




# School and District Leaders' Understanding of Technology Organizations' Cyber Business Practices

Jaye-Jaye Johnson, PhD

Walden University, Minneapolis, MN, United States

 <https://orcid.org/0009-0009-9493-3605>

Contact: [jayejohnson32@gmail.com](mailto:jayejohnson32@gmail.com)

## Abstract

Educational technology (EdTech) interoperability throughout cyberspace provides the financial opportunity to collect and sell student privacy information in digital learning environments, challenging school leaders to govern schools and keep children safe. School leaders provide the resources, funding, planning, decision making, and administration for EdTech cybersecurity practices and policies, yet little is known about what public school leaders understand. A quantitative study was designed using primary data collected from an online survey. Four research questions guided this study: What are the differences in cybersecurity practices and policy response scores (1) between male and female school leaders; (2) among leaders with different educational achievements; (3) among leaders of different age ranges; and (4) among leaders of different types of school districts? Participants were purposefully identified by their roles from 1,121 Texas public school districts. The sample population was  $n = 173$  and consisted mainly of board members, superintendents, principals, and other district managers. Analysis of variance (ANOVA) was used to determine significant differences between the variables, which revealed a significant difference between men and women in terms of technical terminology, with  $F(1, 171) = 5.28$ ,  $MSE = 3.50$ ,  $\rho = .023$ ,  $\eta^2 = .030$ ,  $n = 173$ . Mode analysis revealed that 33.98% of participants correctly responded to questions about EdTech practices affecting children in schools, and 40.70% correctly responded to questions about school cyber practices, indicating knowledge gaps exist. The implications of narrowing the knowledge gap in schools are critical, leading to potential improvements in student digital security and safety. Also, narrowing the gap can mitigate analytical profiling throughout a student's lifetime, which can lead to loss of education, job, and financial opportunities.

**Keywords:** *educational technology, EdTech, cybersecurity, public schools, privacy, data collection, digital profiling, commoditization, Section 230*

**Date Submitted:** July 19, 2025 | **Date Published:** December 4, 2025

## Recommended Citation

Johnson, J.-J. (2025). School and district leaders' understanding of technology organizations' cyber business practices. *Journal of Educational Research & Practice*, 15, 1–15. <https://doi.org/10.5590.2025.15.2063>

---

*Note:* I wish to acknowledge Dr. Ioan Ioanas and Dr. Beate Baltes from Walden University, Neila Strahan, and Judy Hawkins for all their time, effort, and assistance.

---

## Introduction

Little is known about school leaders' basic literacy in cybersecurity when it comes to educational technology (EdTech), cybersecurity practices, and policies affecting students in digital learning environments in K–12 public schools. According to researchers, the majority of individuals in school leadership positions lack sufficient understanding, making it unclear precisely what they know about cybersecurity practices and policies within the schools they govern (Archambault, 2021; Becker & Levin, 2020; Boninger & Molnar, 2020; Moore et al., 2021).

Understanding of cybersecurity practices and policies is critical. School leaders have the responsibility to prioritize curricula, policies, learning applications, resources, decision making, and governance of cybersecurity and digital literacy throughout the schools (Elmali et al., 2020; Fouad, 2022; Moon, 2018). School leaders should also be cognizant of the security issues, practices, and policies affecting students throughout the school environments they oversee (Becker & Levin, 2020; Symons & Pierce, 2019).

Over time, digital dossiers are accumulated on students and are used in predictive analytics, which can result in identity, financial, and future opportunity losses relating to, for example, employment, health insurance, and education (Archambault, 2021; Keeny, 2019; van der Hof et al., 2020). Digital dossier mishandling can lead to unwanted informational exposures, such as “outings” of individuals with alternative lifestyles (Werbin et al., 2017), and can lead to digital redlining—a method of algorithmic discrimination that is nontransparent to the public and can marginalize racial and socioeconomic groups (Brown & Klein, 2020).

Security breaches occur when companies sell and resell information multiple times (Archambault, 2021; Weller, 2018). These breaches, as well as the selling of student information, can lead to cyberbullying, trolling, manipulation of children online, and sex trafficking (Cramer, 2020; Torbert, 2021). Additionally, breached information is often sold on the digital black market (Fontichiaro, 2019; Fouad, 2022; Symantec, 2019; United States Government Accountability Office [USGAO], 2020; van der Hof et al., 2020). As there are no expiration dates or time regulations on EdTech organizations with regard to data collection (Archambault, 2021; Renz & Hilbig, 2020), the consequences of EdTech mismanagement can occur throughout students' adult lives.

## Literature Review

### Educational Technology Rise and Dominance

EdTech began evolving rapidly in 1998, through the internet, in support of collaborative learning. EdTech became a method to lower costs (Renz & Hilbig, 2020; Weller, 2018), as technology provided a means by which educational content could be reused without recreating materials (Renz & Hilbig, 2020; Weller, 2018). Additionally, packaging learning materials in software benefited the educational sector by lowering labor costs, as the world needed only a few examples of content for instruction (Corbett, 2018; Pise, 2019; Weller, 2018). Although these purposes may have contributed positively to the academic field, the potential for problems arose.

