Balancing Student Data Privacy and Innovation:

Practices and Perceptions in Hawai‘i Public Schools

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE UNIVERSITY OF HAWAI‘I AT MĀNOA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

LEARNING DESIGN AND TECHNOLOGY

DECEMBER 2021

By

Minara Mordecai
University of Hawai‘i

Committee members:
Seungoh Paek - Chair
Ariana Eichelberger
Catherine Fulford
Curtis Ho
Jenifer Winter

Keywords: student data privacy, K-12 student data, FERPA

ACKNOWLEDGMENTS

Спасибо! Mahalo! 谢谢你! متشكرم!

Gracias! 감사 해요! ありがとう！ Thank you!

To my dissertation committee and tireless advisor.

To all who helped and encouraged me on this journey.

To my tribe.

ABSTRACT

Advances in educational technology have led to unprecedented accumulation of student information, but there is limited research to inform school practices in protecting student data. At a minimum, school districts must remain in compliance with increasingly complex state and federal laws on student privacy. Moreover, increased cyberattacks on K-12 and growing concerns about the misuse of student data call for additional protections that go beyond legal compliance. However, safeguards of student data should not get in the way of innovative data-driven interventions in improving students' academic and social development. This dissertation explores the complexities of balancing privacy and innovation in public schools. Based on a three-phase exploratory case study, three distinct manuscripts emerged to understand K-12 student data privacy practices in a single school district in Hawai‘i from a perspective of diverse district-level and school-level personnel. The first manuscript offers an interdisciplinary review of literature and legislation related to student data privacy in K-12 to reveal national trends and best practices. The second manuscript is based on a quantitative anonymous survey of district-level administrators to assess their practices and perceptions at the school district. Using semi-structured interviews with school-level personnel, the third manuscript offers insight into the participants' experiences, as well as barriers and enablers of educational technology implementation at the district. Findings that link the three manuscripts suggest the need for improved communication, increased training, and shift of the current practices toward a student-centric data privacy framework. These findings contribute to the literature on student data privacy and provide school districts with recommendations for effective and safe data sharing practices. The dissertation is presented as an alternative model with three manuscripts of publishable quality incorporated as Chapters 3-5.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1. INTRODUCTION AND METHODOLOGY

In line with innovative practices in my selected field, I present this dissertation in a non-traditional format with three manuscripts that maintain the methodological rigor of traditional research. The dissertation consists of Chapter 1 (Introduction and Methodology) and Chapter 2 (Literature Review), followed by three articles of publishable quality presented as Chapters 3-5. The concluding remarks are encapsulated in Chapter 6. To meet the needs of this format, the following Chapter 1 includes a description of the research design, structure of the dissertation, and methodology that would have been traditionally reserved for Chapter 3. This chapter also includes background information, summary of the conceptual framework, rigor and limitations, timeline, and definition of terms.

Background and Supporting Literature

In July of 2019, parents of some 70,000 public school students in Hawai‘i received a letter from the school district that their children's names, addresses, grades, test scores, and other personal information had been exposed to unauthorized access because of improper security protocols in an online portal *My Future Hawai‘i* (*My Future Hawai‘i Possible Data Exposure FAQ*, 2019). Graduation Alliance, a private educational company, was contracted to administer the online portal and its contract has since been terminated (University of Hawai‘i News, 2019).

Unfortunately, this incident is not an exception but a norm in the increasingly attack-prone environment of cloud computing (Abraham et al., 2019; Brenan, 2018), and public schools are an easy target for cyberattacks, cyber extortions, and internal or external data breaches (Cybersecurity and Infrastructure Security Agency (CISA), 2020; Doran, 2018; Hobbs, 2017; Levin, 2021; Nicosia, 2017). School districts are the so-called sitting ducks when it comes to

data security because they compile large digital depositories of personally identifiable information. However, public schools typically lack the finances and the personnel of private entities to strengthen the security networks and to monitor data leaks (Hobbs, 2017). What exacerbates the problem is the increasingly common use of technology in schools, generating digital data and digital footprints with each use (Carmel et al., 2019; Edwards, 2015; Reidenberg et al., 2013). Though there has been a shift toward privacy awareness in recent years, parents still largely accept the culture of digital trust in which school districts manage sensitive student data without parental input until there is a security breach (Abraham et al., 2019).

School districts collect inordinate amounts of student data that requires complex storage, distribution, and management procedures. The student data are accessible to both internal school employees (for example, data governance officers, general counsel, instructional technologists, information technology officers) and external stakeholders (for example, educational technology providers, state legislators, U.S. Department of Education). To meet the demands of data sharing, 90% of school districts report relying on cloud computing to maintain and mine data, however, the vast interconnectivity of cloud computing delivers both convenience and risks (Kaufman, 2009; Reidenberg et al., 2013).

Student records are afforded privacy protections by federal and state laws, but the primary legislation, the Family Educational Rights and Privacy Act (FERPA, 1974), has yet to include a comprehensive set of guidelines related to digital records (Elliott et al., 2014). Thus, educators are left to interpret FERPA based on an outdated model or seek guidance for each new technological development (Chapple, 2019; U.S. Department of Education, Family Policy Compliance Office, 2007).

Problem Statement

With the fast-moving innovations in technology, increased breaches in cyber security, and limited guidance on digital record-keeping, K-12 school administrators are facing complex challenges and have limited research to inform their practices when it comes to student data protections, particularly in a data sharing environment. At a minimum, school districts must maintain compliance with numerous state and federal guidelines on student privacy. However, the legislative process has not kept up with emerging malicious cyber threats and growing concerns among parents (Haduong et al., 2015; Strauss, 2017; Weippl & Min Tjoa, 2005). Even the definitions of privacy have become fluid and uncertain when it comes to digital learning environments (Vance, 2016). Local school districts are left to devise additional protections that go beyond minimum compliance. These concerns, threats, and legislative mandates form one side of the scale.

On the other side of the scale, we see an opportunity to improve students' academic and social development at individual levels using millions of points of data and advanced learning analytics. Educators must find a delicate balance in nurturing these opportunities without letting concerns for student privacy fade to the background. This problem leads to the exploration in my current research. I selected Hawai‘i statewide school district as the site for my study because of its unique attributes which I will discuss in more detail in the Research Context section of this chapter. The purpose of this exploratory, interpretive case study was to understand the policies and regulations that guide K-12 student data management practices, and to assess current practices in a single school district from a perspective of diverse district-level and school-level administrators. Such exploration contributes to the literature on the topic and provides school districts with effective and safe data sharing practices.

Conceptual Framework

'Privacy' is a fluid term that defies well-articulated boundaries or a unitary definition (DeCew, 1997). Consequently, a study examining privacy concerns should be grounded in a narrowly tailored conceptual framework to offset the elusive nature of this term. In my study on student data privacy, I rely on a conceptual framework that combines *activity theory* and the *contextual integrity (CI) framework* as articulated by Engeström (1987) and Nissenbaum (2010), respectively. The conceptual model designed for this study combines both theories and serves as a foundational point of inquiry to inform my research.

To properly examine how digital data collection and its use impact student privacy in a K-12 environment, I must first define the relationship between data, privacy, student records, and the various institutional actors who are directly involved with student data. In this regard, activity theory offers a well-suited system-based framework to examine an activity - such as data collection and use - against the backdrop of its context, actors (subjects), and objectives (or objects) (Nardi, 1996). With its focus on context, activity theory has been adopted as an influential framework in organizational and system-based examination of technology (Clemmensen et al., 2016; Korpelainen & Kira, 2013). In educational technology research, activity theory has been utilized to examine constructivist learning environments, as well as to assess barriers in technology implementation (Bellamy, 1996; Jonassen & Rohrer-Murphy, 1999; Karakus, 2014). More recently, researchers incorporated activity theory in assessing the impact of data analytics in primary and secondary education (Frontiera, 2019).

For this research study, activity theory delivers a suitable system to describe a relationship between institutional actors (subjects) and student data privacy (object) within a K-12 public school district (context). Included as mediating elements of the system are the digital

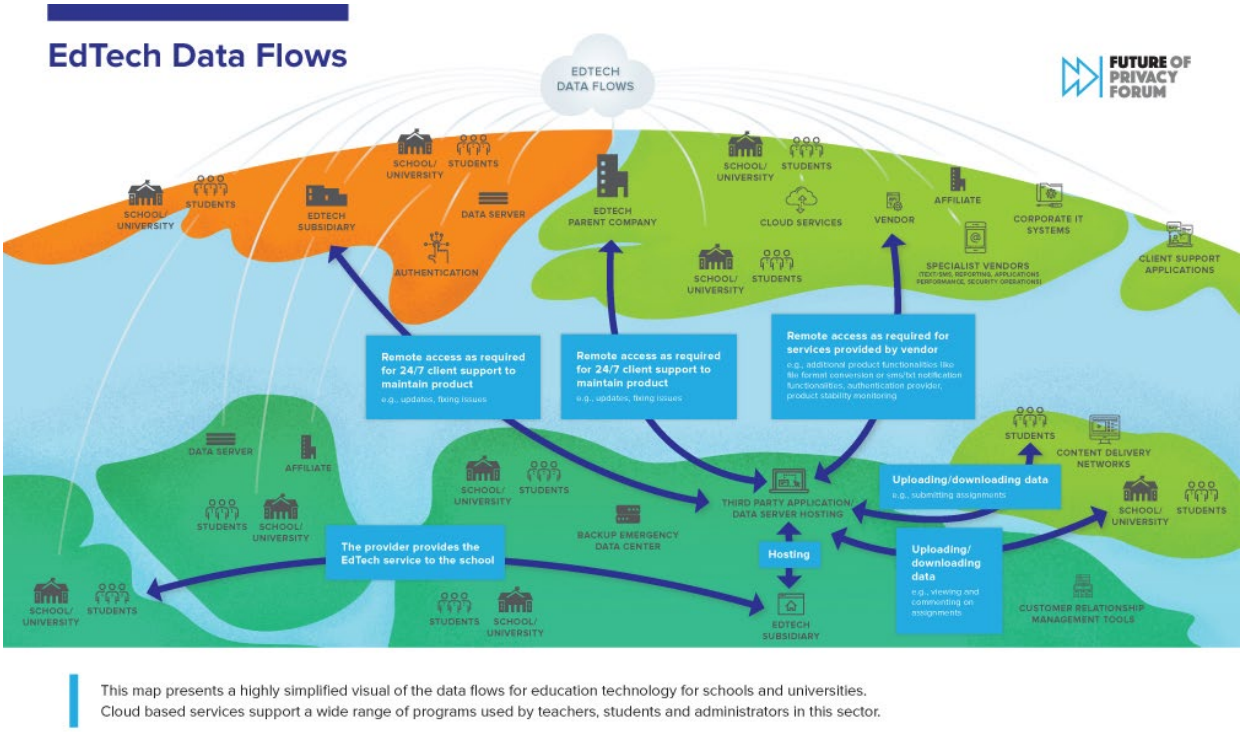
tools (artifacts), laws and policies (rules), stakeholders such as parents and teachers (community), and the defined roles of the school administrators (division of labor). To narrow the scope of the study even further, I append the contextual integrity (CI) framework to formulate a conceptual framework that prioritizes context and privacy.

Nissenbaum's (2010) CI framework was designed to analyze and assess privacy threats. It moves away from the definition of privacy through traditional public-private spheres. Instead, CI aims to identify what we consider private by examining "informational flow," that is "transmission, communication, transfer, distribution, and dissemination" (Nissenbaum, 2010, p. 140) of information along the appropriate information norms. What is key in understanding and applying CI is that information norms are subjective and depend on the context. *Actors*, such as people or organizations involved in the transmission of information, are an important contextual element, prompting discussion of *who* is sending the information, *who* is receiving it, and *about whom* the information is transmitted. Context already plays an important role in information privacy in some regards, for example, information about minors or patients (*about whom*) receive greater protection than for ordinary citizens. Other contextual considerations include the nature and type of information transmitted, and the transmission principles that constrain the flow of information, for example, legislation. Transmission principles encompass both explicit norms, such as laws, and implicit norms, such as practices and procedures that are unique to a specific organization or department. In this case study, school administrators operate under explicit and implicit norms: legislation and policies establish the minimum threshold of norms that must be followed (explicit), and departmental practices are followed even when they are mandated or codified (implicit).

In an education context, the "flow of information," as outlined by Nissenbaum (2010), is a sociotechnical practice, which has both technical and social elements and requires a structural, contextual examination (Bijker, 1997). Students' expectation of privacy when it comes to data sharing is determined by actors involved in data transmission, the technology used, and the purpose for which it is shared. For example, concerns for privacy grows when storage of student data moves from a school-controlled internal server to a Google-owned cloud server even if the end result is the same (Reidenberg et al., 2013). In this scenario, the parameters on how Google will store, manage, and use data determine the context of information flow. The more actors are involved in the transmission of information, the more complex and nuanced the context. Reflecting on this through the CI lens, actors, types of information, and transmission principles, all help cement the students' expectation of privacy (Nissenbaum, 2010). Figure 1 below represents a visual for the numerous actors involved in a modern "flow" of student information, including educational technology (Ed Tech) providers, subsidiaries, cloud-based servers, schools, and students; (Van Eijk & Zanfir-Fortuna, 2021; used under Creative Commons license).

Figure 1

Student Information Flow Among Diverse Actors



Note: The image "EdTech Data Flows" by Future of Privacy Forum is licensed under CC BY 4.0.

Equally important to this study is the philosophical undercurrent of CI framework in which Nissenbaum theorizes that "what people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*" (Nissenbaum, 2010, p. 2). This principle serves a critical role in helping school administrators develop safe and effective student data sharing practices, suggesting that large data collection can be utilized for student success as long as it is done thoughtfully and in an appropriate context.

Nissenbaum's argument to prioritize context fits squarely with the Activity Theory creating a nuanced representation of Engeström's theory through a privacy lens. The *rules* in Activity Theory, which are defined as a set of boundaries that govern and restrict the activity

(Engeström, Miettinen, & Punamäki, 1999), are also the *transition principles* identified by CI as "constraints under which information flows" (Nissenbaum, 2011, p. 33). Similarly, *actors* identified by Nissenbaum can be found in Engeström's *subject, community, and division of labor* elements. In order to preserve privacy, the subjects must ensure that "information flows generated by an action or practice conform to legitimate contextual informational norms" (Nissenbaum, 2019), p. 224).

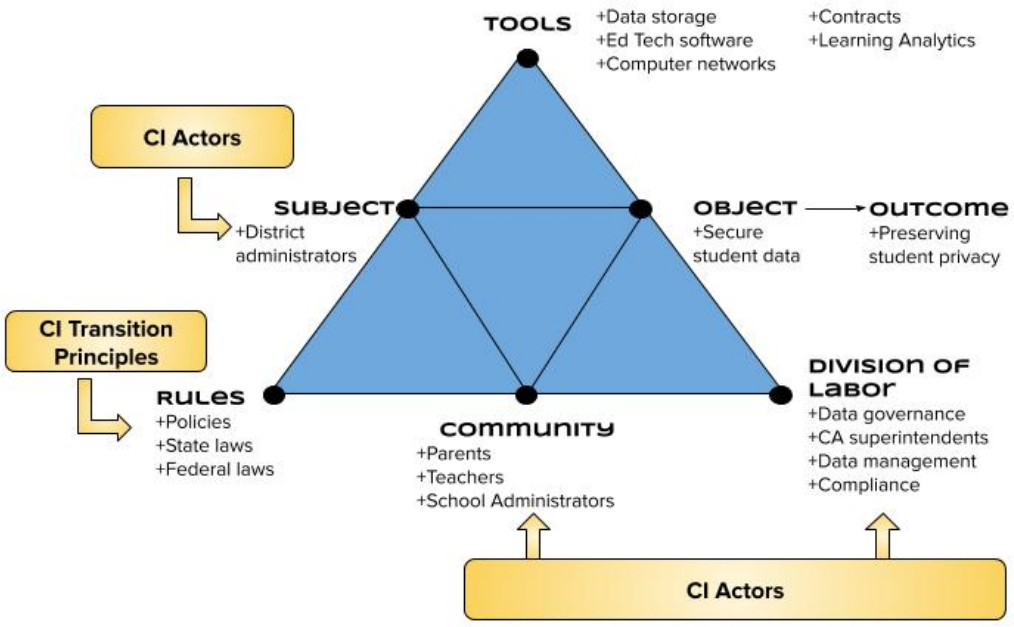
By prioritizing context, this narrowly-tailored conceptual model delivers an ideal framework for the study for a number of reasons. First, the definition of privacy can vary greatly depending on the industry and accepted norms (Solove, 2010). Hence, the study's findings on the issue of privacy will only carry meaning within a specific context, in this case K-12 education. Second, the descriptive nature of the Engestrom's (1987) and Nissenbaum's (2010) theories aids in identifying patterns in a newly emerging phenomenon without normatively dismissing the practices as positive or negative based on outdated assumptions. Third, this conceptual model offers a multi-layered approach to organize both social and technical dimensions of privacy.

