Understanding Student Privacy in K-12 Technology Post COVID-19

KATIE SHUCK, PH.D. CYBER DEFENSE CANDIDATE

March 2022

ABSTRACT

This research continues prior work conducted by the researcher to explore data privacy and data collection methods within the K-12 education environment. This research specifically explores data privacy and collection in four technologies that have become commonplace in K-12 classrooms within the United States throughout distance and remote learning due to COVID-19. The research compares keywords for data collection practices found in the technologies' privacy policies with current data privacy laws and regulations regarding educational records and privacy for minor children. The results show data collection practices that potentially impact privacy for students and K-12 classrooms of which schools, administrators, teachers, and parents should be aware.

BACKGROUND

Prior to COVID-19, numerous K-12 classrooms across the U.S. were adopting technology as a way to create engaging and effective learning environments for young students. However, at the start of the pandemic, the integration of educational technology became a priority and drastically increased as students transitioned from in-person to virtual and/or distance learning. Schools, administrators, and teachers sought out quick solutions to enable continuous teaching and learning. Schools applied for grants that allowed them to purchase laptops so that every student would be able to access the classroom. Yet, as classrooms adapted to keep students healthy during the pandemic, privacy of the students was not always a consideration. In fact, schools and teachers began to seek out greater ways to perform learning analysis through all of the newly available data from the education technology in order to better understand how students were adapting to learning during COVID-19 [1]. Furthermore, cyber incidents and attacks against education increased. This was especially realized as students fell victim to privacy harms through incidents of Zoom bombing and online classroom hijacking, malware and ransomware attacks on schools more directly impacted learning if students were unable to access school resources, and greater data collection of students' data – both personally identifiable information (PII) and educational records [2],[3].

This research study looks at four categories of technologies: (1) eLearning Management, (2) Video-Assisted Learning, (3) Technology Management, and (4) Gamification – with one specific technology chosen in each category – and the data collection practices as listed in their privacy policies. The goal of this study is to better understand data collection practices of technology targeting young students and, ultimately, students' privacy. The study does not seek to judge the specific technologies, but rather assess practices which may impact student privacy.

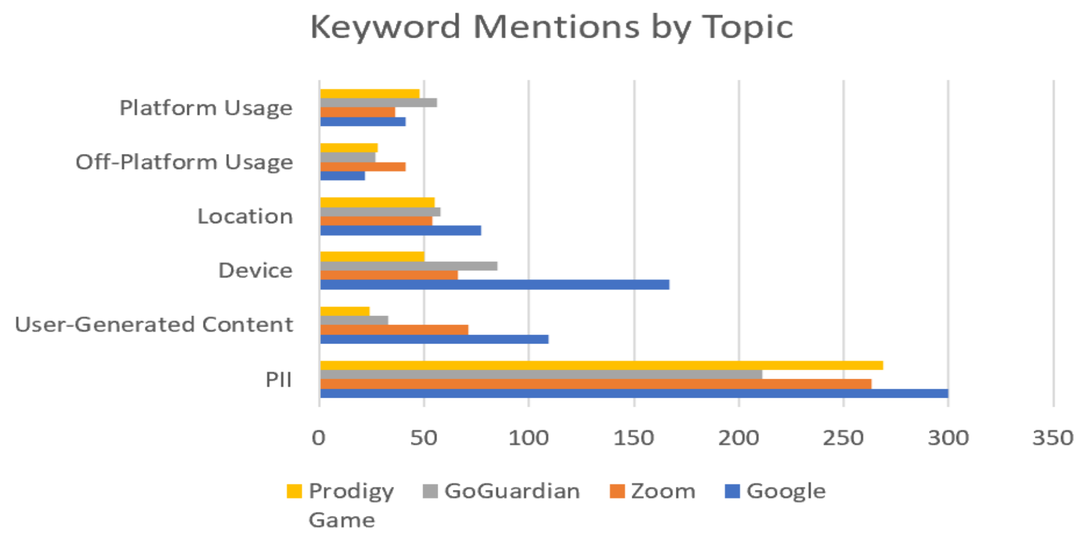
METHODOLOGY

This project used quantitative contextual analysis of PII through topic modeling and keyword analysis that identified and classified language in privacy policies [4],[5].