As EdTech firms evolved, through venture capitalism and lobbying efforts (Boninger & Molnar, 2020; Cramer, 2020), student data became a commodity, collected and sold, for companies such as Google, Microsoft, Apple, Meta, and Amazon (Archambault, 2021). Lobbying by philanthropists, such as Bill and Melinda Gates, prompted the incorporation of EdTech into schools (Boninger & Molnar, 2020). Additionally, during the No Child Left Behind era, student achievement tests resulted in massive data, which provided further circumstances to incorporate technology into education (Boninger & Molnar, 2020). Education

has become so profitable that EdTechs make approximately 90% of their revenue from collecting and selling data (Archambault, 2021), and, in recent years, compounding factors, including the COVID-19 pandemic and private education, forced public school leaders to turn to companies that could provide lower costs, free services, and free products to classrooms (Fouad, 2022).

EdTech companies enjoy favorable laws (Archambault, 2021), such as Section 230 of the Communication Decency Act, an immunity law that provides legal shielding from responsibility and accountability (Cramer, 2020). Historically, Section 230 allowed companies to build and prosper during their startup years (Cramer, 2020). Section 230 also contains the Good Samaritan clause, which enables EdTech organizations to self-regulate (Cramer, 2020; Hill, 2019). This disallows transparency and enforcement (Archambault, 2021; Boninger & Molnar, 2020; Hill, 2019) and becomes an additional legal shield for technology firms to keep data collection processes and procedures hidden from the public (Boninger & Molnar, 2020). Along with Section 230, the Family Educational Rights and Privacy Act (FERPA) was amended so that schools could release information as *directory information* without consent. Directory information is defined according to individual schools' interpretations and differs across applications and schools (Marek & Skrabut, 2017; Parks, 2017). Additionally, FERPA was changed in 2009 and 2011 to allow EdTech organizations to become *school officials*, giving companies the legal right to collect and sell student data without parental consent (Archambault, 2021; USGAO, 2020; Jones et al., 2020). School contracts with school officials allow for sharing data with third parties, which can then use this student information outside the intended domains (Boninger & Molnar, 2020). Contributing to the confusion for public and school leaders is that Section 230 and the Children's Online Privacy Protection Act (COPPA) apply to EdTech organizations but not schools, and FERPA applies to schools but not to EdTech organizations (USGAO, 2020).

Kim et al. (2020) argue that companies are disinclined to prioritize privacy unless compelled by public opinion. Cramer (2020) suggests that technology organizations are disincentivized to protect children's privacy and are rewarded for their practices because there is currently no accountability. The lack of transparency and favorable legal immunity laws perpetuate data extraction business practices (Archambault, 2021; Boninger & Molnar, 2020; Fouad, 2022; Jones et al., 2020; Torbert, 2021). Parents have little recourse when breaches and harm occur and are instructed to file complaints under FERPA. To date, however, no FERPA tort cases exist, as the federal government is disinclined to enforce or take actions against EdTech companies (Boninger & Molnar, 2020; Marek & Skrabut, 2017; Schrameyer et al., 2016). And, as EdTech organizations enjoy insufficient federal oversight during mergers, this allows them to become monopolies and extort market power. Moreover, since few competitive threats exist, these firms can extract data with little privacy protection and maximize profitability (United States House of Representatives, Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law, 2022). Data control is market control (Mahari et al., 2021), and there is no expiration on extracted data (Renz & Hilbig, 2020). With data control practices excluding competitors, data power becomes a dominant force (Mahari et al., 2021).

In addition to monopolization, consequences of the COVID-19 pandemic benefited EdTech. School leaders were generally unprepared to implement technology (Moore et al., 2021), just as schools were forced to shift rapidly to online learning (Bakhshaei et al., 2020). The premature adoption and rapid implementation of technology led to insufficient cybersecurity knowledge within educational domains (de Paula, 2021; Johnson et al., 2021). Companies such as Google provided products and services to the academic sector; Chromebooks, for example, were loaded with Google browsers, Gmail, and G Suite applications (Archambault, 2021; de Paula, 2021). The pretense of free services provided the means for collecting student data, because Google had ample accessibility through its products (Archambault, 2021). The collection, selling, and reselling of data render students and children in schools the de facto assets and products of EdTech organizations (Boninger & Molnar, 2020).

## How Student Data is Extracted

The internet can be considered a massive cyber spider web, where the threads are digital flow, and the connecting points of the threads at each end are the point sources (Human Centered Design & Engineering, 2021). In today's learning landscape, a child moves in and out of applications and is tracked and monitored (Boninger & Molnar, 2020), with data being collected at point sources. Hidden actors accomplish the data extraction at these point sources, and the data is then often sold to the highest bidder in hidden marketplaces (Brown & Klein, 2020). Google is an example of a significant hidden and multi-faceted actor, which operates as a friendly browser and provides navigation to domains in exchange for extracted data (Archambault, 2021; de Paula, 2021; Fontichiaro, 2019).

As the main force behind student data extraction is profit, EdTech organizations' goals are in conflict with the goals of public education (Hackman & Reindl, 2022; Moore et al., 2021; Renz & Hilbig, 2020; Torbert, 2021). Researchers suggest that educators are primarily unaware of the tension between entities, cyber business practices, and consequences affecting children (Buchanan et al., 2019; Center for Democracy & Technology, 2020; Johnson et al., 2021).

