites in databases. Students can get a better understanding of this by looking at web sites, particularly blogs, using the Wayback Machine. Ultimately, teachers must help students realize that once they put something out using any form of digital media (texts, emails, blog content, etc.), they cannot take it back. They are taking a risk. Cyber bullies will use photos and more against them. Employers will "use Web 2.0 technologies and social media to vet profiles of potential hires" (Greenhow, 2010, p. 25). College recruiters often do the same. Therefore, we must help students learn "what information to share and how to

handle their online identity" (Fredrick, 2013, p. 20). As part of this, we must help them become literate in the computer terminology surrounding these issues (cookies, cache, etc.).

Teachers must also help students learn how to mask their online trail by utilizing different usernames. Many youth and adults use the same pseudonym across the Internet, which makes it incredibly easy to background them. I have done this before. Using this strategy, I can often find out people's full names, general location, employer, and ultimately their street address — and I am not even a hacker. I am just skilled at navigating the web, and I know that many people share far too much information attached to their username. I also know that many people do not realize their directory information (home address & phone number) are listed online as public information, often accessed through sites like Pipl.com and Whitepages.com. Unfortunately, as Reddit user travysh points out, "all of this data is public data. The data itself isn't going away, [sic] opting out just makes people who want to find it have to look a little harder." This means we must help students, especially youth, learn to keep their names and their parents' names secret when they use sites across the web.

As a whole, teachers must help students learn to be vigilant about their digital trails online. This conflicts with Ribble (2011), who asserts that internet "users should expect that if they post information to a site … others will enjoy it without vandalizing it, passing it off as their own, or using it as a pretext to threaten or harass" (p. 35). This is a rose-colored glasses approach that masks the reality of the Internet Wild West, and we do students a disservice by teaching them those expectations. Instead, they should expect that there will always be outlaws, just like in the old-fashioned Wild West, who will not abide by common senses of decency and propriety. Thus, students need to exercise awareness about what they share, and they need to take precautions when sharing, such as changing their usernames or even watermarking their photos

and artwork shared online, for example. These are skills that must not be overlooked and undervalued in K-12 education.

A land of misinformation. Not only must we teach students awareness about their digital trail, but we must also help them realize that anyone can post anything to the Internet, regardless of their level of expertise. That means that much of what students find online will be inaccurate, misrepresented, Photoshopped, or otherwise skewed. To help students understand this concept, we could have students watch us publish something online that all students know to be false. Then, they could access the site on their computers or smart phones, thus seeing firsthand that this false information is available to the world. This shows them just how easy it is for anyone to publish falsehoods online. Many people learn this reality in an embarrassing way. For example, one of my uncles reposted a photo of Bill Gates on Facebook. Gates was holding a sign that said something about giving away money to people who reposted the image. My uncle did not realize that the image had been Photoshopped. To help him learn the concept, I replied with a copy of the image — except I had changed the sign in Photoshop so that Gates referred to me by name and said I was awesome. To help students understand this concept as well, teachers can include YouTube videos of Photoshop artists who manipulate such images. It shows students how quickly and easily it can be done. (Modeling videos also show students, particularly girls, how much women's bodies are distorted by the media. I believe this concept should be taught in health or sex education classes beginning at the middle school level.) Teachers can also include current events that include this type of photo manipulation, such as the false Hurricane Sandy photos, many of which went viral via Instagram and Twitter.

Since misinformation abounds, teachers are tasked with helping students learn how to think critically and evaluate sources, particularly on the Internet. Susan Crawford, President

Barack Obama's Special Assistant for Science, Technology, and Innovation Policy, said, “The best software is between the ears” (as cited in Tan, 2011, p. 30-31). How true that is. Many students lack these skills, which Ribble (2011) refers to as “digital literacy” (p. 26). For example, a whole group of seventh graders in Connecticut schools believed a web site about a species of “tree octopus” (Krane, 2006). I presently work within the community college system as a writing tutor, and I continue to see students ages 18 to 30 believe information posted on informal blogs and other unreliable sites. This demonstrates that they lack the evaluation skills necessary to proficiently use the Internet.

To combat this, teachers are tasked with quite a long list of skills to teach, many of which do not fit neatly within particular content areas, such as science or history. Students must learn how to do effective searches online, how to evaluate the credibility of sources, how to track material across the Internet (such as doing a reverse Google image search), and more. I believe that children in the lower grades (K-5) should be directed to specific sites for class projects and should learn the basics of the Internet (domain name extensions, the concept of a URL, etc.), while children at the secondary level should begin learning and practicing search and evaluation skills. Their skills should become more advanced as they progress. However, many adults lack these skills, including teachers. Ribble (2011) states, “Teachers have not had adequate professional development on how to use the technology” (p. 26). For example, many teachers today do not realize that .ORG domain extensions are no longer limited to non-profit organizations. I see many students come into the college system with this misconception. This situation in particular also implies that teachers need to regularly receive technology training as times change so that they are not misinforming their students.