The computing power and digital tools currently used by school districts are unprecedented by all accounts. The present-day practice of collection, storage, and transfer of digital student data should be examined as a new, emerging phenomenon rather than as old record-keeping practice that uses new tools. Consequently, a descriptive conceptual model is appropriate to understand the new processes as a unique phenomenon.

In conclusion, the two theories, collectively, deliver a rich foundation to examine the collection, storage, and use of student data both in policy and in practice. The resulting conceptual model is represented in Figure 2.

Figure 2

Conceptual Model Combining Activity Theory and Contextual Integrity Framework in K-12 School Districts



Note: Adapted from the structure of human activity (Engeström, 1987, p. 78). Reproduced with permission, see Appendix A.

Research Questions (RQs)

Based on the existing gaps in research in the area of student data privacy, I pose the following questions to be addressed in my study:

1) What are the current trends in student data privacy as evidenced by school district policies and legislation related to student data privacy? (RQ #1)
    a) Conceptual framework alignment: Rules

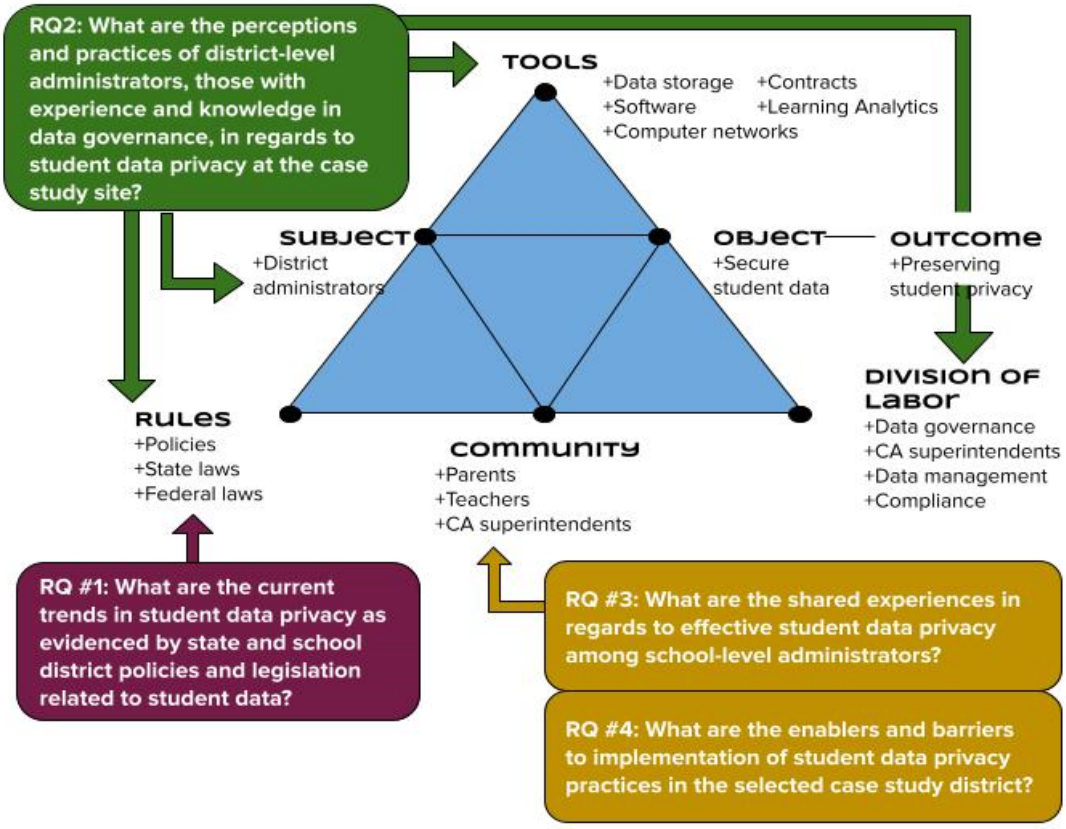
2) What are the perceptions and practices of district-level administrators, those with experience and knowledge in data governance, regarding student data privacy? (RQ #2)
    a) Conceptual framework alignment: Subject; Tools; Division of Labor; Rules
3) What are the experiences among school-level administrators regarding effective student data privacy practices? (RQ #3)
    a) Conceptual framework alignment: Community; Division of Labor
4) What are the enablers and barriers to implementation of student data privacy practices in the selected case study district? (RQ #4)
    a) Conceptual framework alignment: Community

Because contexts are fluid, dynamic, and "are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more" (Nissenbaum, 2010, p. 130), it is important to identify characteristics of the context for any given research study. Defining context offers the reader a clear scope of the research and its findings. In this study, I am focusing on collection and sharing of student data in a single K-12 public school system, which presents several contexts for investigation. The macro context of the study is the district and its schools as a single system. The micro context here is the policy making and policy implementation operation of the school district consisting of institutional actors that monitor, interact with, collect, secure, and share student data. This micro context will be the primary focus of my study. The research questions for the case study are thus informed by the conceptual model which considers the system context (K-12 public school district), micro context (institutional actors within the district), artifacts (technology), and transmission principles as articulated by the CI framework (policies and regulations that govern student data sharing). Furthermore, each research question is part of a larger holistic inquiry aimed at analyzing the

system of data sharing as an activity. Figure 3 offers an alignment of the conceptual framework with the proposed research questions.

Figure 3

Alignment of Research Questions with the Conceptual Framework



Research design and methodology

Structure of the Dissertation

This dissertation follows an alternative model resulting in three distinct but related manuscripts (Chapters 3-5). This model is appropriate for students who seek a professional career in academia, and for research designs that deliver distinct, stand-alone findings. The manuscripts encompass literature review and data collection conducted as part of the overall

dissertation requirements. Chapter 3 and 4 are written as articles of publishable quality to be submitted for publication to peer-reviewed educational research or law review journals. Chapter 5 may be summarized in a conference presentation, or published as a conference proceeding.

The research progressed in three phases, each one documented as a separate publication, see Figure 4.

Phase 1, Chapter 3: Review existing legislation, reports, academic journals, and select school policies to document current trends and best practices related to student data privacy (research question #1).

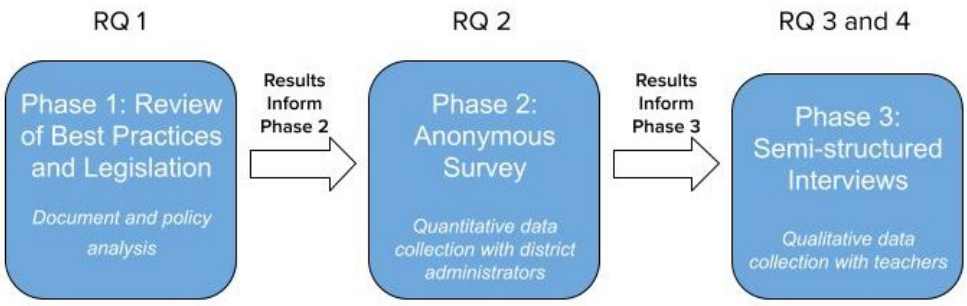
Phase 2, Chapter 4: Conduct an anonymous online survey among selected district-level administrators who monitor, secure, and share student data at the selected school district. This survey is intended to assess the current practices, gaps, and individual perceptions related to student data privacy (research questions #2).

Phase 3, Chapter 5: Conduct semistructured interviews with school-level teachers and technologists discussing: their shared experiences (research question #3), as well as enablers and barriers for effective student data privacy practices in schools (research question #4).

The three phases of the research study are sequential and build on previously collected data.

Figure 4

Exploratory Case Study in Three Phases



The alternative three-manuscript dissertation model is appropriate for this research because 1) the findings are relevant to practitioners who seek guidance and information related to emerging issues on student data privacy, 2) the format of the deliverables is more likely to benefit those who wish to focus on narrowly articulated results in a selected manuscript rather than perusing a hundred page plus thesis, 3)the case study is relevant to educators and researchers in Hawai‘i because of the State's unique statewide single school system, and 4) the selected research design, separated into three phases, fits well into the alternative model. Separately, the manuscripts address the research questions listed above. Collectively, the two articles and the conference proceeding explore the emerging practices, perceptions, and recommendations related to the increasingly important issue of student data privacy.

Research Design: Exploratory, interpretive case study

As an exploratory, interpretive single case study, the goal of this research is to understand "a contemporary phenomenon within its real-life context" in an educational K-12 setting (Yin, 2014, p. 13). Case study research calls for an in-depth analytical investigation of a single subject, such as an organization. Case study research can be either positivist or interpretive (Cavaye, 1996) and is fitting to study a phenomenon that has not been well defined and where "understandings of the contexts of action and the experiences of individuals in a single setting" is relevant (Darke et al., 1998), p. 280). Positivist research assumes an objective reality that exists independent of human interaction and works best as a deductive practice to test an existing theory (Orlikowski & Baroudi, 1991). Interpretative research, on the other hand, assumes that meanings are subjective and dependent on human interaction with the world. This type of research does not aim to generalize or test a hypothesis. Instead, researchers undertaking an interpretative approach strive "to understand phenomena through accessing the meanings that

participants assign to them" (Orlikowski & Baroudi, 1991, p. 5). Interpretative studies also develop a deep understanding of the structure of a phenomenon, thus focusing only on one or a handful of sites.

Case study research design is well suited for the selected conceptual framework because of its reliance on context. It allows for a study of a phenomenon in its natural environment where "the boundaries between the phenomenon and context are not clearly evident" (Yin, 2014, p. 23). As described in the background literature, concerns for student privacy grow alongside technological advancement creating a new phenomenon and requiring an in-depth understanding from a system-based approach. Following the recommendations of experts (Merriam, 1988; Stake, 1995; Yin, 2014), this case study will involve mixed quantitative and qualitative research and diverse data-generated methods. The qualitative data emerged in Phases 2 and 3 through a single open-ended question in the survey and semi-structured interviews. Quantitative data emerged in Phase 2 of the study collected through an anonymous online survey. With multiple units of analysis, this research presents an example of an embedded case study because of the distinct inquiry of subunits, that is phases. By giving attention and defining attributes to each subunit, the research design allows each phase to be embedded in the overarching inquiry with meaning and distinct contribution to theory (Yin, 2014). Table 1 offers a detailed representation of the research design and its alignment with the research questions.

Table 1

Three Phases Aligned with Methods and Research Questions

	Phase 1	Phase 2	Phase 3
Research Question(s)	RQ #1 What are the current trends in student data privacy as evidenced by diverse school district policies and legislation?	RQ #2 What are the perceptions and practices of district-level administrators, those with experience and knowledge in data governance, regarding student data privacy?	RQ #3 What are the experiences among teachers and school-level administrators regarding effective student data privacy? RQ #4 What are the enablers and barriers to implementation of student data privacy practices in the selected school district?
Data Collection	Legislation and Literature Review	Quantitative: Anonymous online survey	Qualitative: Semi-structured interviews
Data Analysis		SPSS descriptive statistical analysis	NVIVO thematic coding

I investigated a single statewide school district in Hawai‘i and its efforts to articulate, develop, and implement policies and practices related to student data privacy. Because this study focuses on a single site and aims to assess a new phenomenon on a deep, structural level, it is well-suited for an interpretative case study design. In the next section I describe the site and research context.

Research Context and Site

Hawai‘i

To understand Hawai‘i’s education system, priorities, and influences, it is important to situate the reader in Hawai‘i. Home to 1.4 million people, this beautiful chain of islands in the Pacific Ocean is known for its stunning landscapes and idyllic vacation sites, but there is far

more to Hawai‘i than meets the eye. Its unique geographic isolation, historical significance as an economic and geopolitical hub, as well as relatively recent annexation to the United States present a State that is entirely unique in its ecological, cultural, and ethnic diversity. The presence and perseverance of *kānaka maoli* culture can be heard in the state motto at public gatherings, seen at celebratory *luau* with dozens of multigenerational members of *‘ohana*, taken in through the sweet aroma of *pikake lei* at graduations, and uncovered in layers of meaning of Hawaiian place names. It is the only state in the Union with two official languages, Hawaiian and English (Encyclopedia Britannica, 2020). In addition to its indigenous population, Hawai‘i is home to descendants of Japanese, Pilipino, Mexican, Vietnamese, Chinese, European, American, and Micronesian immigrants, who arrived in waves as contract laborers during its agricultural booms. As generations of plantation workers bonded and formed families, Hawai‘i of today boasts one of the most diverse, multiethnic populations in the United States with 24% reporting as two or more races (by comparison, the U.S. population of two or more races is 2.7%) (U.S. Census Bureau, 2010). As much as 88% of Hawai‘i’s public school students identify as non-white and over 30% of these are of native Hawaiian ancestry (National Center for Education Statistics, 2015).

Geographically, sharing the common waterways are the seven islands of Hawai‘i: Ni‘hau, Kaua‘i, O‘ahu, Moloka‘i, Maui, and Hawai‘i (the island) (Encyclopedia Britannica, 2020). Some are close enough to be visible on a clear day but transportation from island to island is nevertheless limited to commercial flights or private boats. Most of the inhabited land of Hawai‘i is considered rural. In contrast, the city and county of Honolulu, O‘ahu (pop. 987,638) has more than double the population of all the other islands combined. Not surprisingly, Honolulu serves

as the social and economic hub of the State; however, each island presents its own cultural identity nurtured by centuries of relative isolation.

Hawai‘i is also home to socioeconomic extremes. While it ranks 3rd among the healthiest states in the nation, it came in at a not-so-great 34th place in high school graduation rates (United Health Foundation, 2019). Hawai‘i has the highest cost of living and the lowest wages in the country when adjusted for average income needed for financial stability (Hawai‘i Appleseed Center for Law and Economic Justice, 2016). Lack of affordable housing has led to some of the highest homelessness rates in the country, including for children (DeBaryshe et al., 2020). One other unique characteristic of the State is its education system. It is home to the only single-district statewide public education system in the country (Hawai’i Department of Education, 2021). Below, I discuss how the public school system in Hawai‘i presents a unique context for this research as a case study.

Hawai‘i Department of Education (HIDOE)

Hawai‘i’s families opt out for private school enrollment at higher rates than elsewhere in the country with 14.5 percent of school-age children in the State attending private schools while the U.S. average is at 10 percent (Hawai‘i Department of Education, 2021; National Center for Education Statistics, 2015). Because of the high costs of attendance, students attending private schools come from overwhelmingly middle- and upper-class families, leaving the public school system with 47 percent of students from socioeconomically disadvantaged families (Hawai‘i Department of Education, 2021).

