FDLA Journal

Volume 6 *Winter 2021* Article 3

December 2021

Maintaining Privacy and Security in Cyberspace: What Everyone Needs to Know

Maureen McDermott
Nova Southeastern University, mmcdermo@nova.edu

Jennifer L. Reeves
Nova Southeastern University, jennreev@nova.edu

Gabriela Mendez
Nova Southeastern University, gmendez@nova.edu

Berta Hayes Capo
Nova Southeastern University, cberta@nova.edu

Jason Karp
University of North Carolina at Charlotte, Jkarp3@uncc.edu

Maintaining Privacy and Security in Cyberspace:

What Everyone Needs to Know

Maureen McDermott, Ed.D., Nova Southeastern University
Jennifer Reeves, Ph.D., Nova Southeastern University
Gabriela Mendez, Ph.D., Nova Southeastern University
Berta Capo, Ed.D, Nova Southeastern University
Jason Karp, Ed.D., University of North Carolina at Charlotte

Introduction

You've been hacked!

This cataclysmic message heralded from cyberspace incites panic in the minds and wallets of people around the world. These ubiquitous data breaches occur frequently to seemingly innocuous targets. A breach occurs when a cyber-hacker physically gains access to files on a computer or remotely bypasses a network's security system, gaining access to data, and stealing sensitive information. Remote network security breaches are a common method for taking sensitive information from companies. The confidential information can then be sold on the Deep Web Market, used to steal identities to open up fake credit card accounts, or to blackmail an individual or group (TrendMicro, 2018).

The first data breach of 2019 was reported fewer than 24 hours into the new year (Targett, 2019). Large corporations dominate the news concerning incurred security breaches that expose customers' personal details and financial resources. Recent examples (Targett, 2019) include Facebook (up to two billion accounts compromised), the Marriott Hotel chain (over 500 million accounts hacked), and Under Armour (about 150 million accounts jeopardized). Additionally, Equifax, one of three major credit reporting agencies whose databases contain susceptible personal information such as Social Security numbers, dates of birth, addresses, etc., was hacked in 2017. The breach affected 143 million U.S. consumers and extended to the U.K. with 400,000 U.K. customers affected (TrendMicro, 2018). Quite possibly the largest data breach of all time occurred in January 2019 involving a collection of 773 million unique emails and 21,222,975 unique passwords from thousands of different users onto the deep web (Davis, 2019).

This episodic hacking obliges users to be habitually cognizant that their financial information is vulnerable and could end up being shared with unintended recipients. Future breaches are predicted to be even more creative and impactful, focusing in on biometrics, mobile phones, cloud based storage, and gamers (Bayern, 2018). *Forbes*

contributor Kyle Torpey (2019) attributes this seemingly endless cycle of data breaches to the consumer's desire for convenience overriding concerns about security and the willingness of malicious hackers who wait for these opportunities.

Data Breaches Before the Internet

Data breaches are not a new phenomenon; breaches of paper records in the United States have been traced back almost 70 years. According to Solove (2004), most centralized record keeping at the national level in the United States was done on paper for the Census. In the 1950s, the Social Security Administration of the U.S. government assigned citizens nine digit numbers and required stringent reporting and record keeping of income. Records were computerized and stored in huge databases, and SSNs eventually became useful identifiers in the private sector (e.g., by banks and credit card companies) and as student numbers for colleges and universities.

In the 1970s, the U.S. government began selling batches of Census data containing physical addresses stored on magnetic tapes to marketing companies, but names were excluded to protect privacy (Solove, 2004). This trend of *number instead of name* was the genesis of identity theft thus compromising the "digital dossier" in the early 1980s. However, the invasion of the digital dossier did not pervade tech jargon rapidly. It re-emerged as "digital footprint" during the time when the term "carbon footprint" pervaded mass media. In the mid-1990s, commercial companies and private individuals transformed websites into cyberspace shopping experiences, thus opening the Internet information superhighway for business and cybercrime (Sommer, 1998).