Act in caution. While some false information online will not hurt students beyond a poor grade on an assignment, other falsehoods or misrepresentations put students and adults at risk financially or physically. We have already examined how easy it can be to track people online and to determine their home address using something as simple as a username. When it comes to safety, many adults and students believe they are covered so long as they have installed antivirus software on their computer or other devices. However, they fail to understand that many antivirus software do not catch all viruses and malware, and that antivirus software will not protect them against scams and phishing e-mails. Adults and students alike often do not realize that hyperlinks in e-mails can lead to unanticipated places; this is because they do not understand the nature of html coding, and no one has shown them firsthand how easy it is to write out one URL but yet to link to another. Moreover, many computer users do not know where to look in their browser to identify where a link actually leads. They also don't know how to identify false sites by examining the URLs closely, like this YouTube video demonstrates (The creator does swear at points, so this would unfortunately not be a useful video for K-12 purposes, but it is informative for adults). These are skills that teachers need to help students develop, although it is hard to identify which content area these fit in within secondary education. (The more I study educational technology and the concept of digital citizenship, the more I believe K-12 schools should dedicate a class specifically to technology and critical thinking skills.)

Aside from misleading links, students and adults must also learn how to identify secure sites (https), as well as how to identify rogue "company" e-mails from such corporations as the United States Postal Service, Bank of America, Apple, etcetera. Many fraud artists mimic corporate e-mail messages and construct similar e-mail addresses, which trick readers into following links to mock sites where they willingly put in their username and password. Ribble

(2011) notes that “many … do not know about the hazards of providing sensitive information (such as credit card numbers, bank numbers, or other personal data) to insecure sites” (p. 20).

Sensitive data is not the only area where students and adults should exercise caution, though. They also need to realize that few things are truly free online; most sites have a hidden agenda. We already looked at how sites track users’ data and profit from it — a reality that many people both young and old are not perturbed by. However, many students and adults choose to download “free” icons and wallpaper, games, software, mp3s, or even pornography online. Of course there are ethical concerns with some of these things. Some educators argue that even teenagers “are still developmentally grasping the concepts of right and wrong and understanding the consequences of their behavior” online (Mageau, 2013, p. 3). I disagree. If students have received a moral education from their parents and schools in their K-5 years, then they know that stealing or cheating in any form is wrong, and certainly pornography is always inappropriate for their age group. However, I agree that they do not understand “the consequences of their behavior” — particularly the immediate consequences on their computer, on their digital trail, and in terms of digital law, which we will examine later.

In terms of safety, students must learn that many “free” downloads come with hidden extras. For example, I have a cousin in high school who brought his laptop to me because it had become incredibly slow and unusable. His search history revealed that he had not visited pornography sites but rather had downloaded many rap mp3s from “free” sites across the Internet. When he downloaded these files, he was also unwittingly downloading malware, spyware, and viruses to his computer. He did not recognize symptoms of these either — traits that every student should be taught to at least identify so that they can bring their computer to a specialist to be fixed. While students may not be morally deterred from downloading “free”

movies or mp3s, understanding the digital consequences for their devices may give them more incentive to behave ethically. They will have incentive to protect their property.

Ribble (2011) identifies safety as a facet of "digital citizenship," and he emphasizes that students should take caution to protect their property by also using passwords. Most students and adults understand this basic notion. They equate it with locking their front door, an analogy that Ribble (2011) also makes. However, many students and adults do not understand how to formulate strong passwords. I have witnessed this firsthand within my own extended family, almost half of which have had their Yahoo e-mail addresses compromised. The telltale sign? Sudden spam mail sent from their accounts to everyone in their address book. Most adults have seen it at some point or another. Why does this happen? People have put cheap 25-cent plastic diary locks on their "front doors" rather than a dead bolt; they're using too short, word-based passwords that lack symbols and numbers. Even worse, they use the same password for all their accounts across the Internet. Many also make it easy to break into these accounts by answering security questions that a good searcher could answer using the Internet, such as what their high school mascot was, what their home town was, etcetera.