The State’s public school system is unique in its own right. For purposes of federal reporting and designation, Hawai‘i Department of Education (HIDOE) operates both as a State Education Agency (SEA) and Local Education Agency (LEA) (U.S. Department of Education,

2017). Article X of the Hawai‘i State Constitution established Hawai‘i State Board of Education (BOE) as the policy making entity of the K-12 public education system. The Superintendent of Education, appointed by BOE, serves as both the Chief State Education Officer and organizational lead of HIDOE with direct authority over more than 20,000 administrative and teaching personnel (U.S. Department of Education, 2017).

Because of its statewide reach, HIDOE is the 10th largest school system in the country with close to 180,000 students and a total of 293 schools, including charter schools (Hawai‘i Department of Education, 2019; U.S. Department of Education, 2017). The typical challenges of managing a large district are exacerbated by the State's geographic distribution across the islands. Consequently, HIDOE is divided into seven districts (used for internal classification and not considered separate districts for the purposes of federal reporting), 15 complex areas (CA), and 41 complexes. Detailed distribution of the school system is presented in Table 2.

Table 2

Distribution of HIDOE Complex Areas across the State of Hawai'i

Island	District	Complex Area
O'ahu	Honolulu	Kaimuki-McKinley-Roosevelt
		Farrington-Kaiser-Kalani
	Central Oahu	Leilehua-Mililani-Waialua
		Aiea-Moanalua-Radford
	Leeward Oahu	Pearl City-Waipahu
		Nanakuli-Waianae
		Campbell-Kapolei
	Windward Oahu	Castle-Kahuku
		Kailua-Kalaheo
Hawai'i	Hawai'i	Kau-Keaau-Pahoa
		Hilo-Waiakea
		Honokaa-Kealakehe-Kohala-Konawaena
Maui	Maui	Baldwin-Kekaulike-Maui
		Hana-Lahainaluna-Lanai-Molokai
Kaua'i	Kaua'i	Kapaa-Kauai-Waimea

Complex Areas are led by Complex Area Superintendents who "oversee personnel, fiscal and facilities support; monitor compliance with applicable state and federal laws; and oversee curriculum development, student assessment, and staff development services – all with the goal of increasing student achievement" (U.S. Department of Education, 2017, p. 13).

As a unique school system, HIDOE presents an ideal site to lead to rich, contextual, and in-depth data for this exploratory case study (Eisenhardt, 1989). The participants are administrators and educators who operate at the district and school levels and whose professional responsibilities include one of the following: securing, monitoring, distributing, interpreting, or

managing student data within the boundaries of the existing laws and policies. The sample of participants selected for the study was purposive and diverse to generate information-rich cases using limited resources and to allow for selection of participants who are particularly knowledgeable about the phenomenon (Cresswell & Plano Clark, 2011; Patton, 2001). Because the case study looked at a single, closely interrelated organization and progressed in phases, snowball sampling was also utilized to generate social knowledge that is emergent and interactional (Noy, 2008). Data Governance Office contributed to the selection of participants because of their close work with units and personnel that fit the participant criteria.

The 15 complex areas have relative autonomy with separate budgets and leadership. As such, HIDOE functions as a tri-level system organized by school level, complex area level, and state/district level. As will be discussed in the findings, this unique organizational structure may serve as a barrier for effective student privacy practices because complex areas are not under regulatory pressure to comply yet they often operate with autonomy of a school district.

The HIDOE Data Governance and Analysis (DGA) office oversees district-wide data sharing and data governance processes, including: 1) a process through which schools can propose and contract with a third-party vendor; 2) conditions that would necessitate a data sharing agreement (DSA), such as exposure of student PII; 3) identification of personnel, such as principals or superintendents, who are authorized to sign a DSA; and 4) minimum security standards for data storage, deletion, and sharing. DGA serves as an intermediary to draft and negotiate data sharing agreements with Ed Tech vendors on behalf of the school, complex area, or the district. The DGA office's work is limited by its size with only two full-time employees overseeing student privacy and data sharing tasks for the entire district. Schools or complex areas may designate liaisons to collaborate with the DGA office on student privacy issues; however,

these positions are not mandated or officially designated. The DGA staff are also responsible for statewide trainings on student privacy and research-related data sharing.

In the next three sections I describe in detail the methodology for the three manuscripts, presented in the dissertation as Chapters 3, 4, 5.

Manuscript 1: Review of Legislation and Best Practices

Manuscript 1 (Chapter 3) is a culmination of Phase 1 of this research, focusing on literature review of publications and legislation on the issue of student data privacy and educational technology. Manuscript 1 addresses RQ #1: *What are the current trends in student data privacy as evidenced by school district policies and legislation related to student data governance?* This phase of the research contributes to the context of the case study.

The manuscript delves in depth into a number of interdisciplinary topics related to privacy, law, ethics, and educational technology to provide background and context to the study. It offers a bird's eye view of the national landscape in student data privacy, trends and best practices, and the current policies related to internet safety and student privacy at the selected school district. The manuscript concludes with identification of persistent gaps and issues related to the topic. It is important to note that this review does not amount to empirical data collection or policy analysis, and instead, is intended to contextualize, give background information, and situate the case study in the larger paradigm (Eisenhardt, 1989; Yin, 2014). Systematic policy analysis is a well-established research method requiring a thorough assessment of implementation, evaluation, and articulation through thematic coding (Walt & Gilson, 1994); however, this is not the intent of the manuscript. Phase 1 did not involve empirical qualitative policy analysis. Instead, this case study derived its empirical data in other phases.

Selection Criteria.

Because student data privacy remains a new phenomenon with evolving definitions and issues, the selection criteria was broadened to incorporate the most up-to-date information using empirical studies as well as law review journals, reports, reputable news publications, expert opinions, and advocacy groups. These publications contributed to examination of the following topics: defining privacy and data ownership; threats to information privacy in the digital age; educational technology and data sharing; ethical considerations in the use of technology in schools; data vulnerabilities in schools; and national trends and best practices.

In addition, the selection criteria included federal and state laws and policies on the issue of student data. These include federal laws, such as Family and Educational Rights and Privacy Act (FERPA), Privacy Act of 1974, Children Online Privacy Protection Act (COPPA), Federal Trade Commission Act (FTC Act), Children's Internet Protection Act (CIPA), and Protection of Pupil Rights Amendment (PPRA), which collectively, are considered key protections for student data privacy by school districts and nonprofit organizations (Elliott et al., 2014; National Forum on Education Statistics, 2016; Student Privacy Compass, n.d.-a).

State laws play a lesser but nevertheless important role in student data privacy. Because federal legislation lack comprehensive standards for digital and online environments, 40 states, including Hawai‘i, have passed laws that grant additional protections to student records (Student Privacy Compass, n.d.-b). The manuscript discusses the general trend of the state legislation on the issue of student privacy and educational technology, as well as some specific laws leading the nation in comprehensive legislative mandates (Future of Privacy Forum, 2016). In addition, the chapter covers two laws recently enacted in Hawai‘i: Student Online Personal Information Protection Act (2016) and Uniform Employee and Student Online Privacy Protection Act (2021).

Finally, I reviewed existing Hawai‘i policies related to student data privacy enacted by the Board of Education and are publicly available on its website (State of Hawai‘i Board of Education, n.d.). It is important to consider how state and local agencies develop and implement student data privacy policies and practices in order to inform subsequent phases of the case study. The selection is aligned with the conceptual framework as this data will help connect to the *Rules* element of the activity theory system (Engeström, 1987) and the *Transition Principles* element of the contextual integrity framework (Nissenbaum, 2010), see Figure 2 above. Nissenbaum's framework (2010) helps further to understand *Rules* as explicit norms, such as legislation, and implicit norms, such as established but not codified practices; for example, data sharing agreement templates and employment of the data privacy officers.

The diverse set of laws and policies reviewed in Manuscript 1 provide a rich contextual understanding of what drives the school leaders' perceptions and practices in relation to student data privacy. The criteria also represented a variety of contexts from broad to narrow - federal, state, district - creating a cross-sectional selection.

Document Collection.

Legislation and policy documents collected during Phase 1 were publicly available through online resources. Public school district policies, state and federal regulations, and legislation must remain publicly viewable as part of the federal and state open records laws and can be found on government-administered websites (SOPIPA, 2014; State of Hawai‘i Board of Education, n.d.; U.S. Department of Education, 2016). Summaries and interpretations of privacy laws are also publicly available through nonprofit organizations, such as Student Privacy Compass, the Student Data Privacy Consortium (SDPC), Future of Privacy Forum, Data Quality Campaign, and Electronic Privacy Information Center (EPIC), among others. SDPC, in

particular, is an important resource for collecting up-to-date data as it represents a collaboration of "schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns" (Student Data Privacy Consortium, n.d.). SDPC serves as a convenient, one-stop resource to access state laws and school district policies on student data privacy, with 26 state alliances as members. Future of Privacy Forum provides a comprehensive, curated list of state and federal legislation related to student data privacy (Future of Privacy Forum, 2020).

Document and Legislation Review.

Exploration of the current legislative mandates and best practices grounds the study in the conceptual framework by addressing the rules and context that influence the phenomenon. Documents can serve a valuable role in case studies (Bowen, 2009) helping to "uncover meaning, develop understanding, and discover insights relevant to the research problem" (Merriam, 1988, p. 118). In this manuscript, I synthesized the selected legislation not only for clarification of the law but also for context in which the law has emerged, such as political and social influences, history of the current rules, and proposed reforms (Linos & Carlson, 2017). It is equally important to understand the law's potential for enforcement and implication for violations. In the context of the current study, school districts are responsible for student data privacy but may be subject to different enforcement and liability depending on state legislation. For example, when a provider of educational services commits a data breach exposing sensitive student information, the school system may be fully liable for the breach despite following proper safeguards (Haduong et al., 2015).

Policies can provide further contextual data and background information for a particular research topic. Identification of best practices and existing gaps in policies helped articulate the design of subsequent phases of the case study. Finally, document analysis can be useful in tracking issue-related change and development (Bowen, 2009). As such, I used information drawn from Phase 1 to identify best practices for student data privacy in K-12, to examine persistent gaps in student data privacy framework, to inform questions asked in the subsequent phases, and to contextualize and corroborate data that emerged in the case study.

Table 3

Roadmap with Corresponding Sample Policy Clauses and Conceptual Framework Alignment

Conceptual Framework Alignment	Sample Policy Clauses
Context Community	1. Student data policy is publicly available via SEA website 2. Availability in multiple languages to meet the state population 3. Clear and documented process for receiving and resolving complaints about the use of student PII
Subject Actors Division of Labor	1. Established executive-level support for data governance 2. Ongoing and regular professional development and training for all SEA staff 3. Data privacy and governance orientation for contractors and vendors with access to student data
Rules Tools Object	1. Documented data retention policy with expiration dates and destruction process 2. Regular vetting of approved vendors using data sharing agreements 3. Documented policies for handling privacy incidents

To deeply engage with the documents, I conducted several readings of the material and organized emerging patterns according to the roadmap to help identify trends, gaps, and best practices. An important element of this review is also to identify the availability or incompleteness of documents. Going beyond content, the presence or absence of documents reveals implicit norms, for example, types of resources posted on the website, ease of access, contact information for relevant personnel, among others.

Phase 1 provided context and background information serving an important role in a case study design (Yin, 2014) resulting in a manuscript presented in Chapter 3. With a contextual understanding of what influences district administrators, I continued to the next phase of the research assessing perceptions and practices at the district level.

Manuscript 2: Assessing Perceptions and Practices through Online Survey

Manuscript 2 (Chapter 4) utilized quantitative survey research at the selected school site. This phase revealed an empirical assessment of the perceptions and practices of district-level administrators at HIDOE, addressing Research Question #2: What are the perceptions and practices of district-level administrators, those with experience and knowledge in data governance, regarding student data privacy?

The data was triangulated to validate responses. First, a brief consult with a district representative confirmed which personnel and departments were best suited to provide responses to the anonymous online survey. Second, the survey link was sent to departments and participants identified at the consult. Third, after compiling the results of the survey, I had a second consult with a representative of HIDOE to compare whether the responses matched policies that were in place at HIDOE. By looking at practices and perceptions of district

administrators, Phase 2 delved into site-specific findings of the case study tied closely to the conceptual framework.

Participants

The participants in Phase 2 were district-level administrators whose professional responsibilities included: securing, monitoring, distributing, interpreting, or managing student data. I also requested participation of institutional analysts and other personnel who contribute to policy development related to student data and privacy. The sample selected for the study was purposive to generate diverse perspectives from complementary but distinct organizational units. I also utilized snowball sampling to generate social knowledge that is emergent and interactional (Noy, 2008). With limited resources, selection was focused on personnel who are knowledgeable about the particular phenomenon (Cresswell & Plano Clark, 2011; Patton, 2001).

I have identified the following departments that work closely with privacy, data management, and data security: Monitoring and Compliance Branch; Office of Curriculum and Instructional Design (specifically, Learning and Technology Section); Office of Strategy, Innovation, and Performance (specifically, Data Governance and Analysis (DGA) Branch; Policy, Innovation, Planning and Evaluation Branch); and Office of Information Technology Services. I narrowed participants to those with director, analyst, or education specialist classifications. After receiving the IRB approval, I conducted a brief consult with the DGA office to confirm the proposed participants, and to either expand or narrow down the list of participants accordingly. Overall, the estimated number of district administrators who received the email was 76, with 37 participants who either submitted or started the survey. The number of surveys with a complete dataset for this study was 28.

Instrument

Data were collected using an online anonymous survey. The instrument created for the survey was based on a publicly available online self-assessment questionnaire created by the Consortium for School Networking (CoSN) for the Trusted Learning Environment (TLE) seal. The questionnaire was designed to assess whether school systems had sufficient student data privacy safeguards to qualify for the TLE Seal. The TLE Seal Program was developed by a "collaboration with a diverse group of 28 school system leaders nationwide" (Trusted Learning Environment, n.d.-a, para. 1). School systems across the country may apply and qualify for the seal if they meet the high standards of student data privacy in the areas of: leadership, business, data security, professional development, and classroom. Receiving the Seal signifies that the school system has implemented both policies and procedures with a commitment to continuous protection of student privacy.

The online survey had 38 questions: 37 are closed-ended questions with 1 open-ended question to capture additional comments and to support the triangulation of data. Of the closed-ended questions, 22 are scaled to measure practices and 13 are scaled to measure perceptions. The final 2 questions collect participants' background information in alignment with the conceptual framework. Most questions elicit responses on a 5-point scale: 1 (strongly disagree), 2 (somewhat disagree), 3 (neither agree or disagree), 4 (somewhat agree), and 5 (strongly agree). Positive responses (Somewhat Agree or Strongly Agree) represent higher level of compliance and positive perceptions. Questions that received a high mean score indicate that the district is doing well in that area, while questions with a lower mean score suggest that there is room for improvement.

In addition to the 5-point scale, questions measuring practices allowed for a 'Don't Know' (DK) response to assess knowledge gaps (Durand & Lambert, 1988). Survey instruments commonly include a DK option as an opportunity for respondents to provide an honest assessment of their knowledge level, particularly within organizational settings (Krosnick & Presser, 2010). For questions related to school practices, which may require specialized knowledge, the DK option was available to avoid a guessed response and to measure gaps in knowledge among the participants. In contrast, the DK option was not included in questions measuring perceptions to encourage participants to formulate a meaningful answer based on their experiences or attitudes (Krosnick & Presser, 2010). A single open-ended question was included to capture additional comments and sentiments and to add richness to the survey results (Krosnick & Presser, 2010).

The original TLE questionnaire was modified to offer an insight to the Research Question #2 and to align with the conceptual framework to measure not only explicit norms of an organization, such as policies, but also to examine implicit ones that represent perceptions, departmental culture, and behavior that are not formally codified or mandated (Nissenbaum, 2011) For example, the questions revealed the role of *Tools* ("The school system has implemented a vetting process for online services by outside vendors for data privacy and security") and *Community* (example: "Parents are offered appropriate awareness training and resources about student data privacy and security"). A copy of the consent form and survey questions is attached as Appendix B.