Breaching Education

With the recent revelations of breaches involving social media applications, privacy and security concerns have emerged for administrators, faculty, staff, students, and parents. Academia is far from safe as there has been noted cases of hacking and data loss. In March of 2019, private colleges Grinnell, Hamilton, and Oberlin reported breaches (Smith, 2019). Grinnell and Hamilton reported that applicants received emails from someone who claimed to have unauthorized access to their databases containing personally identifiable information. These emails, which came from official college addresses, offered to sell students their completed admission file that included comments from admissions officers and tentative decisions (Smith, 2019).
A spokesperson from Oberlin said their applicants and students who enrolled during or after the fall of 2014 did not receive emails like the ones at Grinnell and Hamilton; however, their names, addresses, birthdays, emails, and Social Security numbers were possibly exposed. Oberlin suggested that fraud alerts should be added to victim's credit card reports. All three colleges used software system Slate to manage this information, and all three colleges reported this breach to Slate and the Federal Bureau of Investigation (Smith, 2019).

In 2010, the social security numbers of 43,000 Yale affiliates became publicly available on Google because they had been stored on servers that were also used to hold open-source materials (Fuchs, 2018). In July 2018, Yale notified about 119,000 faculty, staff, and alumni that their names and social security numbers had been compromised between the years of 2008 and 2009. This breach also compromised some of the victims' dates of birth, physical addresses, and email addresses. The breach occurred in September 2011 when the university was clearing out unnecessary personal data, and was not discovered by Yale until June, 2018. Yale offered to pay expenses for 12 months of identity monitoring services for victims of both breaches (Fuchs, 2018). According to Mariwala and McCooey (2018), two class action lawsuits have been filed against Yale alleging negligence, unfair trade practices, and reckless, wanton, and willful misconduct. Plaintiffs are requesting further compensatory and punitive damages.

Data breaches have also invaded the privacy of students in PK-12 school districts. The San Diego School District reported a large data breach where data including Social Security numbers from as many as 500,000 students were compromised and possibly stolen (Luke, & Stuckney, 2018). The Hoopeston (IL) Area School District's website was compromised when families received repeated false and outrageous voicemail messages at 3am. No student data was taken; however, this demonstrates the vulnerability that exists in the age of technology (Francis, 2018).

Even though parents may be able to monitor what educational apps their children use at home, they have little input about what happens at school. The Electronic Freedom Foundation, a non-profit organization that defends digital privacy, free speech, and innovation, identified school-issued devices and ed tech platforms as the most vulnerable for data breaches. For these reasons, parents should be asked for consent or given the option to opt-out of education technology.

On December 1, 2015, the EFF filed a lawsuit against Google for data mining student's personal information and internet search histories in Google Apps for Education (GAFE) and Google Chromebook (Alim, Cardozo, Gebhart, Gullo, & Kalia, 2017). Between Dec. 15, 2015 and January 2017, the EFF posted a survey about student privacy on their website and disseminated links on their other social media sources. Over 1,000 responses from students, parents, teachers, and administrators were compiled into the report "Spying on Students" (Alim et al., 2017). It raised concerns about technology usage that tracks online student's behavior before they are old enough to understand the implications of digital footprints, privacy, and security and addressed issues of federal law, state law, and industry self-regulation.

One legal measure is the federal law Children's Online Privacy Protection Act (COPPA) that requires technology providers to acquire parental consent before collecting student's personal information. Enforced by the Federal Trade Commission (FTC), this law includes consent requirements for technology providers that are utilizing student data for anything other than disclosed to the school district. Verifiable parental consent is required for any collection of identifiable student information for students younger than 13. The

FTC also offers a Student Privacy Pledge voluntarily signed by ed tech companies, but the EFF identified glaring loopholes in what constitutes student information.

Developing Digital Citizens

Resulting from increased technology integration in brick and mortar classrooms and the pervasiveness of distance education, the International Society for Technology in Education (ISTE) asserts that educators who use applications to engage students must "Model and promote management of personal data and digital identity and protect student data privacy" (ISTE Standards for Education, 2017, para. 3). ISTE (2019) encourages the development of digital citizens who critically evaluate online information and create positive online footprints.

Ironically, while digital citizens harness technology for the benefit of communities, hackers simultaneously undermine these efforts for their own selfish gains. These violations demonstrate the need for curricular work and professional development for faculty and staff (with support from the administration) in the areas of digital footprints and evaluation of websites for security and privacy.