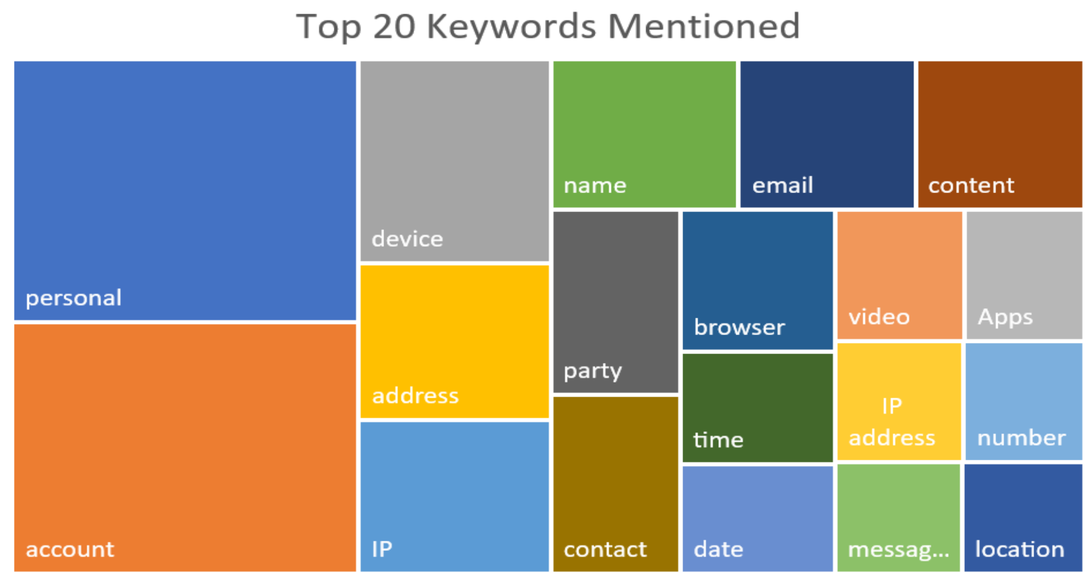
Definitions of personal information from current federal legislation of the Children's Online Privacy Protection Act (COPPA) [6] and Family Educational Records and Privacy Act (FERPA) [7] were used to conduct keyword analysis.

Topics Identified	Seed keywords
Personally identifiable information	Personal, identifiable, telephone, number, phone, telephone number, phone number, mobile, cellular, mobile number, cellular number, IP address, IP, email, email address, name, first name, last name, surname, date of birth, birthday, age, grade, account, location, username, password, contact, zip code, postal code, mailing address, street address, address, city, state, country
User-generated content	user-generated, content, chat, text, chat messages, text messages, images, video, audio, messages, emails, document, assignment, create, photos, docs, spreadsheets
Device information	IP address, IP, device, device information, MAC address, Operating System, OS, Apps, Apps installed, browser, browser type, system, software, peripherals, hardware, Wi-Fi, WiFi, Bluetooth, signals
Location information	IP address, IP, location, zip code, postal code, mailing address, street address, address, city, state, country, Wi-Fi, WiFi, Bluetooth, signals
Off-platform activity	Party, third party/third parties, click, referral, referral site, track, referrer
Platform Usage Information	Date, time, date and time stamp, time on task, user interaction, user engagement, usage, interact, engage, click, mouse movement, track, performance data, move your mouse, mouse

RESULTS & DISCUSSION



PII keywords were most prominently mentioned within all of the privacy policies and Google has more keyword mentions (716) than any other technology analyzed.



Analysis of the top keywords mentioned through all of the privacy policies includes keywords from all of the topic areas. Greater analysis of all keywords shows differing vocabulary within privacy policies—possibly indicating a need for developing common privacy language. Understanding context of these keywords should be considered within future research.

CONCLUSIONS

The COVID-19 pandemic has changed the speed at which K-12 classrooms are adopting educational technology for eLearning management, video-assisted learning, technology management, and gamification. Classrooms no longer seek to include technology as a supplement to learning, but as a requirement for learning. The rapid implementation of this technology has often occurred without privacy for the students and their learning in mind, but rather to continue to keep the "days in school" progressing.

This research shows that privacy policies of common educational technologies indicates PII has the most commonly mentioned keywords. However, because the seed keywords are based on existing laws and regulations, lower indications of data collection in other areas (i.e., platform and off-platform usage, location, device, and user-generated content) may indicate lower definition of these topics within existing laws and regulations and/or lower understanding of how these topics impact privacy.

Future research is needed to better understand the full scope and nature of educational technology data practices as it relates to student privacy. As the education sector continues to be targeted by threat actors, student privacy needs will increase so that these young children do not lose control over their own information before they are given ability to consent to their data being used. The COVID-19 pandemic may have opened Pandora's Box with data collection in K-12 classrooms.

REFERENCES

[1] J. M. Rosenberg and K. B. Staudt Willet, "Balancing' privacy and open science in the context of COVID-19: a response to Ifenthaler & Schumacher (2016)," *Educ. Technol. Res. Dev.*, vol. 69, no. 1, pp. 347–351, 2021, doi: 10.1007/s11423-020-09860-8.

[2] FBI Boston and K. Setera, "FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic," Boston, MA, USA, 2020. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[3] A. Klein, "Cyberattacks on Schools Soared During the Pandemic," *Education Week*, Mar. 2021.

[4] S. Winkler and S. Zeadally, "Privacy Policy Analysis of Popular Web Platforms," *IEEE Technol. Soc. Mag.*, vol. 35, no. 2, pp. 75–85, 2016, doi: 10.1109/MTS.2016.2554419.

[5] J. Kaur, R. A. Dara, C. Obimbo, F. Song, and K. Menard, "A comprehensive keyword analysis of online privacy policies," *Inf. Secur. J.*, vol. 27, no. 5–6, pp. 260–275, 2018, doi: 10.1080/19393555.2019.1606368.

[6] *Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6502-6505*. 1998.

[7] U.S. Department of Education, "Family Educational Rights and Privacy Act (FERPA)," 2021. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (accessed Nov. 12, 2021).