## Purpose of the Present Study

The purpose of this study was to ascertain school leaders' understanding of cybersecurity practices and policies in public schools. School leaders included superintendents, assistant superintendents, principals, assistant principals, board members, and other district leaders with decision-making responsibilities. There were four independent variables and five dependent variables in the study. The following research questions guided the study and were the independent variables:

- 1.0 RQ1: What are the differences between the cybersecurity practices and policy response scores of male and female school and district leaders?
  - 1.0.1 H<sub>0</sub>1: There are no significant differences between the cybersecurity practices and policy response scores of male and female school district leaders.
  - 1.0.2 H<sub>a</sub>1: There are significant differences between the cybersecurity practices and policy response scores of male and female school district leaders.
- 2.0 RQ2: What are the differences among cybersecurity practices and policy response scores in terms of school district leaders' educational achievements?
  - 2.0.1 H<sub>0</sub>2: There are no significant differences among cybersecurity practices and policy response scores in terms of school district leaders' educational achievements.
  - 2.0.2 H<sub>a</sub>2: There are significant differences among cybersecurity practices and policy response scores in terms of school district leaders' educational achievements.
- 3.0 RQ3: What are the differences among cybersecurity practices and policy response scores in terms of school district leaders' age ranges?
  - 3.0.1 H<sub>0</sub>3: There are no significant differences among cybersecurity practices and policy response scores in terms of school district leaders' age ranges.
  - 3.0.2 H<sub>a</sub>3: There are significant differences among cybersecurity practices and policy response scores in terms of school district leaders' age ranges.

- 4.0 RQ4: What are the differences among cybersecurity practices and policy response scores in terms of school district leaders' district types?
- 4.0.1 H<sub>0</sub>4: There are no significant differences among cybersecurity practices and policy response scores in terms of school district leaders' district types.
- 4.0.2 H<sub>a</sub>4: There are significant differences among cybersecurity practices and policy response scores in terms of school district leaders' district types.

The hypotheses and research design were developed to determine if gender, educational achievement, age range, or district type affected leaders' knowledge of cybersecurity practices and policies in schools. The research questions and design specifically focused on factors discovered from the literature research.

## Methods

This study used a quantitative approach with one-way ANOVA and Bonferroni pair-wise post-hoc analysis to determine if there are significant differences among the sample population of  $n = 173$  school leaders in their response scores to an online survey conducted in Qualtrics. All participants were purposely selected by their job roles from public websites. The independent variables were the demographic factors derived from the research questions. The dependent variables were the response scores inductively arranged into categories and summed in SPSS. The theoretical framework guiding this study was Nissenbaum's contextual integrity theory on information privacy and transmission flow (Nissenbaum, 2004, 2009; Human Centered Design & Engineering, 2021). According to Nissenbaum (2009), the structure of information transmission and privacy should be within the boundaries of what is acceptable by societal norms.

## Participants

The purposeful sampling method was used to recruit school leaders from 1,121 Texas Independent School Districts (ISDs) (State of Texas, n.d.). The sample population was  $n = 173$  and consisted of  $n = 92$  females, or 53.2%, and  $n = 81$  males, or 46.8%. Board members were  $n = 52$ , or 30.1%, superintendents and assistant superintendents  $n = 20$ , or 11.5%, principals and assistant principals  $n = 70$ , or 40.5%, and all other district leaders  $n = 31$ , or 17.9%.

The actual sample participants were 96.7% of the G\*Power recommendations, so the full sample rate could not be achieved. 25,965 email invitations were sent to individuals, resulting in  $n = 218$  total responses and  $n = 173$  finished responses. The response rate was less than 1%.

## Instrumentation

The instrument consisted of six background questions, one technology self-awareness question, and 23 true or false questions. The 23 true or false questions were inductively categorized into five dependent variables and summed in SPSS. The assumption was that summing scores would capture a better participant response and measure the same variable. Individual question responses would not be as reliable and reflect an individual's score. Creswell and Guetterman (2019) indicated that summing scores can increase reliability and the respondents' intentions. The five dependent variables were:

- 1.0 Basic school technology understanding
- 2.0 Basic technology terminology understanding
- 3.0 Basic EdTech practice understanding

- 4.0 Basic school cyber practice understanding
- 5.0 Basic school cyber policy understanding

The scales of measure for the instrument were originally nominal and transformed into ordinal scales in SPSS.

## Design

The design was a non-experimental quantitative analysis of primary response scores from an online instrument that was pilot-tested and expert-reviewed with a S/CVI of .98 and CV/U of .90. Participants' responses to the instrument were tested with Cronbach's alpha at  $\alpha = .445$  for a multi-dimensional measure and deemed acceptable (Ekolu & Quainoo, 2019; Taber, 2018). The five dependent variables were inductively categorized and grouped from 23 nominal survey questions. The questions assessed basic understanding of (1) school technology, (2) technology terminology, (3) EdTech practices, (4) school cyber practices, and (5) school cyber policies. Multiple question responses were summed for each category of the dependent variable. Four independent variables were gender, education, age range, and district type. G\*Power analysis for ANOVA with four groups indicated a recommended sample of  $n = 179$ . The ANOVA analysis was chosen to compare the means of the variables without covariates or interactions from other variables.

## Ethics Procedure

Ethics approval for this study was granted through the IRB process (IRB 01-30-24-1186700). All individuals were contacted electronically through Qualtrics and informed of their right to participate or decline participation. The population was notified of the purpose of the study, how the responses would be used, and how long the participants' information would be kept. Participants were not offered incentives.