Digital Footprints Defined

According to Dennen (2015), digital footprints can be likened to physical footprints rendered unique to their owners, and contain the information users leave behind on the Internet resulting from online activity. There are two kinds of digital footprints – active and passive. A passive digital footprint is a data trail users unintentionally leave online. When connecting to the Internet, websites detect IP addresses and locations and download cookies, and search engines save user's histories automatically with no detection. In the past few years, many websites have eliminated this potential for passive footprints by adding pop-up boxes that ask users to read the terms of service and acknowledge agreement by simply checking a box before entering the site (McDermott, 2018).

Active footprints, on the other hand, refer to the data trail users know they are leaving – including signing into social media sites such as Facebook, YouTube, Twitter, Pinterest, Instagram, Snapchat, and various educational learning management systems such as Google classroom, Canvas, and Blackboard. Even "liking" pages, posts, or photos on social media or commenting with an icon to a classmate's discussion board posting contributes to a user's digital footprint.

These active footprints generate when users retrieve email for work and school, as well as when accessing company websites and learning management systems. Regardless of whether digital footprints are active or passive, privacy and security are areas for concern. Although privacy and security are not synonymous, what they have in common is that people do not usually know there is a problem until it has happened already and is broadcast over the news (McDermott, Reeves, Capo, Mendez, & Karp, 2019). Security

from data hackers is not guaranteed even when users select the most stringent privacy options involving how their data is displayed, stored, used, and shared. Security involves how companies protect information users agree to share, so when something is hacked both security and privacy are compromised.

Evaluating Security

Before generating digital footprints, consumers and educators should understand a company's security policy. According to Smith (2018), one of the strongest security indicators of a website is the first few letters on the browser address bar. Early website addresses started with HyperText Transfer Protocol (HTTP), the procedure that allowed network administrators to share information. Unfortunately, intercepting the information was almost as simple as it was to share it, so an encryption encoding system was developed called HyperText Transfer Protocol Secure (HTTPS). Computers using HTTPS send and receive messages through the Secure Sockets Layer (SSL) or the Transport Layer Security (TLS) protocol that validates security certificates (Sheldon, 2017).

Both Sheldon (2017) and Smith (2018) recommend consumers verify five important things prior to its use: (a) authentication and authorization with multi-factor identification, (b) strong passwords that contain at least one uppercase letter and a numerical character, (c) email confirmation when an account is opened, (d) frequent password changes, and (e) sign-in requirements for each session.

In addition to the steps above, consumers should also check Breach Level Index (BLI) that is a dynamic website that invites users from around the world to report/document security breaches. An analysis of data breaches by type was documented from spring 2013 through 2018. Identity theft has topped the number of breach incidents since 2013. In 2018, there were 957 incidents of identity theft, followed by approximately 212 incidents of Financial Access breaches and 211 incidences of Account Access breaches (Data breach statistics, 2019). Malicious outsiders were responsible for more than half of all breaches in 2018, followed by accidental loss. When looking at the loss by industry, social media accounts for more than half of the industry breaches in 2018 with 2,739,445,349 records stolen (Data breach statistics, 2019). Breach Line reported that education had the second lowest number of data breaches at 0.27%; however, this still includes 12,984,701 compromised records in 2018 alone!

Sheldon (2017) reports that the highest threats to mobile app security come from broken cryptography, unintended data leakage, weak server side controls, client side injection, and poor authorization and authentication. Smith (2018) suggests making good choices in regards to safety such as not disclosing too much online, not accepting friend requests or personal messages from strangers, and blocking people who write or display inappropriate things.

When evaluating for security, users should investigate if websites scan for robots. There are many types of "bots" which scan websites that save the contents of every page in the search index. Bots can also be detected when users share networks with others on proxy services, work or school networks, VPNs, and websites such as Amazon, EC2, and Google App Engine. Chat bots monitor for appropriate language and "chatterbots" respond to messages appearing to be an actual person. However, some bots contain malware that raid email address books to link them to spam mailing lists. Other bots raid entire computer systems, duplicate content, and then infect them with viruses (Christensson, 2014).

The security section from Pinterest (We protected your account, 2019) is a good example of some security concepts users should know. It advises users to save Pins from original sources, and use full links instead of using a redirect like bit.ly or other link shorteners. Pinterest's security features enable account blocking when it detects a bot or if users do one or any of the following: log in frequently, comment or save Pins quickly, and follow several people rapidly.