Data Collection

The anonymous online collection of data was intended to encourage openness that may not be attained in face-to-face conversations. Online surveys also serve a convenient and

efficient method for collecting quantitative description of trends, behaviors, or opinions by studying a sample of the population (Creswell, 2014). Qualtrics survey software was used to design the survey and to collect data. The first page of the survey included the informed consent with a checkbox to indicate consent.

The survey was then distributed via email with 1) an initial invitation to participate, and 2) a reminder notice. The participants were asked to respond within a 10-day period. During pilot testing, the survey was estimated to take no more than 15 minutes to complete.

Data Analysis

After the survey window closed, the data was exported into Excel spreadsheet with one copy saved as a backup on a password-protected computer, a copy saved in Qualtrics, and another copy imported into SPSS. Using the Qualtrics survey duration tool, I assessed that the average time for survey completion among the participants was 9 minutes. A total of 37 responses were recorded. I reviewed the dataset to remove 9 entries that were incomplete either because the participants consented to the survey but did not respond to any questions, or answered to fewer than 10 questions. The final dataset included 28 complete responses. I coded the responses with a 1-5 scale, assigning 1 to ‘Strongly Disagree’ and 5 to ‘Strongly Agree’ as commonly used in Likert scaling (Krosnick & Presser, 2010). Responses marked DK were assigned a distinct number 99 to exclude these responses from mean and standard deviation calculations (Durand & Lambert, 1988). The final analysis of the data included data frequency, measures of central tendency, and variability. Using Excel visualization tools, I present the findings using tables and graphs for ease of use and access.

Manuscript 3: Assessing Drivers and Barriers to Student Data Privacy

The third, and last, phase of the research in presented here in Chapter 5 describing perspectives on student data privacy from teachers and technology coordinators who support Ed Tech integration in schools. This section of the study will address Research Questions 3 and 4: *What are the experiences among school-level administrators regarding effective student data privacy? What are the enablers and barriers to implementation of student data privacy practices in the selected case study district?* This phase and the resulting manuscript comprise qualitative empirical research of the case study looking at school-level perspectives in the HIDOE.

Participant Selection

Five participants volunteered to be interviewed for the study. The participants included 2 school teachers and technology coordinators, 2 complex area technology resource teachers, and 1 complex area school renewal specialist (responsible for Ed Tech integration for the complex area). The sample selected for the study was purposive to generate perspectives from educators and technology experts who support schools with educational technology implementation. I also utilized snowball sampling to generate social knowledge that is emergent and interactional (Noy, 2008). The selection was focused on participants who are knowledgeable about the particular phenomenon (Creswell & Plano Clark, 2011; Patton, 2001). All five participants work on the island of Oʻahu.

The criteria for participation required that the participants: 1) be employed at HIDOE, the selected case study site, and 2) provide support and guidance for educational technology at school level. The criteria were aligned with the case study to respond to the proposed research questions and to generate overall exploration of student data privacy at the district. Four participants were members of the Hawaiʻi Society for Technology in Education (HSTE). School-

based participants were responsible for supporting teachers, administrators, and students at their respective schools. Participants employed at the complex area level supported teachers and administrators for the complex area.

Participants were recruited through HSTE. The HSTE board invited me to talk briefly about the study and its impact. After the presentation, an interview sign-up link was distributed to the HSTE members articulating criteria for participation, and options to select a time and date for the interview. The email invitation included IRB approvals and the consent form.

In qualitative research, participants are part of the descriptive narrative, and as such, their stories should be associated with identities beyond the anonymity of a code or a number (Seidman, 2006). Finding pseudonyms for participants is a "sensitive task" that needs to take into consideration participants' identifying attributes (Seidman, 2006, p. 9). For this study, the names of the participants have been replaced by pseudonyms consistent with their gender. Other identifying elements, such as school name or location, are not attributed to them to maintain confidentiality. The pseudonyms used are Carmen, Tasha, Hoku, Kanoe, and Mario.

Instrument and Data Collection

The primary instrument in semi-structured interview research is the researcher (Chenail, 2011). The researcher's facilitation with the interviewee sets up the flow of communication and prompt cues allowing for rich data to emerge. When performing as an instrument, the researcher's role is to construct open-ended questions that "provide openings through which interviewees can contribute their insiders' perspectives with little or no limitations imposed by more closed-ended questions" (Chenail, 2011).

Data for this qualitative study was collected through five 60-minute semi-structured interviews in May-June, 2021. The interviews took place online using Zoom platform. After

introduction of the study, participants were asked eight semi-structured questions with clarifying questions in between. The questions were informed by the supporting literature and were open-ended to encourage in-depth participation and elaboration on details relevant to the research questions (Seidman, 2006). The participants were asked to return the signed consent form prior to the interview. At the time of the interview, participants were asked to confirm consent to be audio recorded for transcription purposes only. The audio recordings were done on the researcher's laptop using licensed Otter.ai transcription service, which stored an mp3 audio files on the laptop hard drive.

While there are limitations with conducting research in virtual spaces, there are some clear advantages, such as overcoming geographical barriers, convenience, and participants' control over of the interview space (Nehls et al., 2015). Furthermore, at the time of data collection, the University IRB office had imposed limitations on in-person research and HIDOE meetings have been moved to virtual environments due to the global pandemic. Interview protocol and questions are presented in Appendix C.

Data Analysis

The audio recordings of the interviews were auto-transcribed using Otter.ai software. To ensure confidentiality and to minimize my bias, I began with assigning pseudonyms to participants and continued to use them throughout the analysis and reporting. Each interview was coded separately because semi-structured interviews empower participants to diverge from the guided questions and find meaning based on their experience (Dearnley, 2005).

As the primary researcher in all three phases of the study, the thematic coding was influenced by previous findings and the focus remained on "securing student data" in this object-oriented study. I listened to the audio recordings and made corrections to the transcriptions,

adding nonverbal cues. Transcriptions were re-read again for accuracy and emergence of themes (Creswell, 2014). Each transcription was subsequently uploaded to NVIVO data analysis software and coded and recoded to reveal emerging themes in alignment with the research questions and conceptual framework. Coding was done in two schemes to correspond with the guiding concerns of the two research questions. First, the responses were coded to identify themes for the experiences of participants in response to Research Question 1. Second coding scheme was based on the reported barriers and enablers to implementation of student data privacy safeguards, which corresponded to Research Question 2. This method of thematic analysis offers a flexible research tool for researchers who are new to qualitative research and generates unanticipated insights (Braun & Clarke, 2006). It is also an appropriate tool for exploratory research as it can be useful in informing policy development. To help relay the richness and meaning of the data, direct quotations that represented the emerging themes were pulled and included in Findings and Discussion sections (Seidman, 2006).

Finally, synthesizing the aggregated results from the literature and legislation review, survey, and interviews was important in preparing the concluding Chapter 6 of this dissertation.

Research Approval

Before data collection, this research was approved by the University of Hawai‘i Institutional Review Board (IRB) and the HIDOE Assistant Superintendent of Office of Strategy, Innovation & Performance. The overall research approval process took over 7 months and was complicated by the COVID-19 restrictions, which significantly limited in-person data collection and the organizations’ capacity for research approvals. Research approval letters are attached as Appendix D.

Rigor and Bias

Case studies can be susceptible to a lack of rigor because they typically examine new or unexplored phenomena, and the relationship between variables have limited grounding in prior research (Yin, 2014). As such, it becomes important to prioritize and ensure internal validity over generalizability. With three distinct phases, I triangulated results from the empirical and non-empirical data to corroborate findings. Supporting evidence from Phase 1 helped minimize bias and establish credibility. In selecting documents for review, I identified why each document was selected, what purpose it served in the overall research design, the context in which the document was produced, and its intended audience (Bowen, 2009). As a subjective interpreter of legislation and school policies, I corroborated my interpretation through best practices identified by government and non-profit organizations. While the quantitative survey instrument has not been validated, the items and categories were adapted from an existing assessment designed by school leaders who are similarly positioned as the participants. Each item has been carefully selected and was subjected to review by subject matter and assessment experts.

Prior to distribution, the survey was pilot-tested with individuals with education or data management expertise to assess the clarity of questions and the dimensions of the survey. The survey was also pilot-tested with a senior level administrator at the selected school district on how well the questions were aligned with the district's organizational structure and internal terminology. The survey was revised after pilot-testing.

The questionnaire was not previously validated, and despite considerable effort, the search to locate a valid instrument to measure the inquiry was unsuccessful. Some studies have assessed perceptions of data privacy, but these surveys were designed to measure personal thoughts about one's own privacy (Apthorpe et al., 2019; Preibusch, 2013; Shvartzshnaider et al.,

2016), or the opinions of privacy experts (Smith, 2016). Instances in which no validated instruments are available, the researcher may design and assess the instrument validity and reliability (Sullivan, 2011). To confirm the validity of the questionnaire, I invited two people with expertise in data management and data analysis to review the instrument. The Cronbach's alpha was run to confirm reliability on the Likert-scaled items after the data were collected, see Table 1. The Cronbach's alpha came back at a strong .914 supporting internal consistency and reliability (Sullivan, 2011).

To confirm credibility of the qualitative data, the interview prompts were tested with faculty and data governance experts to ensure they are worded neutrally and sequenced properly to minimize misunderstanding (Stewart & Shamdasani, 2014). Furthermore, using the same interview protocol and time limit for all five interviews ensured consistent facilitation in each session. During the coding process, I returned to the previously coded transcript after a period of time (about 1 week) to check the validity and consistency of the emerging themes.

It becomes evident by the selected research design and the conceptual framework that underpins this research, my epistemological orientation falls squarely on the side of constructivism in an attempt to find meaning through social roles, norms, and context. As a result, the subtle but consistent bias in this study was the researcher's belief in social constructions of Self as well as group behavior and dynamics. In addition, my training in law may have affected the findings by interpreting and analyzing through a legal lens.

Researcher's Role

When I began research on this topic, the looming issues with data security were already perceived as one of the top operational concerns in the private sector (De Hert et al., 2018; Kaufman, 2009). However, public school systems largely relegated data security and privacy to

the purview of information security and compliance administrators. Fast forward to spring 2020 when the COVID-19 pandemic necessitated a global move to virtual learning, student privacy issue became one of the most controversial topics in K-12 education (Diliberti & Kaufman, 2020). My role as a researcher had to change accordingly. First, I recognize that I must be fully transparent in how this research is disseminated protecting anonymity and confidentiality of the participants who are employed at the only school district in the state. My role had to remain and be perceived as unbiased because the education agency may have been dealing with unanswered questions and public outpouring of concern on the issue of student privacy. At the same time, I had to establish rapport without being too technical or too involved (Merriam & Tisdell, 2015).

Given the context of Hawai‘i and its culture of connectedness, it was important to introduce myself both professionally and personally, and to discuss my connection to Hawai‘i and to HIDOE. My training as a lawyer and professional background in and education may have helped establish trust and credibility in the research and the selected topic. However, it may have also stifled frank responses during the interviews when discussing relevant laws and regulations. Also, prior to data collection, I was employed temporarily at HIDOE Data Governance and Analysis Office (DGA) district office, during which I met some of the participants.

Limitations

The primary limitation of this study traces its roots to the very nature of case studies: It is limited in scope and may not be generalizable because the data are associated with a single school system. Further, the analysis of the existing policies may not be indicative of the most up-to-date practices if the policies are amended after the data collection stage. Similarly, both federal and state laws may shift rapidly in light of the increased dependence on online learning environments and subsequent security threats. The political landscape during Covid-19 epidemic

will likely have a dramatic impact on how educators and key stakeholders implement future policies related to student data privacy. By the time this dissertation enters the University's ScholarSpace repository, my research may already be obsolete. Also, the questions posed to participants may alert them to the gaps in practices and lead to proactive changes before the dissertation is published.

The survey responses, document accessibility, and interview responses may lack full transparency because data privacy and security practices are increasingly scrutinized by community organizations and parent groups. Because the results of the study will be published and publicly available in the University's digital repository, the participants may have restricted their responses so as not to expose gaps in the existing practices. The interviews were impacted by my personal bias, reflected in the tone, questions asked, and selection of data from Phases 1 and 2. Furthermore, a virtual interview lacks perceptible body language and social cues that generally aid in social interactions. Because of the limited resources, the research did not cover every agency and department that receives or shares student data, of which there are many (for example, the Board of Education, Department of Health and Human Services, internal auditors, just to name a few). Furthermore, the inquiry was limited to student data even though school districts also collect diverse personal information related to employees, contractors, and parents, and such data may be governed by alternative data privacy considerations.

Significance of the proposed body of work

Collectively, the three manuscripts have meaningful theoretical and practical implications in the field of student data privacy. For the theoretical framework that informs this study, the findings help identify additional or existing subunits of a system. Defined as an activity system, the results showcase the relationship and interconnectedness between laws, policies, as well as

perceptions and practices of school administrators in diverse roles. One of the challenges in policy effectiveness is implementation. In examining school administrators' perceptions and practices as part of an activity system, the study brought to the surface some of the barriers to implementation. Furthermore, because issues with data privacy typically outpace academic research, this research contributed to the urgent need in understanding privacy in educational context.

For practitioners in Hawai‘i and beyond, the results of the study offer relevant information on the nascent but critical issue of safeguarding student privacy. Manuscript 3, in particular, is intended to be shared widely through a conference proceeding and a presentation in Hawai‘i. Finally, because of Hawai‘i's unique political environment and its statewide school system, this dissertation may even further additional legislative state reforms to protect privacy of students in the digital era.

Product

In addition to the three manuscripts presented as Chapters 3-5, the empirical product of the three phases is organized and delivered through tables and other visual representation. Quantitative data are displayed as descriptive statistics in tables and charts. Qualitative data resulting in codes and themes are organized in a table as well.

Key Terms

Big Data. Large volume of varied personal information that can be systematically analyzed, operationalized, and commodified for marketing and other purposes (Zuboff, 2019).

Data. Information systematically collected from or about students and their parents and digitally stored (Chapple, 2019).

Data governance. A process of data management in a school system with the aim of maintaining consistent, reliable, accessible, and secure data; based on internal standards and policies unique to the organization (U.S. Department of Education, Privacy Technical Assistance Center, 2015).

Data stewardship. Organization's practice and commitment to ensure that education data: are accurate and complete; are collected, maintained, and used properly with respect to privacy and confidentiality; accessible for evaluation of educational progress and programs (National Center for Education & Statistics, 2010).

Educational Technology (Ed Tech). Computer software, mobile applications (apps), and web-based tools provided by a third-party vendor to a school or district that students, parents, teachers, or administrators access via the Internet and use as part of a school activity or for administrative purpose (U.S. Department of Education, Privacy Technical Assistance Center, 2014).

Personally Identifiable Information (PII). Information that can be used to identify a student or trace their identity by linkage with other information, such as student's or parents' names, address, Social Security Number, and other unique identifiers (National Center for Education & Statistics, 2010)

School-level administrator. School administrator who supports one or more schools and is responsible for policy implementation at school level.

District-level administrator. Administrative personnel employed at school system level and whose work has districtwide impact.

Summary

The gravity of potential data breaches, lawsuits, and political backlash, is creating a country-wide concern among educators for urgent protection of student privacy. Educational technology has allowed for improved pedagogies in reaching student learning outcomes and accountability, and the state and local education agencies strive for a consistent, secure, and uniform practice of data sharing and data governance. The intention to protect student privacy is present among all stakeholders who are invested in public education. The persistent issue, however, is that practices in protecting student privacy are not always aligned with these intentions, often resulting in perceived disregard for privacy, or worse yet, unauthorized data breaches.

This relevant and timely case study explored this issue through an in-depth research of a single but complex school district. By looking at the perspectives and practices among diverse district-level administrators, followed by interviews with school-level personnel, the results of this study contribute to the body of research on the topic of student data privacy and educational technology. Moreover, the study may help shed light on the gaps in the existing national and state legal frameworks and generate valuable data for state policymakers.