## Data Collection

Participant population contact information was compiled from public websites. Email reminders were sent to unfinished survey participants in two intervals. Data collection occurred from February 25, 2024 to April 25, 2024. The total emails sent were 25,965 and distributed through Qualtrics. Of the  $n = 173$  sample participants,  $n = 147$  had advanced educational degrees, representing 84.97% of the sample population. The participants' ages ranged mainly between 40 and 60 years,  $n = 138$ , representing 79.77% of the sample population. The districts represented were 38.2% rural,  $n = 66$ ; 35.3% suburban,  $n = 61$ ; and 26.1% urban,  $n = 46$ . The response data were collected in CSV format from Qualtrics and downloaded into MS Excel 2021 for filtering, organization, and initial analysis. The data were re-coded from the nominal to the ordinal scale, identifying information was deleted, and the remaining data were uploaded into IBM's SPSS (Version 29) for ANOVA statistical analysis. Non-parametric data were analyzed through Kruskal-Wallis (K-W). The response scores were inductively categorized and summed in SPSS into five dependent variables based on question types. Any missing response data were excluded from the summation.

## Data Analysis

Data analysis was performed in SPSS (Version 29). One-way ANOVA tests were used to analyze the variables. ANOVA was selected to focus on the variables' difference in variances. One-way ANOVAs were chosen to compare the means from the research questions as independent factors with the dependent variables without covariates or interactions of other variables. The Fisher analysis of variance, or  $F$  ratio, was calculated from the ANOVAs to determine the variations between and within the variables or the overall difference among the variables tested (Salkind & Frey, 2020; Tanner, 2012). The ANOVA calculated the descriptive statistics, such as mean, standard deviation, standard error of the variables, and frequency. Levene's test was used to check homogeneity. Normality was analyzed through skewness and kurtosis testing. Partial eta-squared sampling was used to check effect sizes and confirm sample size adequacy. Bonferroni pair-wise comparisons were

performed post-hoc where significant differences existed between the means of the variables. Significant values were determined through post-hoc analysis with  $\rho < .05$ . Kruskal-Wallis was conducted where data indicated non-parametric conformity. Alpha was set at  $\alpha = .05$ . (See Table 1.) Correct responses to the true and false portion of the survey were calculated in MS Excel to determine the percentage of correct responses. (See Table 2.)

## Results

Table 1 contains the SPSS statistical analysis summary. There were significant differences between genders in terms of technology terminology, with  $F(1, 171) = .528$ ,  $MSE = 3.50$ ,  $\rho = .023$ , and  $n^2 = .030$ . Bonferroni ad-hoc pairwise testing showed significance between males and females in terms of basic technology terminology knowledge, with  $\rho = .023$ . No other significant differences were found between the variables. Alpha was set at  $\alpha = .05$ .

**Table 1. SPSS Summary**

Independent variable	Dependent variable	Sample	<i>M</i>	<i>SD</i>	Sig	<i>F</i>	n2	K-W	<i>DF</i>
Gender	School technology	173	10.399	1.021	0.522	0.411	0.002		1
Gender	Technology terminology	173	4.960	0.824	0.023*	5.285	0.03		1
Gender	EdTech practices	173	8.000	1.649	0.713	0.136	0.001		1
Gender	School cyber practices	173	5.595	0.895	0.584	0.301	0.002		1
Gender	School cyber policies	173	6.619	0.924	0.256	1.298	0.008		1
Education	School technology	169	10.402	1.025	0.260	1.349	0.024		3
Education	Technology terminology	169	4.970	0.826	0.812	0.318	0.006		3
Education	EdTech practices	169	7.976	1.643	0.510	0.774	0.014		3
Education	School cyber practices	169	5.586	0.890	0.251	**	**	4.103**	3
Education	School cyber policies	169	6.603	0.921	0.089	2.211	0.039		3
Age range	School technology	172	10.407	1.019	0.050	0.792	0.014		3

Age range	Technology terminology	172	4.959	0.826	0.413	0.96	0.017	3
Age range	EdTech practices	172	8.006	1.653	0.916	0.171	0.003	3
Age range	School cyber practices	172	5.605	0.889	0.658	0.536	0.009	3
Age range	School cyber policies	172	6.616	0.926	0.169	1.698	0.029	3
District type	School technology	173	10.399	1.021	0.462	0.775	0.009	2
District type	Technology terminology	173	4.960	0.824	0.420	0.872	0.010	2
District type	EdTech practices	173	8.000	1.649	0.320	1.148	0.013	2
District type	School cyber practices	173	5.595	0.895	0.173	1.77	0.020	2
District type	School cyber policies	173	6.619	0.923	0.542	0.614	0.007	2

**Table 2.** Mode Analysis of True or False Responses

Dependent variable	Correct (n)	Incorrect (n)	Total (n)	Correct (%)	Incorrect (%)
School technology	764	271	1035	73.82	26.18
Technology terminology	348	162	510	68.24	31.76
EdTech practices	351	682	1033	33.98	66.02
School cyber practices	280	408	688	40.70	59.30
School cyber policies	458	229	687	66.67	33.33

Symons and Pierce (2019) stated that school leaders should be cognizant of the security issues, practices, and policies impacting the students throughout their school districts, as prior evidence suggests that children are adversely affected by digital profiling and the commoditization of their privacy data (Lou & Kim, 2019; Radesky et al., 2020; van der Hof et al., 2020). In this study, the cyber practices inquiry covered collecting, selling, and reselling children’s school privacy information. In one example, participants incorrectly thought EdTech firms must be certified, regulated by the government, and are liable for the harm they cause—or contribute to—in civil court. Study findings also revealed that only 34% of school leaders responded correctly to questions about essential EdTech organizations’ cyber practices, indicating that approximately 66% did not

answer the questions correctly, and it can be determined that their knowledge is insufficient. Additionally, only 41% of participants responded correctly to questions about basic school cyber practices. This finding indicates that approximately 59% did not answer correctly. As an example, school leaders did not understand that EdTech entities are immune from harm caused by their actions and that because of that immunity status, parents (whose children are harmed) are told to file a complaint with FERPA, with no recourse. Section 230 protects EdTech companies from liability. Archambault (2021) argues that there have been no civil cases through FERPA and that parents have little legal remedy.