Additionally, Pinterest's first requirement compels users to verify they are at least 13. Other security tips (from their website) include activating two-factor authentication, connecting the account to Google or Facebook, verifying current email, and changing passwords regularly. Pinterest also retains the rights to suspend accounts if they believe users have violated the website's Acceptable Use Policy. Pinterest also has a user-friendly contact page if users have been blocked and not restored within 24 hours.

Evaluating Privacy Policies

Before generating digital footprints, users should also be aware of a company's privacy policies to protect personal information and learn how the company uses the data it collects (McDermott, 2018). The privacy statement should be dated and current, address how users communicate with each other, what details users can see about each other, and if data will be shared with third parties.

Typically, school districts and universities evaluate applications, programs, and software endorsed for educational use. However, this is not always the case. Everyone, in particular parents and educators, need to understand how to evaluate the privacy and security of apps and websites. Fortunately, there are resources educators can use to address this task.

One useful tool to evaluate privacy policies and practices is Haimson's (2017) list of 20 questions individuals should use to evaluate companies' privacy policies regarding personal data. The questions address numerous topics such as definition of terms to examining data sharing practices and individuals' rights and legal recourse. They also recommend inquiring about companies with which personal data will be shared, whether these companies are prevented from using advertising or selling data, and the reasons for disclaimers of liability.

The Education Privacy Resource Center of FERPA/SHERPA (2019) offers recommendations for using applications in the classroom. This set of best privacy practices recommends using products and apps approved by the school district, given that school districts need to evaluate the tools for privacy and security prior to adoption. FERPA/SHERPA also includes a list of 10 questions to help individuals evaluate whether apps and other online products protect students' information. The questions focus on the collection of personally identifiable data, vendor's commitment not to share information, the inclusion of advertisements within the learning product, and claims regarding change of privacy policies.

FERPA/SHERPA (2019) also recommends websites that can be used to evaluate company privacy policies. One designated as very useful is commonsense.org, developed by Common Sense, a nonprofit organization dedicated to making the technological world a better place for kids. Commonsense.org, has three main areas: (a) a Parent portal with a plethora of information about current technology and popular apps, movies, books, games and TV shows; (b) an Educator portal with lessons, games, and resources on digital citizenship; and EdTech reviews, videos, and privacy evaluations; and (c) an Advocacy area for those wanting to help keep our children safe.

Common Sense determines some of its recommendations based on App Triage, a detailed privacy evaluation workflow (Fitzgerald, 2016). Staff members review the privacy terms present, create sample accounts, use app data to verify privacy information provided, and verify that terms of privacy and service policies are linked correctly when users are logged in. They also evaluate social app sharing policies by testing them from accounts created. When evaluating websites termed "https" the staff verifies the same site cannot be found with just "http." Fitzgerald said the information is freely available and can be used by anyone. However, these steps are time-consuming and the policies are difficult to read. Therefore, Common Sense compiled an easily searchable database of app evaluations. Since policies change over time (Kelly, 2019), Common Sense developed a tool which uses an open source software (named *Wdiff*) into its policy annotator to scan the policies and determine the actual policy changes. Then they update the original app's policy evaluation in the database (Kelly, 2019).

In order to use this evaluation tool, users simply enter the name of the app, game, or website in the search area at https://privacy.commonsense.org/ and click enter. The results provide a synthesis of the evaluation that includes a recommendation for use (i.e., *use responsibly*, *use with caution*, *not recommended*); an overall score of the app (ranging from 0 to 100 and based on answers to the Common Sense's evaluation questions); whether advertising is displayed; and whether the company sells or rents data to third parties, shares data for advertising or marketing, uses data to target advertisements, or allows third parties to use the data for advertising (Common Sense, 2019). Figure 1 presents the privacy evaluation of ABCmouse.com, which has a *use responsibly* recommendation. In contrast, Figure 2 illustrates the privacy evaluation of Pinterest, which has a *use with caution* recommendation due to a number of privacy concerns.