CHAPTER 2. LITERATURE REVIEW

The literature review for this study discusses in depth a number of interdisciplinary topics related to education, law, ethics, and technology that provide background and context to the study. Because of the rapidly evolving definitions and issues related to digital privacy in education, I gathered information empirical studies as well as academic journals, case law, current events, expert opinions, and online-based advocacy groups. The topics included in this literature review are: understanding privacy through legal and societal lenses; legislation related to student data privacy; collection and sharing of student data through technology; and the conceptual framework.

The issues brought to light by this study have been typically addressed in separate, distinct fields without significant overlap. For example, legal experts have covered many issues related to privacy law (Angwin, 2014; Ataei, Degbelo, Kray, & Santos, 2018; DeVries, 2003) but few of them address privacy within education (Zeide, 2015). Similarly, educational journals examine ethical issues related to the use of technology in schools but not specifically formal legal implications within a K-12 environment (Bowers, Bang, Pan, & Graves, 2019; Ifenthaler & Schumacher, 2016a; Slade & Prinsloo, 2013; Yeaman, 2015). My goal in this Chapter is to gather sources that are relevant to the study and to highlight the gap in research specifically related to student data privacy in K-12 education.

Understanding Privacy through Sociocultural and Legal Doctrines

One of the key considerations in data privacy research is defining what constitutes privacy. Depending on the country's legal system and its cultural norms, privacy definitions can range from the right to be left alone (Warren & Brandeis, 1890) to the right to control and to

limit personal information (Bygrave, 2014; Heath, 2014a; Solove, 2004)**.** While the U.S. Constitution does not explicitly guarantee an individual's right to privacy, American jurisprudence has gradually developed a set of protections under 'privacy' doctrine using various legal disciplines, such as common law, torts law, constitutional law (as interpreted in Supreme Court cases), and multiple state and federal statutes (Solove & Schwartz, 2018). This section aims to outline how privacy is conceptualized both as a sociocultural phenomenon and as a legal doctrine.

Privacy as a Sociocultural Concept

What defines the boundaries of privacy depends greatly on the cultural norms of a particular country (Bygrave, 2014). In the U.S., the traditional discourse on privacy frequently has revolved around the "secrecy paradigm," meaning people deem information that is not publicly available as private and all other information as open (Richards & Hartzog, 2016). This concept is best represented by an image of privacy visualized as a padlock or a shut door, while invasion of privacy is represented by an eye peeking inside a home. However, the ease of aggregation and transfer of data between different contexts has given rise to new, more comprehensive theoretical definitions of privacy. An alternative conceptualization of privacy has emerged in recent years that recognizes a person's right to control and to use information even if that information is not inherently "secret" (Bennett & Raab, 2006; Solove, 2004). As Solove (2004) argues, the secrecy paradigm is a simplistic, binary view that does not always represent the reality of our expectations. For example, while buying over-the-counter medication is done in public, a person making the purchase would likely expect this activity to remain confidential. In other words, information does not have to be secret for there to exist an expectation of privacy.

Going beyond the secrecy paradigm demands that we recognize information not simply in a vacuum but within a context.

Establishing Privacy as a Constitutional Right

Despite common misconception, the U.S. Constitution never directly guarantees the right to privacy even though several key cases infer Constitutional protections against government infringement on privacy (McWhirter & Bible, 1992). The U.S. Supreme Court has interpreted the Fourth and Fourteenth Amendments to include reasonable expectation of privacy (*Griswold v. Connecticut*, 1965; *Roe v. Wade*, 1973; *Whalen v. Roe*, 1977). The Fourth Amendment focuses on an individual's expectation of privacy against unreasonable searches and seizures (U.S. Const. amend. IV), while the Fourteenth Amendment was interpreted to grant privacy rights through substantive due process (U.S. Const. amend. XIV). *Griswold v. Connecticut* (1965) established the right to marital privacy overturning the Connecticut law that criminalized the use of contraceptives. Using the Fourteenth Amendment, the Court argued that Connecticut had violated the couple's substantive due process right by infringing on their privacy. Another important decision *Whalen v. Roe* (1977) extended the right to privacy to encompass security of personal information. This case became the source of informational privacy doctrine in the U.S. jurisprudence (Brkan & Psychogiopoulou, 2017). However, one of the key limitations of the Constitutional protection of privacy is that it applies solely to governmental intrusions. In a digital age when private entities own and control massive amounts of information, the constitutional precedents offer little protection against unauthorized exposure of private information by private actors.

Privacy Defined by Context

Defining privacy within a context is driven by how much control of information the person can exert on personal information rather than by a public-secret dichotomy. When data is taken out of context, people feel a violation of privacy even if they have agreed to sharing this information elsewhere. Nissenbaum's (2010) approach breaks away from the traditional doctrine of privacy which characterizes information as sensitive by its properties regardless of how and with whom it is shared (Heath, 2014b). As cultural and ethical norms evolve, so does our concept of privacy, and effective understanding of privacy requires a consideration of both the interests of affected actors and the contextual values (Nissenbaum, 2011). Consistent with the contextual integrity theory, a study by Ifenthaler and Schumacher (2016) showed that students who shared their personal information on social media platforms were overwhelmingly opposed to the use of that data in learning analytics because it was outside of the intended context.

Threats to Information Privacy in the Digital Age

The laws have not kept up with the digital world because we have very little knowledge of how our personal data is being used and we lack control over this data (Nissenbaum, 2009; Solove & Schwartz, 2018). Personal data is continuously recycled and reused from such sources as governmental public records, online browsing history, and purchasing preferences, among others (Solove, 2004). The trajectory of data transfer is cyclical from the government, to private entities, between private entities, and back to the government for background checks and investigations. The value of such exchange lies in how companies and the government both use data to predict patterns of behavior as consumers and as citizens (Chander, Gelman, & Radin, 2008; Richards & Hartzog, 2016).

Big Data refers to vast amounts of information that can be systematically analyzed, operationalized, and commodified for marketing and other purposes (Zuboff, 2019). It is frequently touted as the digital era's oil because of its value and impact on the tech industry's growth. With machine learning and natural language processing, vast amounts of datasets can be operationalized as behavioral data and used for individualized advertising. Prior to the explosion of the 'big data' economy, invasion of privacy was largely envisioned as a Big Brother-like governmental surveillance manifesting itself as ever-present, visibly surveillant, and deliberately oppressive and controlling (Zuboff, 2019). Current patterns of privacy infringements, however, do not stem from a single centralized power and the means of control are distributed among private and governmental entities. Information is collected in massive databases largely unseen and unannounced (Zuboff, 2019). One of the reasons for undisclosed collection of data is that the private entities benefit from inconspicuous collection to avoid feelings of powerlessness, threat, and distrust among the public (Larson, 1994; Rosen, 2011). Furthermore, there is little direct injury, such as restrictions on speech or association, from the modern collection of personal data, so the silent surveillance for marketing purposes is perceived as bearable albeit uncomfortable (Zuboff, 2019).

Defining Privacy through Data Ownership

Another important factor in setting up the scope of data privacy is determining who owns the data. The perception of privacy in the U.S. is that it is alienable and thus can be transferred & waived (Bennett & Raab, 2006). While in the United States privacy laws allow the collector to claim ownership over generated data, Europe's enhanced privacy regulations define personal data as belonging to the individual, which in educational context would belong to the learner

(Borthwick, Anderson, Finsness, & Foulger, 2015; De Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez, 2018; Weippl & Min Tjoa, 2005).

The cultural sentiments about data ownership in Europe were codified in the EU General Data Protection Regulation (GDPR) expressly articulating the rights of the data subject, such as the right to data portability, right of access, right of erasure, and limitation to unauthorized data transfer, among others (GDPR, 2016, Ch. 3). Furthermore, the GDPR provides an updated definition of "data subject" reflecting that, in the age of big data, a person's privacy may be tied not only to their name but also to a unique identifier: "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR, 2016, Ch. 1, Art. 4(1)). Portability of data is a unique concept as a legal mandate, and it represents a shift toward user-centric data practices addressing both personal and economic interests of the individual (De Hert et al., 2018).

The U.S. norms when it comes to data ownership vary in subtle but significant ways. For example, companies can easily purchase, transfer, use, and sell individuals' names, addresses, and other identifiable information without express consent (Garfinkel, 2001). Major technology firms, such as Microsoft and Dropbox, which store significant amounts of customer data, assign to themselves a license to use and share information with others with just a click of the button through click-through Terms of Service agreements (Michels, Millard, & Joshi, 2019). The license does not automatically transfer ownership if the existing legal standards have set up clear definition of ownership for the particular set of data. For example, uploaded photographs are typically perceived as creative content and thus receive certain copyright protections (Michels et

al., 2019). However, the newly emerged type of data, such as a pattern of clicks through a specific website or GPS tracking of a car, do not have traditionally defined ownership rights. In the EU, this type of data now falls under GDPR's protection but the U.S. has yet to grant individuals' explicit ownership rights.

Similar issues of data ownership have emerged on college campuses as universities mine identifiable and extensive student data for a number of purposes, including learning analytics, recruitment and retention, and academic program development, among others (S. Jones, 2012; Jones, Thomson, & Arnold, 2014). The question of ownership may revolve around who created the data; for example, was it generated by a student who checked out books in a library? Or was it system-generated, such as a map of every location where the student accessed the university's Wi-Fi network. Jones et al. (2014) argued that regardless of whether the data is created by the student or system-generated, if it is personally identifiable, then the student should have legal rights to control it. In a K-12 environment, the concept of data ownership can be complicated by the Terms of Service agreements that have intentionally vague, non-transparent differentiation between "data" and "personal information" (Lindh & Nolin, 2016).

Privacy as a Right to Be Forgotten

Digital data has a much greater shelflife over the period of an individual's life as compared to traditional paper records. Archives of digital news and social media, which remain available unless removed, can be easily accessed on the internet and may impact a person's professional and academic trajectory for decades. The GDPR's right to be forgotten, i.e. right to have one's personal information deleted from private companies' networks, is premised on "the fundamental need of an individual to determine the development of his life in an autonomous

way" (Mantelero, 2013, p. 2). Under the right to be forgotten, an individual may request removal of certain records depending on the timing and relevance of the information.

Perceived as immutable American rights, the United States doggedly protects the freedom of speech and freedom of information, generally providing few protections for an individual to suppress publicly available information (Mantelero, 2013). While there is no statutory universal protection of the right to be forgotten in the U.S., some laws do allow restricted access to records, such as criminal expulsion records (Calvert & Bruno, 2010).

As expressed in this section, data privacy protections require a complex analysis of defining what is private in the first place. In the context of K-12 education, administrators must engage in a holistic, multi-departmental reflection to identify the essential elements of protected information before instituting appropriate data privacy policies and best practices (Heath, 2014). Below I examine how educators' decisions in this regard are constrained by the existing set of laws.

Protecting Student Privacy through Legislation

Lack of a National Standard for Student Data Privacy

Student data privacy has been an issue in political circles for the last decade. President Obama announced student data privacy as one of the key issues in his administration (Lestch, 2015). In a rare occurrence during a historically divided Congress, a bipartisan amendment to establish a student data privacy committee passed with 89-0 votes (Roscorla, 2015). Eight separate student data privacy bills were introduced in the 2015 legislative session both from the Republican and Democratic representatives (National Association of State Boards of Education, 2015). Unfortunately, the student data privacy issue fell off the political agenda after 2015, at least on the federal level (Bartow et al., 2016; Gross, 2018).

While a number of states have passed laws related to student data privacy, we have yet to see a comprehensive national legislation to address it (Electronic Privacy Information Center (EPIC), n.d.). Two acts proposed by President Obama in 2015, *Personal Data Notification and Protection Act* and *Student Data Privacy Act* would have set up a single, federal standard for data protection and would have banned private companies from profiting off student data, respectively (Shear & Singer, 2015). Both acts failed. A common challenge with passing federal legislation on student data privacy is ensuring that innovative learning and student improvement goals are not stifled (Lestch, 2015). Any legal framework designed to protect student privacy must also create pathways for data to support learners in a meaningful way (Roscorla, 2015). Hence, what becomes integral to the legislation is ensuring allocation of resources and ongoing training of educators and school officials who have access to student data. Below are some of the federal and state laws that currently govern educators' practices with student data privacy.

Privacy Act of 1974

In the aftermath of the Civil Rights era, public cases of illegal government spying, and the rise of computerized databases, the Privacy Act of 1974 became the key privacy protection law in the United States, regulating collection and use of personal information by the federal government (Coles, 1990). At the time, the public largely perceived the federal government to be the biggest threat to personal privacy because of its access to sophisticated and powerful computing systems and sensitive data through various federal agencies. The Privacy Act was influenced by a report, *Records, Computers, and the Rights of Citizens* (1973), which recommended extensive transparency in governmental record-keeping, access to personal records, limited use of information based on the original purpose, and the opportunity to correct records of identifiable information. Many of the recommended practices ended up in the Privacy

Act, but the mandates for transparency and proper use of information were limited to government thus exempting private entities (Coles, 1990).

The proliferation of digital data collection and distribution by private companies has prompted passage of important federal legislation that extended information privacy in specific economic sectors, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Children's Online Privacy Protection Act (COPPA) of 1998, and the Gramm-Leach-Bliley Act of 1999 (offering people to opt out of disclosures made by financial institutions) (Solove, 2004). However, unlike most countries with robust use of technology, the United States has yet to pass a comprehensive law for information security across *all* sectors (De Hert, 2018; O'Connor, 2018). Instead, the U.S. legal framework on this issue is sector-based and dependent on the user's activity or status rather than personhood (O'Connor, 2018). For example, the federal laws will protect an individual's record as a medical patient but not as a Facebook user.

In 2015 Microsoft's survey of 12,000 internet users across the globe found that cyber fears are increasing in both developed and developing countries. "Majorities of respondents in every country but India and Indonesia say current legal protections for users of personal technology are insufficient, and only in those two countries do most respondents feel fully aware of the types of personal information collected about them" (Penn, 2015, para. 17). The friction between the existing laws and the public's increased fears of invasion of privacy stems from the new paradigm where private companies now have unprecedented access to complex and comprehensive information about individuals that used to be available only to the government agencies (Penn, 2015).

Federal Trade Commission Act (FTC Act)

Because the U.S lacks a universal information security law, the FTC Act has emerged as the default legislation to oversee unfair or deceitful practices as part of its consumer protection mandate (Serwin, McLaughlin, & Tomaszewski, 2014). In 2003, Gateway Learning Corporation, seller of the learning software "Hooked on Phonics," was charged by the Federal Trade Commission (FTC) with violating Section 5 of the FTC Act for renting consumers' information, including names, addresses, children's age ranges, to third party advertisers and telemarketers (Federal Trade Commission, 2004). Gateway Learning did not notify consumers or give them an opportunity to opt out when it updated its privacy policy to allow for rental and sale of consumer data, including children's data. As part of the settlement, Gateway Learning was barred from misrepresenting its use of customer information and from applying new privacy policies to existing customers without their consent (Federal Trade Commission, 2004).

The FTC's regulation of privacy infringements has several limitations. First, the FTC Act does not protect information privacy as an end goal, it only prohibits *misleading* practices; thus, companies are free to share as much or as little consumer information as long as they include appropriate disclosures in their policies (Serwin et al., 2014). Second, consumers rarely know when their information is being sold, which means that finding violations of privacy policies is increasingly difficult among thousands of data collectors, analyzers, and brokers of data (Chander et al., 2008).

The gap in research on the subject of information security in education is evident in its absence in leading legal publications. Published by experts in the field of information security, *Privacy, Security, and Information Management: An Overview* book lists financial privacy,

outsourcing to foreign countries, health records, and social networking as "current hot issues" but omits education (Serwin et al., 2014).