The lack of EdTech certification and test requirements conceals current practices. Boninger and Molnar (2020) explained that transparency and scientific rigor are lacking and that EdTech companies are selling and using buzzwords for economic gain without certifying their applications to meet standards that would avoid negatively affecting children. Additionally, no regulatory framework discloses how the student's information is collected—and for what purposes it will be used (Boninger et al., 2017). Furthermore, since legislators require minimal governance from technology companies, oversight is remanded to school districts (Cramer, 2020; Hill, 2019), but the school districts mostly overlook EdTech cyber practices (Fouad, 2022).

The question about school cyber practices involved FERPA and COPPA policies and compliance, addressing parental consent, transmission, and posting of student data, as well as basic school data violations. The study findings indicated that 59% of school leaders were insufficiently knowledgeable regarding emailing student information, posting pictures on social media, parental notifications, and FERPA age requirements. This is arguably because cyber business practices are counterintuitive to norms, values, and the expectations of society Nissenbaum (2009). The findings of this study also indicate that approximately two-thirds of participants were insufficiently knowledgeable regarding data extracting, selling, and reselling operations, and many student data violations occurred because educators emailed information to incorrect sources or posted privacy information on websites (USGAO, 2020). Actions of staff members, teachers, administrators, and support personnel are attributed to approximately 33% of the cybersecurity violations in U.S. schools between 2015 and 2020 (USGAO, 2020).

As noted above, researchers maintain that student privacy data can be disclosed to EdTech companies under the FERPA school official exception clause without parental or student consent (Archambault, 2021; USGAO, 2020; Jones et al., 2020). Under the school official rule, institutions can release student data to contractors, consultants, volunteers, and all parties who could otherwise perform an educational function (Jones et al., 2020). Researchers argue that data mining of children's digital information will only increase as companies develop newer technologies and methodologies driven by the value of student data (Marcu & Danubianu, 2019; van der Hof et al., 2020).

The study findings indicate that gender could affect school leaders' understanding of technology terminology (the comprehension of digital communication), which can assist school leaders in making informed decisions regarding the digital products and services planned, implemented, and maintained throughout school districts. The sample size of females, for this study, was  $n = 92$  and males  $n = 81$ , with the female sample size being 12% more than male. The ANOVA results for this study showed significant differences between males and females in terms of their knowledge of basic technology terminology,  $F(1, 171) = 5.26$ ,  $MSE = .350$ ,  $\rho = .023$ ,  $n^2 = .030$ ,  $n = 173$ . These ANOVA results align with prior research and suggest that gender can affect decision making and outcomes (Davidson et al., 2020; Guedes et al., 2023). Therefore, it can be argued that gender plays a factor in understanding technology terminology and its implications at the school district governing levels, which can influence district and school technological decision-making.

The State of Texas grants independent school districts (ISDs) autonomy over school governance (Texas Education Code § 13.001, 1995), indicating that ISD leaders have authority, decision-making power, and

oversight of cyber decisions, policies, and practices. Because leaders plan, implement, and govern within state laws (Texas Education Code § 13.001, 1995), they can establish criteria and oversee EdTech organizations.

## Discussion

Educators lack an understanding of data flows and the data collection process used by technology companies (Livingstone et al., 2019). Specific data mining targeted at education is a new field of research that allows academic decision-makers to have a deeper understanding of the educational needs of their institutions (Marcu & Danubianu, 2019).

The mode analysis for this study found that school leaders lacked sufficient understanding of cyber policies and practices in public schools—and that there are knowledge gaps in digital literacy, as leaders often remand cyber issues to IT departments, where personnel have little authority to institute policy interventions and lack decision-making power and oversight (Fouad, 2022). Researchers also suggest most leaders are unaware of the data collection activities, potential consequences, and cyber violations that can occur within digital learning environments (Buchanan et al., 2019; Center for Democracy & Technology, 2020; Johnson et al., 2021).

Additionally, the study findings show a significant difference between male and female response scores in terms of technology terminology, such as understanding the terms and operations of the Internet of Things and thumb drives. The respondents were 85% advanced degree holders. Pew Research (2019) found that understanding of technology-related issues varies greatly depending on the topic, term, or concept and that adults with bachelor's or advanced degrees tend to understand technology better. Nevertheless, the findings suggest that even among those with advanced degrees, there are gender differences with regard to technology concepts. And the knowledge gaps are expected to continue and grow as digital technology rapidly advances and school districts attempt to keep pace (McDermott et al., 2019).

Researchers argue there is no evidence that student cybersecurity issues are likely to go away, because, as technology evolves, the practices of privacy invasion will, as well (Adams, 2017; Livingstone et al., 2019; Moon, 2018). Profitability will influence the commoditization of student data, affecting those responsible at the districts and schools for keeping children and their information safe (Archambault, 2021).

Regardless of EdTech companies' profitability, society expects children to be kept from harm in educational domains, but the current cyber practices and policies are in tension with the expectations of societal norms. Nissenbaum (2009) argues that the digital information flow is disrupted when this tension occurs, and the contextual integrity framework is violated. Additionally, there is rising concern about losing control over personal information in the public discourse, an individual's ability to discern privacy boundaries, and understanding legal boundaries for private and public parties regarding privacy (Livingstone et al., 2018).