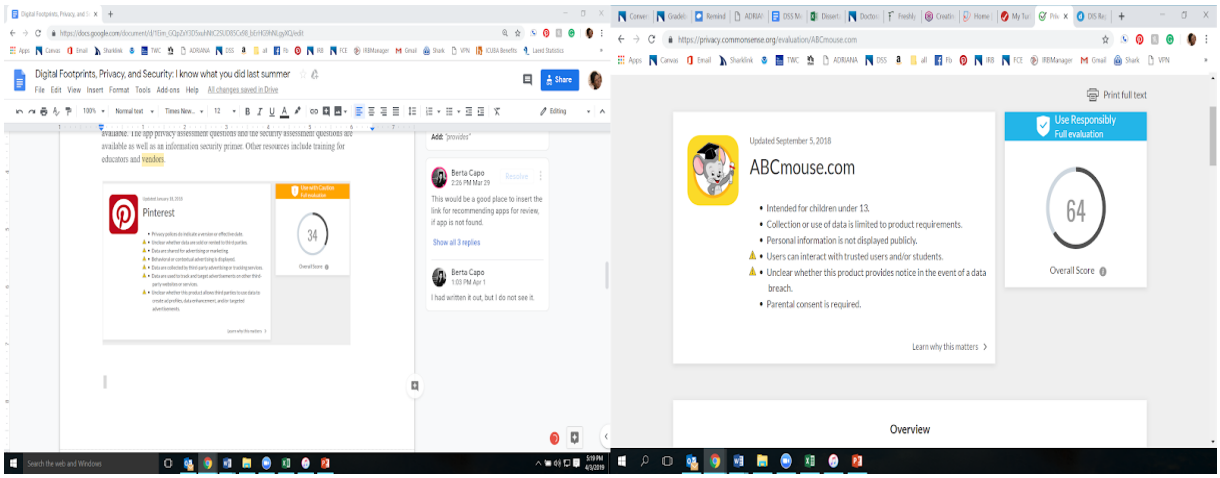

Figure 1. Privacy Evaluation for ABC Mouse. Reprinted with permission from Common Sense.

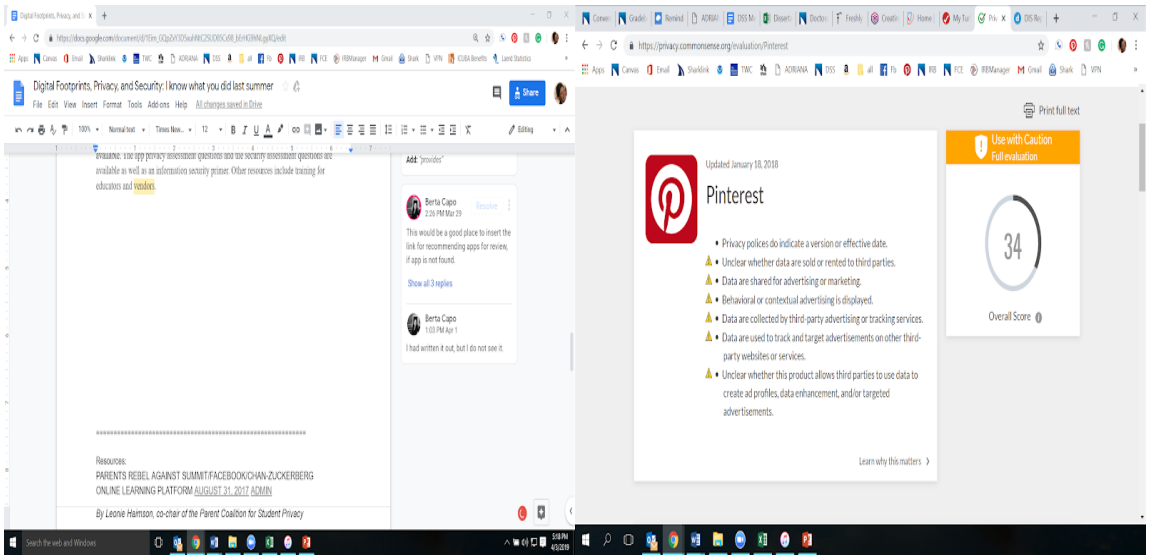

Figure 2. Privacy Evaluation for Pinterest. Reprinted with permission from Common Sense.