Family and Educational Rights and Privacy Act (FERPA)

Often referred to as the Buckley Amendment, FERPA was passed in 1974, well before the introduction of digital data and record-keeping as it is practiced today. It broadly defines education records as records, files, documents and other materials which, (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution (FERPA, 1974, §99.3). In short, the law requires that, as a condition of receiving federal education funds, schools must agree: 1) not to disclose education records without the consent of the student or parent of a minor student; and 2) students and parents of minors have a right to access their education records. Federal case law has remained largely silent on what is considered "education record" with only two cases decided by the Supreme Court, and neither one addressed digital data (Owasso Independent School Dist. No.I-011 v. Falvo, 2002; Gonzaga Univ. v. Doe, 2002).

Despite FERPA's passage before the digital boom, the law does address the issue of digital data (Zeide, 2015). Senator Buckley who introduced the law, explained part of the impetus for the law: "The growth of the use of computer data banks on students and individuals in general has threatened to tear away most of the few remaining veils guarding personal privacy, and to place enormous, dangerous power in the hands of the government, as well as private organizations" (Buckley, 1975, as cited in O'Donnell, 2002, p. 681).

An important element in FERPA's implementation has been the use of the "legitimate educational interest exception" where schools can share student data if there is an educational purpose (FERPA, 1974, §1232g(b)). School districts tend to interpret this exception widely,

which allows them to share information with private vendors without parental or student consent (Bartow et al., 2016). There are a number of issues that arise with the use of this exception. First, once the information is shared with the private vendor, FERPA regulations do not apply to the vendor. Schools must expressly stipulate in a contract how and when this data will be used. Second, the data can be used for non-educational purposes as long as at least one of the purposes has a legitimate educational interest (Bartow et al., 2016). Thus, a vendor can store student data both to improve the curriculum and to create targeted advertising.

During the exponential growth of educational technology (Ed Tech) companies, the U.S. Department of Education's (USDOE) policies favored broad disclosure of student data to private vendors. In 2008 and 2011, the federal government introduced two related amendments to FERPA regulations that had a significant impact on how student data is shared with private and outside entities (Bartow et al., 2016; U.S. Department of Education, 2008). The 2008 amendment stated that schools were allowed to disclose student data, including personally identifiable information, to a "contractor, consultant, volunteer, or other party" performing "an institutional service or function for which the agency or institution would otherwise use employees" (FERPA, 2008, 34 C.F.R. § 99.31(a) (1)(i)(B)(1)). This rule was based on the "school official" exception which was part of the original FERPA language (FERPA, 1974). This exception was traditionally used to give teachers access to student information. However, by allowing a broader interpretation of the "school official" exception, the USDOE instead gave broad discretion to schools and educational agencies to release student data to contracted vendors, such as Google, without parental consent (Bartow et al., 2016; Gross, 2014).

Subsequently, in 2011, the USDOE further expanded the definition of "authorized representative" which allowed state politicians access to sensitive student records as long as they

complied with confidentiality standards (Bartow et al., 2016). Experts suggest that the broadening of such definitions (i.e. agents deemed suitable to collect student data without parental consent) jump started the current concerns for student privacy (Gross, 2014). Eventually acknowledging the unprecedented flow of student data in public schools and its potential for misuse, the USDOE had issued a set of guidelines in 2014 to respond to the pertinent questions from school administrators regarding safeguards of student privacy and data sharing (U.S. Department of Education, 2014). Enforcement and monitoring of FERPA compliance falls under the USDOE's Student Privacy Policy Office (SPPO). SPPO also issues guidance for schools and parents through its Privacy Technical Assistance Center (PTAC) (U.S. Department of Education, 2014). It is important to note, however, that parents or students do not have a right to sue for FERPA violations because the Supreme Court ruled that FERPA law does not grant a private cause of action, meaning parents may not sue the school districts for violations (Gonzaga Univ. v. Doe, 2002). A complaint to SPPO is the only remedy available to parents under FERPA.

Other Student Related Legislation

Children Online Privacy Protection Act of 1998 (COPPA) limits how online providers collect data for minors under the age of 13 (COPPA, 1998). While this act was not intended exclusively for education, it has influenced how educational technology companies develop privacy agreements in order to comply with the law (Gross, 2014). It also impacts how educators set policies on the use of YouTube and other external multimedia in elementary and middle schools (Federal Trade Commission, 2019).

Children's Internet Protection Act (CIPA) governs how public school districts monitor, filter, set acceptable use policies, and educate students on internet practices in schools (FCC, 2017). This law is administered by the Federal Communications Commission (FCC) and is tied

to eRate funding. Under CIPA, schools are required to use an internet filter, to adopt and enforce a policy that addresses hacking and unauthorized disclosure of personal information, i.e. Internet Safety Policy, and educate students about safe online behavior in order to qualify for eRate grants (Federal Communications Commission (FCC), 2017).

Legislation proponents struggle to mediate the tension between innovation and the individual right to privacy (EPIC, n.d.). The lesser but still important issue remains in the limited choices offered to the user in how data is shared. Recognizing the potential for data leakage and possible lawsuits, states have begun to pass student privacy legislation but without a consistent, comprehensive reach (Electronic Privacy Information Center (EPIC), n.d.; Student Privacy Compass, n.d.-b). The state laws differ dramatically in liabilities that are imposed on third-party vendors and enforcement practices (Vance, 2016).

California has been on the forefront of protecting student privacy by passing the Student Online Personal Information Protection Act (SOPIPA), the most comprehensive legislation on the issue of student privacy in the U.S. (Future of Privacy Forum (FPF), 2016; SOPIPA, 2014). SOPIPA prohibits online education service providers from creating a student profile for non-educational purposes and from using student data to create targeted advertising. SOPIPA goes further than collection of data and governs how the data is used and managed (California Department of Justice, 2016). One of the driving forces for the law was the revelation that Google was scanning student emails for advertising (Shear, 2014). SOPIPA bans scanning of student information for all non-educational purposes stating that companies may not use "information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a K-12 student except in furtherance of K-12 school purposes" (SOPIPA, 2014, § 22584 (b)(2)).

Home to the largest K-12 student population in the country, California heavily influences policies and products of educational services companies. Hence, the impact of SOPIPA extends well beyond the state of California. When the same products are used in other states, the school districts benefit from the same level of student privacy protection as SOPIPA mandates (FPF, 2016). Forty states have passed 125 laws addressing student privacy regulation since 2013 (Parent Coalition for Student Privacy, 2019). SOPIPA became effective in California in 2016 (FPF, 2016).

The federal government released a report in 2014 calling for an update to federal legislation on student privacy, among other data privacy issues (Podesta, 2014). The report also calls for increased digital literacy among students and parents to raise awareness of how student information can be protected recommending that:

The federal government should ensure that data collected in schools is used for educational purposes and continue to support investment and innovation that raises the level of performance across our schools. To promote this innovation, it should explore how to modernize the privacy regulatory framework under [FERPA] and [COPPA] to ensure two complementary goals: 1) protecting students against their data being shared or used inappropriately, especially when that data is gathered in an educational context, and 2) ensuring that innovation in educational technology, including new approaches and business models, have ample opportunity to flourish (The White House, Executive Office of the President, 2014).

The 2018 report on the State of EdTech by Common Sense, a non-profit organization that promotes safe technology for children, also revealed inconsistency with how companies are using and sharing student data and overall lack of transparency (Common Sense, 2018; Kelly, Graham, & Fitzgerald, 2018). The report evaluated 100 of the most popular school applications

and found that only 10 percent of the applications met their transparency criteria. Inconsistent, outdated regulations pose a consistent challenge to school administrators when attempting to develop and implement effective student privacy practices. In recent years, 64% of school IT professionals reported increased concerns about data privacy (Passut, 2016).

These numbers are alarming as school districts increasingly rely on outside vendors to provide educational technology, data storage, and learning management systems. While the federal government has recognized the need for legislative overhaul, the current regulations, at least on the federal level, place the burden of compliance with the school administrators. This means administrators at the school district level must carefully review vendor contracts, establish complaint processes, and conduct periodic systemwide audits of student data privacy practices. In the next section, I will examine literature related to current data practices in education.

Collection and Sharing of Student Data through Technology

Ethical Considerations in the Use of Technology in Schools

While laws and policies have an impact on the organization's behavior with data, they are but one factor in the overall information sharing practices. In addition to formal guidelines, "cultural and institutional factors that exert profound influences on the development and implementation of privacy protection tend to be forgotten in debates over the most appropriate legal and regulatory responses to new technological invasions of privacy" (Bennett & Raab, 2006).

Institutional practices must comport not only with legislative mandates but also with the stakeholders' interests. In education contexts, students have expressed the need for limitations in how their personal information is used. For example, students' disclosure of personal

information on social media does not necessarily imply that the students wish to have that information included as part of the learning analytics process (Ifenthaler & Schumacher, 2016). Even high school students have expressed concerns over the use of private information collected through Facebook-supported learning programs (Strauss, 2018). A study conducted in Turkey in 2018 with over 1,000 ninth-graders found that over 80% of students believed that privacy protection was a basic human right, but most were not knowledgeable as what type of data fell under the definition of personally identifiable information (Gogus & Saygın, 2019). The problem arises from the seemingly non-transparent practices of collecting and storing personal information even if the purpose of the data collection is to improve student learning (Bowers et al., 2019; Pardo & Siemens, 2014; Slade & Prinsloo, 2013).

Using a sociocritical perspective, Slade and Prinsloo (2013) posited that students and educators exist in an inherently unequal power relationship, and thus educational institutions bear the burden of ethical considerations when collecting, storing, transferring, and using student data. This power relationship resembles the one between researcher and subject: "Ethical challenges and issues in the use of educational data can be usefully viewed in the context of the history of Internet research ethics and against the backdrop of the development of research ethics after cases such as the Tuskegee experiment" (Slade & Prinsloo, 2013, p. 1512). The move to increased use of educational technology has also contributed to gaps in inequity and commercialization of public education (Selwyn, 2013). Thus, institutions not only have an obligation to comply with relevant privacy laws but also have an ethical obligation to protect students as a vulnerable population with limited autonomy (Allen-Brown & Nichols, 2004; Buchanan, 2011).

Technological advances have heightened ethical concerns in education even when the law is silent (Yeaman, 2015). People, particularly in democratic countries, express an almost knee-jerk reaction to undisclosed surveillance despite its legality in educational settings. In a recent widely-publicized incident, a student was visually tracked at home through a school-issued computer without the student's or parents' knowledge (Hill, 2010). The school alleged that camera surveillance was installed in student computers as a security measure in case of theft. However, the case garnered wide national attention and a class action lawsuit, including an amicus brief from the ACLU, leading to a $610,000 settlement from the school (ACLU, 2010; Hill, 2010). Despite the fact that the school district's actions were legal, the publicity and parental pushback suggest that surveillance without consent was at the very least unethical.

Cyber (In)security in Schools

Innovations in technology have also led to an unprecedented use of cyberspace both to enhance the human experience, and inevitably, to exploit it. Lack of stability and security in cyber environments is demonstrated by the annual Gallup polls, where Americans report worries of identity theft and computer hacking as their top concerns (Brenan, 2018). Cyber-crimes have been at the top of the list since their introduction to the poll, with 71% of people indicating frequent or occasional fear of hackers getting access to personal information. These fears are not unwarranted with 48% of all data breaches being caused by malicious or criminal attacks (Cisco, 2018).

Schools and school districts have been so-called "sitting ducks" when it comes to data vulnerability. First, school districts are mandated by state and federal regulations to maintain large databases with sensitive information, including medical history, addresses, and social security numbers (Lynch, 2015; Reidenberg et al., 2013). Second, a large number of users, such

as teachers and administrators, have access to school networks increasing the risk of breach (Stepanek, 2000). Finally, public schools are notoriously underprotected when it comes to cyber security, lacking resources for advanced technology and up-to-date training (Hobbs, 2017).

In recent years, hackers, often suspected to reside outside of the U.S., have exposed thousands of records with sensitive student and teacher information, and sometimes have gained access to school security cameras, which prompted the USDOE to issue a set of guidelines to protect school districts against such attacks (R. Jones, 2017; Ta & Clayworth, 2017; U.S. Department of Education, 2016). Prior cyber attacks at schools have caused shutdown of services, daily disruptions, such as students' inability to take exams (Nicosia, 2017), and theft of paychecks (Hobbs, 2017). But a new type of extortion hacking goes a step further. According to the USDOE, cyber thieves now aim to extort money from school districts that have weak data security systems, frequently threatening shaming, bullying, and even violence against students (U.S. Department of Education, 2016).

Ed Tech companies have not been immune to breaches of sensitive data. With schools frequently outsourcing management and distribution of data to third-party vendors, potential exposure becomes particularly worrisome as these companies are likely to serve multiple districts and aggregate records of thousands, sometimes millions of students ("Dozens of high-school students tied to cheating scandal," 2018; Ta & Clayworth, 2017). In 2017, the education platform Edmodo, which connects teachers and parents around the globe, was hacked exposing the usernames and passwords of 77 million users (Nicosia, 2017). The information was subsequently put up for sale for $1,000 on the dark web. In another incident, the educational data storage company Schoolzilla inadvertently created public access to students' and school officials' records, including test scores and social security numbers (Wan, 2017). The researcher

who discovered the exposed data contacted the U.S. Department of Education to consult on the issue only to discover that the USDOE voicemail box was full (Kromtech Security Center, 2017).

The Cambridge Institute of International Education (CIIE) made a similar mistake of exposing thousands of names, passport details, and extensive personal information of the host families of international students (DataBreaches, 2017). CIIE corrected the oversight but stated that their records of international students are not subject to FERPA because they operate as a consulting firm rather than an educational institution, which further highlights the failure of the current legal framework to protect student informational privacy.

Schools' reliance on outside vendors has created unprecedented and complex challenges for school administrators, such as the need for encryption of data both in storage and in transit (Wan, 2017). A study by the Center on Law and Information Privacy at Fordham Law School found that 20 percent of the surveyed school districts fail to have policies on the use of online services and that "school district cloud service agreements generally do not provide for data security and even allow vendors to retain student information in perpetuity with alarming frequency" (Reidenberg et al., 2013, p. 6). The study reviewed contract agreements in 34 school districts across the country, which collectively covered educational services for over one million students.

Even with added security measures in computer networks, there is a constant threat of human error and social engineering as humans are the weakest link in secure computer systems (Orgill, Romney, Bailey, & Orgill, 2004). Social engineering hacking grants access to a secured network by obtaining an authorized user's login information. Administrators' login credentials are particularly at risk as they have access to thousands of confidential student records.

Exploitation of human error can happen internally as well. In 2018, the Gadsden School District in New Mexico discovered that 55 high school students in the district had illegally accessed the online platform Edgenuity to change their grades (Bieri, 2018). In the next section, I will address how the use of educational technology affects privacy concerns as well as collection and sharing of student data on an institutional level.

Educational Technology and Data Sharing

K-12 education has become increasingly reliant on data, which is driven both by top-down policy initiatives and the pedagogy utilized in the classroom (Watters, 2013). On a policy level, school districts are mandated to report detailed student information, including academic assessment, progress, attendance, demographics, and to focus their efforts on evidence-based interventions (Hess & Eden, 2017; Klein, 2018). In a game of 'pass the baton,' school districts are relying on individual schools to collect and maintain complex databases that require specialized expertise in data entry. While data governance offices have become standard at the school district level, individual schools struggle to meet the needs of information management with limited resources (Hess & Eden, 2017).

The governmental mandates did come with incentives, and in 2005, the federal government began awarding millions of dollars in grants to support Statewide Longitudinal Data Systems (SLDS) with over $265 million awarded by 2009 (Gross, 2014). The goal of the initiative was to track student progress with an individualized ID from preschool to workforce. This jumpstarted the age of massive data collection and exchange, and tech entrepreneurs were eager to collaborate with school districts to develop centralized computing systems monitoring millions of student records (Lynch, 2018).