What do we see as a whole? "In the absence of adult supervision, young people increasingly play with their own safety online" (Tan, 2011, p. 31). I would also argue that even with adult supervision, young people can still be led astray. The Jenkins MacArthur Digital Project found that "most young people are trying to make the right choices in a world that most of us don't fully understand yet, a world where they can't get good advice from the adults around them, where they are moving into new activities that were not part of the life of their parents growing up" (as cited in Tan, 2011, p. 31).

Laws still apply. In the midst of all the misinformation and abundant amount of scam attempts, students may begin to feel that the Internet is truly a Wild West with no sense of order. However, they must learn that the same laws that govern our day-to-day society also apply for Americans using the Internet within the United States. Ribble (2011) refers to this concept as "digital law" (p. 31). In my own experience, I did not learn much about law within my K-12 education beyond the basics: Murder, robbery, rape, and so forth are illegal and may result in jail time. Many students may understand these concepts when they study current events in their K-5 years or in their later history courses. Today's media centered lifestyles reveal many students' ignorance around public law. This can especially be seen with "sexting," which many students do not realize constitutes child pornography (Ribble, 2011, p. 32). Many students also do not realize that hacking information online is akin to breaking into someone's house (Ribble, 2011, p. 32). Often students have not heard of the terms libel or slander, either. For decades students have engaged in name calling on the playground, but with digital media, they can suddenly find themselves being perpetrators of libel. If they post online that a classmate is a "slut," for example, they could actually face legal repercussions. The deeper implication is that students need a more solid education in these issues, as well as in the concept of "free speech" within America. History classes seem like a prime candidate for teaching these concepts.

Students also have a skewed sense of ownership. "For young people today, 'sharing information is so natural and so often encouraged that the lines that were once so bright and clear are blurring" (Mageau, 2013, p. 3). The Internet is obviously one of the causes of this misperception. Sites like Tumblr and Pinterest encourage users to take and share freely, and some students start to perceive the Internet as a kind of free-for-all. In the article "Rethinking Plagiarism in the Digital Age," authors Evering and Moorman (2012) cite a study showing that

"because there are so many ways to access information and often multiple authors of that information, lines of ownership are blurred" (p. 37). They also assert:

> Students often have experience using search engines, social media, and multimedia tools such as digital and video cameras outside of academic environments. However, these digital literacy experiences are unlikely to include the skills, knowledge, and expertise necessary to locate, navigate, and evaluate information in an ethical manner (as cited in Evering & Moorman, 2012, p. 37).

The authors ultimately claim that K-12 and college teachers must begin teaching students these skills in order to make a difference (Evering & Moorman, 2012, p. 37).

Anonymity makes communication harder. Students may struggle to understand concepts of digital law, digital safety, and the digital trail because of one alarming aspect of the Internet: the concept of anonymity. Students who do not exercise digital safety and monitor their digital trail mistakenly believe they are anonymous when they are not. Their usernames and IP addresses give them away. Others have mastered these techniques but use their anonymity online to behave unethically and/or unkindly. "The alluring option of anonymity can blur one's perception of cause and effect, action and consequence — especially among the young" (Orth & Chen, 2013, p. 58). Ultimately, there is something about being behind a screen that makes even kind, moral people sometimes behave in uncharacteristic ways. This can be seen with aggressive driving as well. Research finds that "drivers placed in an anonymous setting are more likely to engage in aggressive driving behavior" (as cited in Ayar, 2006, p. 131). Ribble (2011) categorizes the concept of digital behavior under "digital etiquette" (p. 29), but I have a different perspective. Just like ethics, etiquette is something routinely taught by parents and schools in the early grades, and students should be expected to transfer these skills. The problem, then, is

something deeper, and in this case I believe anonymity and communication are at the heart of the problem.

To help students communicate better digitally, teachers must help students learn about the nature of communication — a skill that is sadly already under taught. Public K-12 schools do not often explicitly teach students about verbal and nonverbal communication skills. They also often do not teach students how to assert themselves and their feelings rather than to act aggressively or submissively in communication; nor do they teach students how to practice the art of reflective listening. (Both skill sets are discussed in the novel *People Skills* by Robert Bolton). In group work situations, many teachers just expect students to get along and work cohesively even though they have not been taught anything about group dynamics or teamwork. In digital text exchanges, students can really be at a loss because two key components of communication are suddenly absent: tone (paralanguage) and body language. Research shows that these two components of communication impart more meaning than the words themselves (as cited in Putnam, n.d.). This means that many students will misinterpret others online or else be misinterpreted. Students need to deeply understand all of these concepts so that they can moderate their own reactions on digital devices and also carefully craft their messages, regardless of whether it is a text to a friend or an e-mail to a potential employer.