## Conclusions and Recommendations

Nissenbaum (2018) argues that something is missing from the bodies of law and regulations regarding privacy and that new technologies, practices, and institutions cross the privacy thresholds, as evidenced by public hearings, while legislation and enforcement lag behind. Although it may be unfair to place the sole responsibility for children's cyber safety on school leaders, EdTech organizations and parents are obligated to provide cybersecurity oversight and protection for their children. It is also reasonable to believe that these companies should be accountable for protecting children and their privacy.

This study focused on school leaders from the state of Texas who were tasked with governing schools under their charge, including the expectations that students and their data will be safe, utilizing the technology approved for district use—schools are where society expects children to be as safe as possible from harm. The combination of cyber business practices, inadequate and oblique laws, and school cyber violations, however, hinders cybersecurity and puts children and their privacy at risk (Nissenbaum, 2019).

School leaders' lack of cyber business practices and understanding can lead to consequences for children, including barriers to future educational opportunities, employment, health care, and financial and identity losses (Brown & Klein, 2020; Cramer, 2020; Torbert, 2021). Leaders with a solid understanding of cyber business practices can assist with providing support and resources to schools, establishing age-appropriate curricula, raising the awareness of teachers and staff, and practicing governance of EdTech firms throughout districts.

Because the study results indicate educational leaders have cyber knowledge gaps, narrowing these gaps can assist with establishing safe cybersecurity procedures throughout districts. This can be accomplished through a multi-faceted approach, such as increasing the cybersecurity knowledge of public school personnel; developing age-appropriate cyber literacy curricula; and implementing safeguards, such as Nissenbaum's *ought or ought not* concept, which can be implemented during the planning, designing, developing, and implementing stages of technology in schools. Nissenbaum's (2009) contextual theory can lead to improving student digital security and safety in public schools throughout the United States and internationally. As suggested by Nissenbaum (2009), the *ought or ought not* concept is an ethical question to be asked at each stage, by relevant personnel from engineers to lawmakers: Ought this to be as society expects or ought not? If the answer is "Ought not," there is a disruption.

## Limitations

The limitations of this study included generalizing that the individual participants represent the population by restricting the study to the state of Texas, having less than the recommended sample rate response, and discovering that the majority of the sample participants were advanced degree holders. The sample population collected for the study was  $n = 173$  from the Texas ISDs, representing 96.7% of the G\*Power recommendation for an ANOVA with four group levels. The participants represented a well-educated sample population, with approximately 85% earning at least a master's or higher degree. Purposeful sampling with the quantitative approach confined participants' responses to the online survey, based on their roles. The instrument questioning was closed-ended and did not help to understand the participants' responses. Some participants had incomplete answers. Additionally, there may have been occurrences where some participants attempted to provide acceptable responses instead of truthful answers or may have guessed and rushed because of survey fatigue. Cronbach's alpha to the response questions from the instrument was calculated at  $\alpha = .455$ , which may raise reliability concerns to some researchers but, according to prior research, is deemed acceptable because of the multi-dimensional content the instrument measured (Ekolu & Quainoo, 2019; Taber, 2018). Barera et al. (2021), Ekolu and Quainoo (2019), and Taber (2018) concurred that any standard threshold or criteria for alpha for an instrument that measures multiple concepts should be between .15 and .5 (Ekolu & Quainoo, 2019). The instrument assesses participants' basic understanding of EdTech cybersecurity practices and policies and should not be highly consistent, because the measurement assesses multiple and different concepts of EdTech cybersecurity practices and policies.

## References

- Adams, M. (2017). Big data and individual privacy in the age of the Internet of Things. *Technology Innovation Management Review*, 7(4), 12–24. <https://doi.org/10.22215/timreview/1067>
- Archambault, S. G. (2021). Student privacy in the digital age. *BYU Education and Law Journal*, 2021(1), Article 6. [https://scholarsarchive.byu.edu/byu\\_elj/vol2021/iss1/6/](https://scholarsarchive.byu.edu/byu_elj/vol2021/iss1/6/)
- Bakhshaei, M., Seylar, J., Ruiz, P., & Vang, M. C. (2020). The valuable role of Edtech coaches during the COVID-19 pandemic: A national survey. *Digital Promise*. <https://doi.org/10.51388/20.500.12265/101>
- Becker, J. D., & Levin, D. A. (2020). Like moths to a flame: Unsecured networks, tech-savvy students, and district policy. *Journal of Cases in Educational Leadership*, 23(2), 47–59. <https://doi.org/10.1177/1555458919899458>
- Boninger, F., & Molnar, A. (2020). *Issues to consider before adopting a digital platform or learning program*. National Education Policy Center. <https://nepc.colorado.edu/publication/virtual-learning>
- Boninger, F., Molnar, A., & Murray, K. (2017). *Asleep at the switch: Schoolhouse commercialism, student privacy, and the failure of policymaking*. National Education Policy Center. <https://nepc.colorado.edu/publication/schoolhouse-commercialism-2017>
- Brown, M., & Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. *Journal of Higher Education*, 91(7), 1149–1178. <https://doi.org/10.1080/00221546.2020.1770045>
- Buchanan, R., Southgate, E., & Smith, S. P. (2019). “The whole world’s watching really”: Parental and educator perspectives on managing children’s digital lives. *Global Studies of Childhood*, 9(2), 167–180. <https://doi.org/10.1177/2043610619846351>
- Center for Democracy & Technology. (2020, October 22). *Research shows teachers, parents, and students need more support to protect privacy and advance digital equity*. <https://cdt.org/press/research-shows-teachers-parents-students-need-more-support-to-protect-privacy-and-advance-digital-equity>
- Corbett, C. J. (2018). How sustainable is big data? *Production and Operations Management*, 27(9), 1685–1695. <https://doi.org/10.1111/poms.12837>
- Cramer, B. W. (2020). From liability to accountability: The ethics of citing section 230 to avoid the obligations of running a social media platform. *Journal of Information Policy*, 10, 123–150. <https://doi.org/10.5325/jinfopoli.10.2020.0123>
- Creswell, J., & Guetterman, T. (2019). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed). Pearson.
- Davidson, A. M., McGregor, R. M., & Siemiatycky, M. (2020). Gender, race and political ambition: The case of Ontario school board elections. *Canadian Journal of Political Science Revue*, 53(2), 461–475. <https://doi.org/10.1017/S0008423919001057>
- de Paula, A. S. N. (2021). The learning-market of Edtech in Brazilian education: The impacts of the COVID-19 pandemic on the educational sector. *Journal for Critical Education Policy Studies*, 19(1), 249–270. <https://eric.ed.gov/?id=EJ1300486>
- Ekolu, S. O., & Quainoo, H. (2019). Reliability of assessments in engineering education using Cronbach’s alpha, KR and split-half methods. *Global Journal of Engineering Education*, 21(1), 24–29. <https://www.wiete.com.au/journals/GJEE/Publish/vol21no1/03-Ekolu-S.pdf>