While initially schools utilized tools that were designed for business productivity, such as Microsoft Office and Google Analytics, the tech companies began developing tools designed specifically for education (Chen, 2015). The Ed Tech market is now split into four distinct categories: content and instruction (ex. Duolingo and Khan Academy); instructional support (ex. Canvas and Google Classroom); management (ex. Parchment, SchoolMessenger, and MySchoolBucks); and "special categories" that are designed for individualized needs, such as special education.

Each tool effectively operates as an outsourcing solution to assist school administrators with managing increasingly complex information systems. The marketing model promulgated by the private Ed Tech sector was consistent across the board: outsource tech management so educators can focus on school management (Watters, 2013). There were few conversations, however, about the regulatory schemes that affect third-party access to a large amount of individualized education data. The business models still vary from fully free non-profit organizations (ex. Khan Academy) to expensive annual enterprise licenses (ex. Blackboard) (Borthwick et al., 2015; Chen, 2015).

Ed tech tools are mostly cloud-based, which means that the information generated by and about users is stored remotely on centralized servers (Kamenetz, 2014). Often these data storage and management systems are controlled by private and non-profit agencies. Centralized data can be effective in state- and citywide initiatives. For example, New York City found a discrepancy in the high school curriculum when the data revealed that four out of five graduates were placed in remedial courses after graduation (Kamenetz, 2014). Detailed and comprehensive data exchange across institutions can also help identify students who fall behind in well-performing districts. However, cloud computing is significant for the legal framework because the student

privacy laws, as they were originally designed, defined educational records as physically maintained by school offices (Daggett, 2008). Cloud storage of records no longer fits this definition.

Institutional Sharing of Student Data in School Districts

Despite increased awareness of risks associated with the use of technology, school districts widely accept and welcome Ed Tech because of its considerable value and utility in managing district-wide data. This can lead to unexpected behaviors among individual actors that generate and share student data. As students generate and share their personal information via Ed Tech, which occurs both on- and off-campus through school-issued devices, school administrators must grapple with the legal and institutional responsibilities of regulating and monitoring such widespread distribution of student information (Robertson, Muirhead, & Leatham, 2019). Furthermore, studies that analyze consumer behavior have found that convenience often outweighs privacy considerations (Miyasaki & Fernandez, 2001) even when people express concerns about privacy (Norberg, Horne, & Horne, 2007). This so-called "privacy paradox" described as "the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors" (Norbert et al., 2007, p. 100) has been documented with online users. One reason cited for the existence of privacy paradox is that the immediate benefits associated with technology use outweigh any potential loss of private information in the future (Dinev, Xu, Smith, & Hart, 2013). By that same logic, school administrators and teachers are more likely to engage in "risky" behavior with technology when presented with immediate benefits, unless there are strict policies and procedures in place to regulate it. Teachers have also reported lack of awareness of institutional policies and definitions of "digital privacy" even with high use of digital tools (Leatham, 2017).

With SPPO overseeing student privacy compliance on a federal level, individual school districts typically establish data governance offices to oversee proper data collection and sharing practices at the district level. SPPO mandates that all school districts develop a Student Privacy Program, which includes policies, procedures, roles, and responsibilities designed to protect student personal identifiable information (U.S. Department of Education, 2015). School districts must have at least one person with designated privacy protection responsibilities. Furthermore, the USDOE has stated that student privacy programs should involve "users and managers of student information, such as data managers, IT staff, and school administrators" (U.S. Department of Education, 2015, p. 2).

It is important to note that the USDOE does not aim to stifle appropriate data sharing intended to achieve institutional goals, which may vary from district to district. Instead, a number of government and nonprofit organizations have produced frameworks and practical guidelines to aid school administrators in proper data collection (Blair et al., 2015; Grama, 2016). One of the issues associated with data sharing is that "technologists and policymakers are not using the same language to describe data protection outcomes" (Grama, 2016, p. 1). Thus, one of the primary recommendations for educational data sharing is establishing baseline identifiers of information security protections and privacy standards (Grama, 2016). The data governance structure must also be collaborative involving diverse institutional offices and data management actors (Blair et al., 2015). It should involve operational area managers, identified as employees who work with data on a daily basis and understand data life cycles, and institutional executives, identified as school leaders who utilize data for decision-making.

Data practices of some state education agencies have already begun to raise concerns and have garnered national attention. Over 30 education organizations submitted a letter to the Governor of Florida urging him to halt the implementation of a statewide student database to track students who are deemed a threat (Collins & Vance, 2019). Such a database would contain data on students' social media posts, bullying reports, mental health records, and foster care placement, among others, and would be shared with state employees and law enforcement. Since 2018, Florida has required schools to collect such data, including mandating disclosure of mental health information as a requirement for public school enrollment (Florida Department of Education, 2018). Stating an urgent reason for implementing a statewide database, i.e. prevention of school violence, Florida is utilizing technology, such as data analytics, social media algorithms, and cloud-based storage, to compile an unprecedented collection of sensitive student information. However, this practice also raises unprecedented questions of how schools should balance student safety against student privacy, surveillance against freedom of movement, and confidential counseling against mandatory reporting (Brown, Carr, Mehta, & Kochanowski, 2018). These questions become particularly relevant in schools serving primarily students of color where administrators were "more likely to rely on more intense surveillance measures than other schools" (Nance, 2016, p. 765). This further highlights the need for holistic, contextual analysis of student data sharing practices as they often lead to unintended and unexpected consequences.

In designing appropriate policies, districts should take into consideration the *innovation-policy* gap and *knowledge* gap identified by Davis (2014). Davis argued that policies attempting to regulate technology will inevitably run into barriers because policies are time-consuming endeavors while technological innovation moves at a rapid speed. This is exacerbated by lack of

technical knowledge among institutional policymakers as to "how identity and privacy are technologically instantiated in any given system… and how identity and privacy are managed generally across many different systems" (Davis, 2014, p. 88). What emerges, and is relevant to this study, is the *culture clash* between technology, which is used to solve problems, and policymaking, which regulates such solutions and methods of problem solving. In my study, I aim to review the practices, perceptions, and policies related to student data privacy on a district level to gain a better understanding of the connections and gaps between use of technology and privacy protections.

Conceptual Framework

The conceptual framework for this study utilizes two distinct but complementary theories that prioritize contextual examination of an inquiry. Activity theory, as developed by Engeström (1987), provides a broad foundation to assess any activity system, while the conceptual integrity theory (Nissenbaum, 2010) offers a useful insight into digital information flow specifically as it pertains to privacy. Both theories have been widely applied in the fields of technology and Human Computer Interaction (Benthall, Gürses, & Nissenbaum, 2017; Clemmensen, Kaptelinin, & Nardi, 2016; Nardi, 1996). The section below provides a brief overview of the two theories and the conceptual foundation for the current study.

Activity Theory

Activity cannot be understood or analyzed outside the context in which it occurs… we must examine not only the kinds of activities that people engage in but also who is engaging in that activity, what their goals and intentions are, what objects or products result from the activity,

the rules and norms that circumscribe that activity, and the larger community in which the activity occurs (Jonassen & Rohrer-Murphy, 1999, p. 62).

Activity theory, originally articulated by Soviet psychologist Alexey Leontiev, offers a foundational socio-cultural approach to human consciousness and knowledge creation (Leontiev, 1978; Yamagata-Lynch, 2010). One of the main tenets of activity theory focuses on the relationship between consciousness and human behavior in a contextually relevant environment. Leontiev posited that human consciousness is developed by human activity, which affects both the outside world and the person: "Acting on the external world, they [humans] change it; at the same time they also change themselves. This is because what they themselves represent is determined by their activity" (Leontiev, 1978, p. 41). Activity theory is ontologically contextual suggesting that the development of human consciousness is dependent on its cultural and societal environment, which is in line with Lev Vygotsky's cultural-historical psychology (Clemmensen, Kaptelinin, & Nardi, 2016). Activity theory is often discussed as Cultural-Historical Activity Theory by scholars (Roth & Lee, 2007; Russell, 1997; Yamagata-Lynch, 2010). This position creates a critical connection to Nissenbaum's contextual integrity framework, which places equal importance on the social norms that define and maintain privacy expectations, discussed in more detail later in this section.

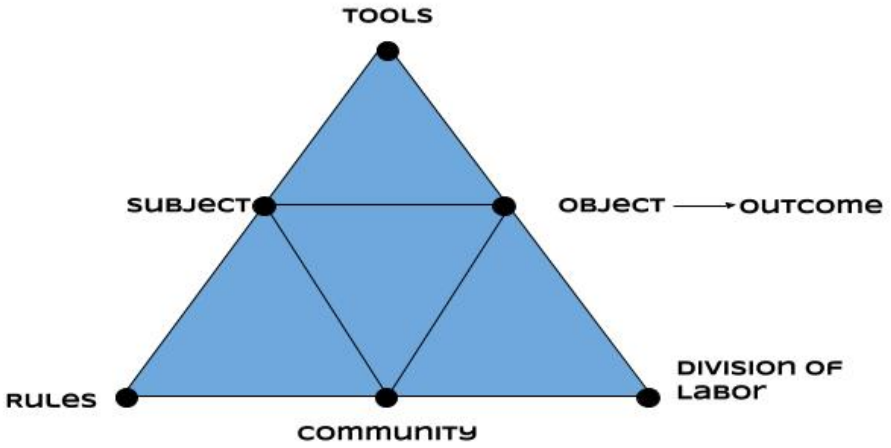
Activity theory, in summary, looks at the mediated interaction between the *Subject* (human actor) and the *Object* (purpose of the desired outcome). "Activity is a process of intertraffic between opposite poles, subject and object" (Leontiev, 1978, p. 3). The individual performs an activity motivated by an object, which exists both independently as part of an

objective world and as an interpretation of the subject's experience. Activity is always intentional and cannot exist without a purpose.

Because Leontiev's work was grounded in the field of psychology, his concepts were predominantly applied to the activities of a concrete individual, a single human being (Kaptelinin, 2005). Engeström (1987) broadened the scope of activity theory into other disciplines by applying it to organizational and collective environments (Kaptelinin, 2005). In conceptualizing the activity theory as a system, Engeström interpreted activities as a collective phenomenon adding a third interacting entity – the community – and mediating factors: *artefacts* (tools and instruments), *social norms* (rules), and *social hierarchy* (division of labor) (Engeström, Miettinen, & Punamäki, 1999). Community here is perceived as the aggregate of people or organizations that share a set of social meanings, while the rules are the normative guides imposed by the community. Engeström's interpretation of the activity theory is represented by a visual model in Figure 5.

Figure 5

The structure of human activity (Engeström 1987, p. 78)



Engeström's (1987) version of activity theory was more accessible and applicable to researchers in the field of organizational change and was easily adopted into Human Computer Interaction (HCI) studies (Bødker, 1989): "Activity theory offers a rich framework that covers a wide range of HCI-relevant issues and factors including the historical, social, and organisational context" (Clemmensen et al., 2016, p. 615). Unlike earlier information processing psychology frameworks (Sowa, 1983), activity theory takes into account the relevant context that prompts the development and the use of interactive technologies. As a descriptive rather than a predictive theory, activity theory allows for system-based examination of technology as it interacts with and impacts the subjects, communities, and artifacts (Nardi, 1996). It rejects the notion that humans function in the same pattern as machines within a system (Nardi, 1996). The motivation and consciousness of a human mind makes humans inherently different from a machine, and consequently, positions machines as tools that mediate human behavior and thought. A comprehensive literature review also found that context, as outlined in activity theory, was commonly discussed in HCI-related studies (Clemmensen et al., 2016).

In an educational context, Engeström (1987) rejected the traditional definition of knowledge acquisition and argued in favor of expansive learning that matches and grows with societal change. An important element of activity theory maintains that changes within a single component of the activity system may have unintended and separate consequences in other areas. Activity theory allows for analysis of such effects by looking at the activity as a complete system (Engeström et al., 1999). Another key factor of this theory is the activity's relationship with the culture in which a subject operates. The tools that mediate an activity are created for and by a particular sociocultural environment. Consequently, the tools shape the subject and the activity itself (Nardi, 1996).

Contextual Integrity Theory

Privacy only exists in context, meaning privacy is a relative, contextual concept. It is the complex blend of varying parameters which gives it a certain tenor. Shed privacy of its institutional, social, cultural, religious, historical, and epistemological context, and it becomes a useless, naked notion, bare to the bone (Gutwirth, 2002, p. 29).

As discussed earlier, the right to privacy is grounded in and continues to be interpreted through the public/private dichotomy and the individual's right to control the flow of information from private to public (Gavison, 1992; Turkington, 1989; Warren & Brandeis, 1890; Westin, 1967). Statutory laws, such as FERPA, rigorously outline the scope of what information should remain private and draw rigid lines between publicly allowable information and confidential data (FERPA, 1974). This view is consistent with the *secrecy paradigm* described by Solove (2004) where a privacy violation exists only when *hidden* information is revealed. However, private versus public labels neglect the contextual expectation of privacy in line with sociocultural norms. In many instances, the nature of information that is deemed private is not in fact secret but depends on how it is shared. For example, while parents may not wish to see their child's report card posted on the school's website, this information is not fully secret. Parents and students are required to share transcripts and report cards for purposes of admission to college, job applications, and scholarship considerations. Thus, the content of the report card is neither private nor public but is shared according to the context. Furthermore, the parent often has an expectation that the released transcript will not be made public even when there are no assurances of such practice. This highlights the normative rules of privacy.

Helen Nissenbaum (2010), a renowned expert on information science, advances a theoretical privacy framework that diverges from the traditional secrecy paradigm and instead

situates privacy within larger social constructs. In her contextual integrity (CI) framework, Nissenbaum argues that people's expectation of privacy is linked to proper flow of information extending beyond the simplicity of public versus private domain. To identify what is an appropriate flow, we must consider several independent factors: *actors* (subject, sender, recipient), *information type*, and *transmission principles* that limit the information flow. To put it simply, appropriateness of information sharing depends on the context. The subjects of data collection in the case of educational technology can be students, parents, or employees. The senders can be data governance officers, principals, IT professionals, or vendors as designated "school officials." The recipients of information can be vendors, agencies, or the general public. One of the more obvious transmission principles is consent, but there are a number of other transmission principles that alter normative expectation of privacy depending on the context; for example, posting public records online has a very different implication on the privacy of the individual as compared to printed records publicly available in a building (Nissenbaum, 2019).

The goal of the CI framework is to describe and to prescribe a privacy paradigm in the digital age. As Nissenbaum (2010) defines it, "a right to privacy is neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information" [emphasis in the original] (p. 127). In examining the use of educational technology through the CI framework, Nissenbaum argues that data sharing in schools can be based on how it advances or hinders the general goals of education. Nissenbaum utilizes Walzer's (1984) articulation of universal purposes of education, such as: a multi-generational transmission of knowledge, traditions, and rituals; improvement of intellect and understanding; discovery of talent that is beneficial to society; and development of character and citizenship. As such, when schools and administrators consider utilizing technology that would aggregate and disclose student data, the benefits and

detriments of such use should be thought of "against the backdrop of the specific ends, goals, purposes, and values" of the educational sphere (Nissenbaum, 2010, p. 171). In other words, context brings to light not only the benefit of disclosing student information but also the chilling effect it may have on student's freedom of expression and development. But at the same time, it offers a pathway toward articulating proper data sharing practices when they align with the goals of education. It bears mentioning here that the goals of the educational agency, i.e. school district, are not always synonymous with the goals of education. When the two are in conflict, the focus must be redirected to broader educational goals.

An important distinction for the CI framework is that it operates as both a normative and descriptive foundation for a study. It is descriptive because it enables the researcher to identify the context and the existing information norms. Once the context of the activity is defined, the researcher is able to perform a normative evaluation of the new, untried information practices deeming them appropriate or flawed.