Not everyone has access. Finally, adults and youth alike should remember that not all people have an equal amount of, or even any, access to read the Internet (Ribble, 2011, p. 16) and, just as important, to generate content on the Internet (Means, Bakia, & Murphy, 2014, p. 95). Even though minorities within the United States continue to gain more access to the Internet through smart phones, these devices “appear to be more suited to information access and social interactions than to supporting complex learning interactions and content creation”

(Means, Bakia, & Murphy, 2014, p. 95). We begin to see that in spite of increased access, "the digital divide is growing, not shrinking, because those with greater literacy skills and more access to supports for learning how to use new technologies are obtaining larger and larger learning benefits not available to people of limited means" (Means, Bakia, & Murphy, 2014, p. 96).

This problem around digital access could be taught alongside any lesson about inequality and its effects within our nation or around the world. As teachers, this means we should be mindful about how we deliver material to our students and how much access we create for them within the school setting. Some critical theory attacks how many educators misappropriate technology usage within their classrooms:

> Teachers, while concerned about equity, held attitudes which hindered access: They believed that better behaved students deserved computer time and that the primary benefit of computers for low-achieving students was mastery of basic skills. ... Thus, children who were minority, poor, female, or low achieving were likely to be further behind after the introduction of computers in schools (as cited in The Association for Educational Communications and Technology, 2001).

If students do not receive access to technology and especially education in digital skills, we set them up for failure in a world that increasingly requires these traits for well-paying employment. This also means that school administrators should require students in K-12 to take typing classes and/or demonstrate typing proficiency, because their ability to type affects their level and speed of access, as well as their likelihood of being hired in many industries.

In summation, we can see that K-12 teachers must help students fully understand certain facets of the Internet and of digital technology in general. We must help our students learn six

vital components: the digital trail, the land of misinformation, the importance of acting in caution, the laws still apply, anonymity makes communication harder, and not everyone has access. Ribble (2011) identified nine facets of digital citizenship, but I believe these six concepts cover the concerns he addressed and frame them in a different direction. I realize my synopsis may have a negative, almost fearful, slant, but it is because I believe students need to fully understand what they are up against with technology and modern concepts of privacy. I embrace technology and believe it can increase our quality of life and improve knowledge distribution within society, but I also realize it comes at a price and with certain dangers, which all users must understand.

References

The Association for Educational Communications and Technology (2001, August 3). Topics in critical theory of educational technology. Retrieved from http://www.aect.org/edtech/ed1/09/09-07.html

Ayar, A. A. (2006). Road rage: recognizing a psychological disorder. *Journal of Psychiatry & Law*, 34(2), 123-150. Retrieved from http://ebscohost.com

Evering, L. C., & Moorman, G. (2012). Rethinking plagiarism in the digital Age. *Journal of Adolescent & Adult Literacy*, 56(1), 35-44. doi:10.1002/JAAL.00100

Fredrick, K. (2013). Fostering digital citizenship. *School Library Monthly*, 29(4), 20-21. Retrieved from http://ebscohost.com

Gardner, J. (2013, December 8). Why America's kids need a national digital citizenship curriculum. *Venture Beat*. Retrieved from http://venturebeat.com/2013/12/08/why-americas-kids-need-a-national-digital-citizenship-curriculum/

Greenhow, C. (2010). A new concept of citizenship for the digital age. *Learning and Leading with Technology*. 37(6). 24-25. Retrieved from http://ebscohost.com

Krane, Beth. (2006). Researchers find kids need better online academic skills. Retrieved from http://advance.uconn.edu/2006/061113/06111308.htm

Mageau, T. (2013). Teaching digital responsibility. *T H E Journal*, 40(8), 3. Retrieved from http://ebscohost.com

Means, B., Bakia, M., & Murphy, R. (2014). Learning online: What research tells us about whether, when and how. New York: Taylor & Francis.

Moreillon, J. (2013). Leadership: Teaching digital citizenship. *School Library Monthly*, 30(1), 26-27. Retrieved from http://ebscohost.com

Orth, D., & Chen, E. (2013). The strategy for digital citizenship. *Independent School*, 72(4), 56-63. Retrieved from http://ebscohost.com

Putnam, M. (n.d.). Nonverbal communication: Chapter 7. Retrieved from http://www.uta.edu/faculty/mputnam/COMS3312/Notes/Ch7.html

Ribble, M. (2011). The nine elements of digital citizenship. In *Digital citizenship in schools* (chapter 2). Retrieved from http://www.iste.org/docs/excerpts/DIGCI2-excerpt.pdf

Tan, T. (2011). Educating digital citizens. *Leadership*, 41(1), 30-32. Retrieved from http://ebscohost.com