- Elmali, F., Tekin, A., & Polat, E. (2020). A study on digital citizenship: Preschool teacher candidates vs. computer education and instructional technology teacher candidates. *Turkish Online Journal of Distance Education*, 21(4), 251–269. <https://doi.org/10.17718/tojde.803423>
- Fontichiaro, K. (2019). Data literacy: Negotiating convenience and data privacy. *Teacher Librarian*, 47(1), 51–63. <https://www.proquest.com/magazines/data-literacy-negotiating-convenience-privacy/docview/2334269398/se-2>
- Fouad, N. S. (2022). The security economics of EdTech: Vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy, Regulation and Governance*, 24(3), 259–273. <https://doi.org/10.1108/DPRG-07-2021-0090>
- Guedes, M. J., Patel, P. C., & Casaca, S. F. (2023). On the same page? Differences between male and female board members on the benefits of a gender-balanced representation. *Corporate Governance: The International Journal of Business in Society*, 23(3), 514–533. <https://doi.org/10.1108/CG-01-2022-0032>
- Hackman, S. T., & Reindl, S. (2022). Challenging EdTech: Towards a more inclusive, accessible and purposeful version of EdTech. *Knowledge Cultures*, 10(1), 7–21. <https://doi.org/10.22381/kc10120221>
- Hill, S. (2019). Empire and the megamachine: Comparing two controversies over social media content. *Internet Policy Review*, 8(1). <https://doi.org/10.14763/2019.1.1393>
- Human Centered Design & Engineering. (2021, March 10). *2021 distinguished lecture: Helen Nissenbaum: Contextual integrity* [Video]. YouTube. <https://youtu.be/VPwmCoSfe50>
- Johnson, J., Daum, D., & Norris, J. (2021). I need help! Physical educators transition to distance learning during COVID-19. *Physical Educator*, 78(2), 119–137. <https://eric.ed.gov/?id=EJ1293160>
- Jones, K. M. L., Rubel, A., & LeClere, E. (2020). A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics. *Journal of the Association for Information Science and Technology*, 71(10), 1227–1241. <https://doi.org/10.1002/asi.24327>
- Keeny, A. J. (2019). School social workers' perceptions of ethical dilemmas associated with electronic media use in school settings. *Children and Schools*, 41(4), 203–211. <https://doi.org/10.1093/cs/cdz019>
- Kim, J., Baskerville, R. L., & Ding, Y. (2020). Breaking the privacy kill chain: Protecting individual and group privacy online. *Information Systems Frontiers*, 22(1), 171–185. <https://doi.org/10.1007/s10796-018-9856-5>
- Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science. [https://eprints.lse.ac.uk/101283/1/Livingstone\\_childrens\\_data\\_and\\_privacy\\_online\\_evidence\\_review\\_published.pdf?utm\\_source=chatgpt.comprivacy-online-report-for-web.pdf](https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf?utm_source=chatgpt.comprivacy-online-report-for-web.pdf)
- Lou, C., & Kim, H. K. (2019). Fancying the new rich and famous? Explicating the roles of influencer content, credibility, and parental mediation in adolescents' parasocial relationship, materialism, and purchase intentions. *Frontiers in Psychology*, 10, Article 491161. <https://doi.org/10.3389/fpsyg.2019.02567>
- Mahari, R. Z., Lera, S. C., & Pentland, A. (2021). Time for a new antitrust era: Refocusing antitrust law to invigorate competition in the 21st century. *Stanford Computational Antitrust*, 1, 52–63. <https://doi.org/10.51868/4>
- Marcu, D., & Danubianu, M. (2019). Learning analytics or educational data mining? This is the question. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, 10, 1–14. <https://doi.org/10.70594/brain/v10.s2/1>