Additionally, the evaluation provides an overview of the app and a detailed privacy report, with scores for safety, privacy, security, and compliance with federal laws. Users can see the full privacy report, as well as read Common Sense's EdTech review (see Figure 3) with pros, cons, teaching tips, and teacher reviews. For Pinterest, although Common Sense recommends caution when using the app due to privacy concerns, they give it 4 out of 5 stars for high engagement, pedagogy, search features, and the simple layout. Teachers also give it 4 out of 5 stars; according to one teacher, "I love Pinterest…[it] is so helpful [for finding] so many wonderful lessons, crafts, and activities…that go with what you are teaching."

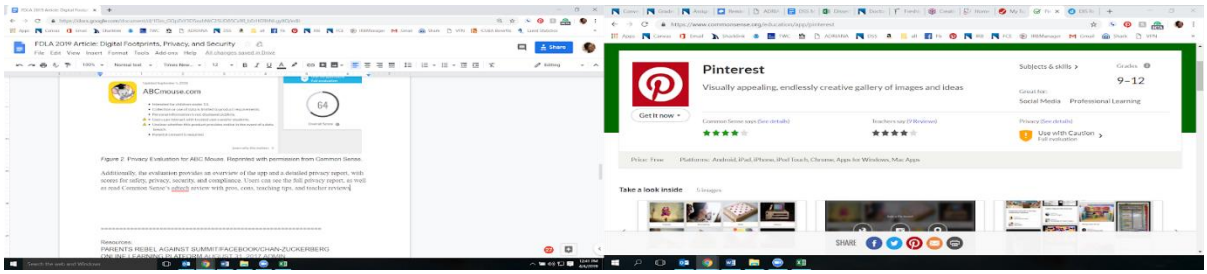

Figure 3. EdTech review of Pinterest. Reprinted with permission from Common Sense.

Conclusion

Parents, university/college personnel, teachers and other adults working in the K-12 systems are held accountable to higher standards when determining levels of technology infusion. In today's digital world, they are obligated to have more than just a basic understanding of digital footprints, privacy, and security. They need a survival tool kit! Parents need to be aware of these risks when monitoring children's screen time at home and determining choices (when possible) about technology used at school. Students need to know what happens to their information when they click on something and leave a digital footprint. As we rapidly move further into this digital reality, educators, parents, and students alike must learn to utilize online space for respectfully interacting with others and furthermore, to include those with differing beliefs (ISTE 2019).

The growth of educational technology will always outpace legal and ethical understanding concerning digital footprints, privacy and security; therefore, the implications seem insurmountable. Ironically, one of the best ways to stay ahead of the curve is to educate oneself by reviewing the non-profit websites developed by ISTE, Common Sense, and EFF. These websites provide digital tips for adult usage as well as parental guidance for minors. The websites also advocate professional development for teachers and offer online training modules, but it is up to the administration to provide professional development time.

Developing digital citizenship through this type of education has the capacity to empower everyone to avoid unnecessary risks concerning digital footprints, privacy, and security. However, the risks are too high to leave the solution to isolated individuals. Consistent review of these non-profit websites and other resources should be a part of multiple strategies implemented. Schools need an organized approach to include not only professional development, but also a curriculum that integrates digital citizenship as necessary knowledge that is essential for digital literacy skills. Developing digital citizenship is a complex task that requires collaborative efforts from all stakeholders including students, parents, teachers, administrators, and everyone employed at school districts and institutions of higher learning.

References

Alim, F., Cardozo, N., Gebhart, G. Gullo, K., & Kalia, A. (2017 April 13). Spying on students: school issued devices and student privacy.
Retrieved from https://www.eff.org/wp/school-issued-devices-and-student-privacy

Bayern, M. (2018, December 3). 5 major data breach predictions for 2019.
Retrieved from https://www.techrepublic.com/article/5-major-data-breach-predictions-for-2019/

Christensson, P. (2014, February 14). *Bot Definition*. Retrieved from https://techterms.com

Common Sense. (2019). https://commonsense.org/

Data breach statistics. (2019). Retrieved from https://breachlevelindex.com/

Davis, J. (2019, January 23). Massive data breach exposes 773 million emails, 21 million passwords. Retrieved from https://securitytoday.com/articles/2019/01/23/massive-data-breach-exposes-773-million-emails-21-million-passwords.aspx

Dennen, V.P. (2015). Technology transience and learner data: Shifting notions of privacy in online learning. The Quarterly Review of Distance Education, 16(2), 45-49.