- Marek, M. W., & Skrabut, S. (2017). Privacy in the educational use of social media in the U.S. *International Journal on E-Learning*, 16(3), 265–286.  
[https://www.researchgate.net/publication/300080104\\_Privacy\\_in\\_Educational\\_use\\_of\\_Social\\_Media\\_in\\_the\\_US](https://www.researchgate.net/publication/300080104_Privacy_in_Educational_use_of_Social_Media_in_the_US)
- McDermott, M., Reeves, J., Mendez, G., Capo, B., & Karp, J. (2019). Maintaining privacy and security in cyberspace: What everyone needs to know. *Distance Learning*, 16(3), 16–25.  
<https://eric.ed.gov/?id=EJ1302888>
- Moon, E. C. (2018). Teaching students out of harm's way: Mitigating digital knowledge gaps and digital risk created by 1:1 device programs in K–12 education in the USA. *Journal of Information, Communication and Ethics in Society*, 16(3), 290–302. <https://doi.org/10.1108/JICES-02-2018-0012>
- Moore, S. D. M., Jayme, B. D. E., & Black, J. (2021). Disaster capitalism, rampant EdTech opportunism, and the advancement of online learning in the era of COVID19. *Critical Education*, 12(2), 1–23.  
<https://doi.org/10.14288/ce.v12i2>
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1) 119–157.  
<https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.
- Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, 24(3), 831–852. <https://doi.org/10.1007/s11948-015-9674-9>
- Parks, C. (2017). Beyond compliance: Students and FERPA in the age of big data. *Journal of Intellectual Freedom and Privacy*, 2(2), 23–33. <https://doi.org/10.5860/jifp.v2i2.6253>
- Pise, V. H. (2019). Cloud computing: Recent trends in information technology. *ANWESH: International Journal of Management and Information Technology*, 4(1), 27–29.  
<http://www.publishingindia.com/anwesh/106/cloud-computing-recent-trends-in-information-technology/778/5406/>
- Radesky, J., Chassiakos, Y. R., Ameenuddin, N., & Navsaria, D. (2020). Digital advertising to children. *Pediatrics*, 146(1), Article e20201681. <https://doi.org/10.1542/peds.2020-1681>
- Renz, A., & Hilbig, R. (2020). Prerequisites for artificial intelligence in further education: Identification of drivers, barriers, and business models of educational technology companies. *International Journal of Educational Technology in Higher Education*, 17(14), 1–21. <https://doi.org/10.1186/s41239-020-00193-3>
- Salkind, N. J., & Frey, B. B. (2020). *Statistics for people who (think they) hate statistics* (7th ed). SAGE Publications.
- Schrammeyer, A. R., Graves, T. M., Hua, D. M., & Brandt, N. C. (2016). Online student collaboration and FERPA considerations. *TechTrends*, 60(6), 540–548. <https://doi.org/10.1007/s11528-016-0117-5>
- State of Texas (n.d.). *State board of education*. <https://sboe.texas.gov/>
- Symantec. (2019, February). *Internet security threat report* (Vol. 24). <https://docs.broadcom.com/doc/istr-24-2019-en>
- Symons, D., & Pierce, R. (2019). Programs, packages, and apps: Some guidance for investment in technology. *Australian Primary Mathematics Classroom*, 24(1), 3–6.  
<https://eric.ed.gov/?id=EJ1289321>

- Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, 48(6), 1273–1296. <https://doi.org/10.1007/978-94-6300-749-8>
- Tanner, D. (2012). *Using statistics to make educational decisions*. SAGE Publications.
- Texas Education Code § 13.001 (1995). Definition. In *Title 2. Public education; Subtitle C. Local organization and governance; Chapter 13. Creation, consolidation, and abolition of a district; Subchapter A. General provisions*. <https://statutes.capitol.texas.gov/Docs/ED/htm/ED.13.htm>
- Torbert, P. (2021). Because it is wrong: The immorality and illegality of the online service contracts of Google and Facebook. *Case Western Reserve Journal of Law, Technology and the Internet*, 12(1), 1–173. <https://scholarlycommons.law.case.edu/jolti/vol12/iss1/2>
- United States Government Accountability Office. (2020). *Data security: Recent K–12 breaches show that students are vulnerable to harm* (GAO-20-644). <https://www.gao.gov/assets/gao-20-644.pdf>
- United States House of Representatives, Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law. (2022). *Investigation of competition in digital markets: Majority staff report and recommendations: Part II* (H.R. Prt. No. 117-8). U.S. Government Publishing Office. <https://www.congress.gov/committee-print/117th-congress/house-committee-print/47833>
- van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefwaard, T. (2020). The child's right to protection against economic exploitation in the digital world. *The International Journal of Children's Rights*, 28(4), 833–859. <https://doi.org/10.1163/15718182-28040003>
- Weller, M. (2018, July 2). Twenty years of Edtech. *EDUCAUSE Review*, 53(4), 35–48. <https://er.educause.edu/-/media/files/articles/2018/7/er184101.pdf>
- Werbin, K. C., Lipton, M., & Bowman, M. J. (2017). The contextual integrity of the closet: Privacy, data mining and outing Facebook's algorithmic logics. *Queer Studies in Media & Popular Culture* 2(1), 29–47. [https://doi.org/10.1386/qsmprc.2.1.29\\_1](https://doi.org/10.1386/qsmprc.2.1.29_1)



The *Journal of Educational Research and Practice* is a peer-reviewed journal that provides a forum for studies and dialogue about developments and change in the field of education and learning. The journal includes research and related content that

examine current relevant educational issues and processes. The aim is to provide readers with knowledge and strategies to use that knowledge in educational or learning environments. *JERAP* focuses on education at all levels and in any setting, and includes peer-reviewed research reports, commentaries, book reviews, interviews of prominent individuals, and reports about educational practice. The journal is sponsored by The Richard W. Riley College of Education and Human Sciences at Walden University, and publication in *JERAP* is always free to authors and readers.