FERPA I SHERPA. (2019). Best privacy practices for using apps in the classroom.
Retrieved from https://ferpasherpa.org/educators/using-apps-in-the-classroom/

Fitzgerald, B. (2016, July 20). Evaluating apps, step by step. Retrieved from https://www.commonsense.org/education/privacy/blog/evaluating-apps-step%20-by-step

Francis, J. (2018, September 3). Hoopeston Area School District hacked. Retrieved from https://foxillinois.com/news/local/hoopeston-school-district-hacked

Fuchs, H. (2018, August 2). A decade later, Yale discovers major data breach. Retrieved from https://yaledailynews.com/blog/2018/08/02/a-decade-later-yale-discovers-major-data-breach/

Haimson, L. (2017, August 31). Parents rebel against Summit/Facebook/Chan-Zuckerberg online learning platform. Retrieved from https://www.studentprivacymatters.org/parents-rebel-against-summitfacebookchan-zuckerberg-online-learning-platform/

ISTE (2019). Digital citizenship in education. Retrieved from https://www.iste.org/learn/digital-citizenship

ISTE Standards for Education, (2017). Retrieved from https://www.iste.org/standards

Kelly, G. (2019, April 11). Our privacy evaluation process keeps track of policy changes so you do not have to. Retrieved from https://www.commonsense.org/education/articles/how-we-keep-track-of-privacy-policy-changes

Luke, S. & Stuckney, R. (2018, December 21). Data breach might impact 500,000 San Diego Unified School District students, former Students, and some staff. Retrieved from https://www.databreaches.net/data-breach-might-impact-500000-san-diego-unified-school-district-students-former-students-and-some-staff/

Mariwala, J., & McCooey, S. (2018 October 22). Second data breach lawsuit filed against Yale. Retrieved from https://yaledailynews.com/blog/2018/10/22/second-data-breach-lawsuit-filed-against-yale/

McDermott, M. (2018). Digital footprints: Creation, implication, and higher education. *Distance Learning, 15* (1), 51-54.

McDermott, M., Reeves, J.L, Capo, B., Mendez, G., & Karp, J. (January, 2019). Digital footprints, privacy, and security: I know what you did last summer! Presentation at the meeting of the Florida Distance Learning Association, Orlando, FL.

Pinterest. (2019). We protected your account. Retrieved from https://help.pinterest.com/en/article/we-protected-your-account

Sheldon, R. (2017 December). A mobile app security checklist for developers. Retrieved from https://searchmobilecomputing.techtarget.com/tip/A-mobile-app-security-checklist-for-developers

Smith, M. (March 8, 2019). Hackers breach admissions files at three private colleges. Retrieved from https://www.washingtonpost.com/education/2019/03/08/hackers-breach-admissions-files-three-private-colleges/?noredirect=on&utm_term=.0e6a01bd781e

Smith, P. (2018, March 6). The Definitive Guide to Simple Internet Privacy and Security. Retrieved from https://staysafeonline.org/blog/definitive-guide-simple-internet-privacy-security/

Solove, D.J. (2004). *The digital person: Technology and privacy in the Information age.* New York University Press. New York, NY. Full e-book retrieved from https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications

Sommer, P. (1998). Digital footprints: Assessing computer evidence. Retrieved from http://www.pmsommer.com/CrimLR01.PDF

Targett, E. (2019, January 2). *2019's First Data Breach: It Took Less than 24 Hours.* Retrieved from https://www.cbronline.com/news/2019s-first-data-breach

Torpey, K. (2019, February 28). If you don't care about online privacy, you should read this. Retrieved from https://www.forbes.com/sites/ktorpey/2019/02/28/if-you-dont-care-about-online-privacy-you-should-read-this/#d0ee3a3886c7

TrendMicro: Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes. (2018, August 10). Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

Figures

Figure 1. Privacy Evaluation for ABC Mouse. Reprinted from Common Sense, retrieved from https://privacy.commonsense.org/evaluation/ABCmouse.com Copyright 2019.

Figure 2. Privacy Evaluation for Pinterest. Reprinted from Common Sense, retrieved from https://privacy.commonsense.org/evaluation/Pinterest Copyright 2019.

Figure 3. EdTech review of Pinterest. Reprinted with permission from Common Sense, retrieved from https://www.commonsense.org/education/app/pinterest Copyright 2019.