In response to the criticism of the seemingly unrealistic contextual standards, Nissenbaum argues that CI is in fact already being applied in the well-established legal doctrine of "reasonable expectation of privacy" (Nissenbaum, 2010). The determination by a judge when there is a violation of reasonable expectation of privacy is inevitably normative because the decision maker must first assess what is reasonable. Digging deeper, she exposes that reasonableness is grounded in the judge's discretion to determine when a particular action, for example, the use of facial recognition software, fits within the socially accepted norms. The judges "not merely assess how common the technologies are and how familiar people are with them, but how common and how familiar they are in context, and if this is known, whether the

particular application in question violates or conforms to relevant context-relevant informational norms" (Nissenbaum, 2010, p. 235).

Nissenbaum further cautions against applying the public versus private labels when it comes to technology. Instead, her framework focuses on a system or a set of acts that collectively create the potential for harm, similar to pollution. She situates privacy within a sociotechnical system where each questionable practice of privacy violation has meaning "beyond its immediate reach, its direct impact, taken alone" (p. 243). This view is epistemologically similar to critical theory of technology (Feenberg, 2002). Positioning technology in social and cultural spheres, information technology is a phenomenon that both impacts and is impacted by cultural norms, and the expectation of privacy inevitably evolves along with it.

Activity Theory, Contextual Integrity, and Student Data Privacy

Korpelainen and Kira (2013) point out that the activity theory's systematic and holistic attributes provide an important advantage in assessing organizational behavior, thus exposing contradictions and tensions that may not be visible in a more linear evaluation. This study on student data privacy benefits from a holistic theoretical model because it is affected by a number of systems – legal, pedagogical, and technical – which do not reveal the full picture when looked at as separate enterprises. It is an appropriate framework to reveal the breakdown in the interaction and the tensions between data sharing, educational goals, and privacy.

In similarity to Nissenbaum's (2010) contextual integrity framework, the activity theory focuses on the context of any particular performance (Jonassen & Rohrer-Murphy, 1999). Juxtaposing and overlapping the two frameworks – contextual integrity and activity theory – delivers a theoretical foundation that narrowly fits the purpose of this study: preservation of student data privacy in the context of technology use in K-12 environment. First, the contextual

integrity (CI) framework, designed "to respond to the challenges of rapidly evolving sociotechnical practices," is a good fit for the assessment of unprecedented use of technology in a previously non-technical industry such as education (Nissenbaum, 2019, p. 231). Second, instead of increasing barriers, CI allows for the introduction of new types of flow of information that would be beneficial in the context of education; it does not conservatively prohibit all collection and sharing of student data based on previously established norms. Such a framework ideally meets the goals of this study, which is to conduct an interpretative case study in how data sharing through technology impacts student data privacy in K-12. Third, CI embodies the elements of both descriptive assessment (ex. describing the structure of the informational norms) as well a prescriptive one (ex. establishing a process to balance entrenched informational norms against novels ones) (Benthall, Gürses, & Nissenbaum, 2017). Activity theory is a descriptive theory, and collectively, CI and activity theory offer a complementary conceptual framework for the current study. While the activity theory framework can help assess the relationship between various entities, CI provides the tools to explore new and emerging issues of student privacy in K-12.

In applying activity theory, the critical initial steps involve: 1) understanding relevant context where the activity occurs; and 2) understanding the motivations of the subject (actors) as well as perceived contradictions in the system (Jonassen, 1999). In the current study, the subject in the inquiry are the actors who are involved in ensuring secure student data either directly or indirectly, such as data governance officers, legal counsel, institutional researchers, and IT professionals. The object is to secure student data, leading to the outcome of preserving student privacy. It is important to note that the assumption in this activity system is that preserving student privacy beyond the existing legal framework is the desired outcome. The artifacts include

educational technology software, learning management systems, contracts designed to anticipate data leaks, and cyber security software. The evolution and variety of technology is a key element in this study because, according to the activity theory, the type of tools used in the performance of an activity has an important impact on the activity, as the tool both alters and is altered by the activity (Jonassen, 1999). I chose to review how data is shared at an institutional level rather than at individual schools because district-level administrators directly work with policy development and implementation broadly impacting appropriate information norms.

Under activity theory, the activity examined in this study is the *collection and sharing of student data.* In the CI framework, this activity is identified as the *information flow*. Informational norms as defined by the CI framework provide a nuanced view of the *rules* component of the activity theory model, governing and limiting the activity as discussed by Engeström (1987), and the *subjects*, i.e. the senders and recipients of the data. If we consider the flow of information as the activity of sharing data, then privacy "is preserved when information flows generated by an action or practice conform to legitimate contextual informational norms" (Nissenbaum, 2019, p. 224). To determine the context of the activity, one must consider: actors (subjects), information types (type of student data that is being collected and stored), and transmission principles (tools and artifacts; for example, contractual obligations between the schools and vendors). The visual application of the model is represented in Figure 2 (Chapter 1).

In sum, the conceptual model represented by the activity theory and contextual integrity framework delivers an important foundational structure to examine how the collection, storage, and use of student data operates as an activity in the context of technology use in a K-12 environment. This activity can also be labeled as the "flow of information" as outlined in

Nissenbaum's (2010) CI framework. The framework outlined above will provide important insight in understanding the motives and goals of the activity system.

Conclusion

The conceptual framework articulated above is appropriate for this study because of its emphasis on context. As an interpretive case study, the goal of this research is to understand "a contemporary phenomenon within its real life context" (Yin, 1994, p. 13) in an educational K-12 setting. Looking at a single school district and the perceptions of different actors (subjects) who are tasked with articulating and implementing policies related to student data privacy, it becomes important to contextualize their perceptions and to understand the diversity of actors who are involved in the activity through different roles.

CHAPTER 3. MANUSCRIPT 1

Balancing Student Privacy and Innovation:

Review of Best Practices and Legislation (working title)

Abstract

K-12 educational technology tools are transforming education landscape as private companies gain access to unprecedented amount of student data. Educators rely on these data to make informed decisions about innovative teaching and individualized learning. However, these trends also lead to heightened risks of data breaches and growing concerns about schools' capacities to maintain confidentiality of student records. As a relatively new phenomenon, student data privacy requires a close examination of risks and opportunities emerging with the advent of educational technology. This article provides a review of literature on the issues of student data privacy as well as emerging best practices in order to assess the tension between innovative use of data and risks to student privacy. It concludes with a premise that innovation and privacy are not inherently at odds and can be reconciled by addressing existing gaps in the current framework.

Introduction

> In 2021, the state of kids' privacy is far below parents' expectations, and products used by children are not nearly as privacy-protecting as they should be.
>
> - 2021 Common Sense State of Kids' Privacy (Kelly et al., 2021)

What does online privacy mean to parents and educators? The answer to this inquiry could fill a book, but regrettably, there is little consensus for a legally binding definition of privacy when it comes to online environments. In recent years, the COVID-19 pandemic blurred

the lines between the physical and the virtual, and in the process revealed how few privacy protections exist in the U.S. vis-à-vis the private sector. K-12 education was no exception during this deep dive into a virtual reality, exposing gaps in practice and in knowledge in the use of technology in the classroom (Anand & Bergen, 2021; Diliberti & Kaufman, 2020; Keierleber, 2020). In 2020, cybersecurity and student data privacy emerged as the top two priorities for school IT professionals; yet, the risk awareness and understanding of the necessary safeguards remains low (Consortium for School Networking, 2021). Forty states have passed 125 laws on student data privacy since 2013 and new ones are being implemented each year in an attempt to address the limited federal protections for digital student records (Student Privacy Compass, n.d.-a). In the meantime, the use of privately-owned educational technology (Ed Tech) is increasing exponentially in public schools with millions of student and parental data points moving from schools to private sector (Feng & Papadopoulos, 2018). Educators and parents struggle to keep track of new legislation, best practices, and risks to children's privacy amid these emerging phenomena.

This article provides a review of the relationship between educational technology and student data privacy in K-12, including careful examination of reports, academic research, national and state laws, district and state policies, and best practices as outlined by governmental and nonprofit organizations. The purpose of the review is to assess what is currently mandated, what is practiced, and what remains unaddressed in the United States. First, I begin with a review of literature on privacy in the context of education and Ed Tech, reviewing publications and legislation on the topic. Second, I examine the emerging best practices and trends on the national scale. Finally, based on the first two sections, I identify the persisting gaps in student data privacy and recommend means to address them.

The current publication also serves as the first in a series of research articles on student data privacy in a single school district in Hawai‘i. As part of an overarching exploratory case study, Phase 1 (current article) sets up the national context and will inform the subsequent two phases to identify alignment between emergence of the phenomenon at the policy level and its implication at school level in Hawai‘i. The three phases are designed to examine the issue comprehensively from three perspectives: national experts, district administrators, and school teachers.

Literature Review

It is important to note that there are a number of other issues in student data privacy unrelated to Ed Tech. For example, the use of student data by law enforcement and immigration officials (American Civil Liberties Union, 2019; Bellows, 2019; Reddy, 2020), the monitoring of student social media and emails (Beckett, 2019; Hankerson et al., 2021; Vickery, 2015), and ethical implications of learning analytics (MacCarthy, 2014; Willis et al., 2016) all call for a meaningful conversation and research on their own merits. This article, however, has a specific focus on student data privacy in the context of third-party educational technology use in public schools. Review of the supporting literature below is organized by: 1) identifying general concerns about privacy in the digital age; 2) assessing the emerging threats to student privacy in K-12; and 3) reviewing existing federal and state legislation on the issue of student data privacy. The last section also addresses laws and policies that are specific to Hawai‘i. First, I reviewed key federal laws that directly or indirectly protect privacy of students and minors, as well as seminal works by privacy experts in defining the parameters of privacy. The criteria for the literature review selection was then broadened to incorporate academic and news publications

related to law, information security, data privacy, and education. Prominent law and education journals were reviewed to identify past and existing threats to information security and privacy in schools, using terms such as "student data privacy," "FERPA [Family Educational Rights and Privacy Act]", and "information security." Further, privacy advocacy and parent groups, such as Future of Privacy Forum and Data Quality Campaign, maintain exhaustive resources and news article related to future and emerging risks. Finally, I assessed laws and policies in Hawai‘i that impact student privacy.

Privacy in the Digital Age

Defining Privacy and Data Ownership

A key consideration in data privacy research is defining privacy. Depending on the country's legal system and its cultural norms, privacy definition can range from "the right to be left alone" (Warren & Brandeis, 1890) to the right to control and to limit personal information (Bygrave, 2014; Heath, 2014; Solove, 2004). While the U.S. Constitution does not explicitly guarantee an individual's right to privacy, American jurisprudence has gradually developed protections under the 'privacy doctrine' using common law, torts law, constitutional law (as interpreted in Supreme Court cases), and multiple state and federal statutes (Solove & Schwartz, 2018). In the U.S., the traditional discourse on privacy has revolved around the 'secrecy paradigm' - not publicly available information is private and all other information is public (Richards & Hartzog, 2016). However, the radically increased ease of aggregation and transfer of digital data between different contexts has given rise to a new, more nuanced definition of privacy: An alternative conceptualization of privacy that recognizes a person's right to control and to use information even if that information is not inherently 'secret' (Bennett & Raab, 2006;

Solove, 2004). As Solove (2004) has argued, the secrecy paradigm is a simplistic, binary view that does not always represent the reality of our expectations.

Defining privacy within a context is driven by how much control the person can exert on personal information. When data is taken out of context, people feel a violation of privacy even if they have agreed to sharing this information elsewhere (Heath, 2014; Nissenbaum, 2010). Our concept of privacy also evolves with changing cultural norms and requires a consideration of both the interests of affected actors and the contextual values (Nissenbaum, 2011). For example, a study by Ifenthaler and Schumacher (2016) showed that students who shared their personal information on social media platforms were overwhelmingly opposed to the use of that data in learning analytics because it was outside of the intended context.

Determining who owns the digital data is another important factor in delineating the scope of data privacy. American jurisprudence largely deems personal data as transferrable and its ownership can be waived with a click of the "Agree to Terms of Service" button (Bennett & Raab, 2006). Companies can easily purchase, transfer, use, and sell Americans' personal data, such as names, addresses, and other identifiable information, without express consent (Garfinkel, 2001). Europe's enhanced privacy regulations, on the other hand, define personal data as belonging to the individual, which in an educational context would belong to the learner (Borthwick et al., 2015; De Hert et al., 2018). The cultural sentiments about data ownership in Europe were codified in the European Union's General Data Protection Regulation (GDPR) expressly articulating the rights of the data subject, such as the right to data portability, right of access, right of erasure, and limitation to unauthorized data transfer, among others (De Hert et al., 2018).

Moreover, new types of data, such as a pattern of website clicks or GPS tracking of a car, lack traditionally defined ownership rights. In the EU, this type of data now falls under GDPR's protection, but the U.S. has yet to grant individuals explicit ownership rights over computer-generated data. Issues of student data ownership have surfaced as universities mine student data, without consent or notice, to improve academics, retention, and academic program development, among others (Jones et al., 2014; Jones, 2012). The question of ownership may revolve around who created the data; for example, data may be generated by a student who checked out books in a library, or it may be system-generated, such as a map of locations where the student accessed the university's Wi-Fi network. Jones et al. (2014) argued that regardless of who created the data, the student should have legal rights to control any personally identifiable information (PII). In both higher education and K-12, the concept of data ownership can be complicated by third-party Terms of Service agreements with intentionally vague definitions of 'personal information' and by definitions of 'educational records' (Lindh & Nolin, 2016).

Threats to Information Privacy in the Digital Age

Privacy protections have not kept up with the digital world largely because of the fast pace of technological advancement and limited knowledge of how our personal data is being used (Nissenbaum, 2011; Solove & Schwartz, 2018). Personal data is continuously recycled and reused from such sources as governmental public records, online browsing history, and purchasing preferences (Solove, 2004). The trajectory of data transfer is cyclical from the government, to private entities, between private entities, and back to the government for background checks and investigations. The value of such exchange lies in how companies and the government use data to predict patterns of behavior of individuals as consumers and as citizens (Chander et al., 2008; Richards & Hartzog, 2016).

Prior to the explosion of the 'Big Data' economy, in which vast amounts of information can be systematically analyzed, operationalized, and commodified, invasion of privacy was largely envisioned as visibly controlling and oppressive governmental surveillance (Zuboff, 2019). Current patterns of privacy infringements, however, do not stem from a single centralized power and the means of control are distributed among private and governmental entities. Information is collected in massive databases largely unseen and unannounced (Zuboff, 2019). Private online companies actually benefit from inconspicuous collection to avoid the sense of powerlessness, threat, and distrust among their users (Larson, 1994; Rosen, 2011). Furthermore, contemporary collection of personal data is not likely to lead to readily apparent injury, such as a restriction on speech or association, so the silent surveillance for marketing purposes is perceived as bearable albeit uncomfortable (Zuboff, 2019).

Emerging Risks to Student Privacy

Educational Technology and Data Sharing

Like other industries, K-12 education has become increasingly reliant on data, driven both by top-down policy initiatives and new pedagogical efforts (Mandinach & Gummer, 2021). On a policy level, school districts are mandated to report detailed student information, including academic assessment, attendance, and demographics, just to name a few, and to focus their efforts on evidence-based interventions (Hess & Eden, 2017). School districts often rely on individual schools to collect and maintain complex databases that may require specialized expertise in data entry. While data governance offices have become standard at the district level, individual schools struggle to meet the mandates for information management with limited resources (Hess & Eden, 2017).

The Ed Tech industry grew to meet the demands of the K-12 education sector. The Ed Tech market is now split into four distinct categories: content and instruction; instructional support; management; and individualized categories, such as special education (Chen, 2015). Each tool effectively operates as an outsourcing solution to assist administrators and teachers (Watters, 2013). There were few conversations, however, about the regulatory schemes that affect third-party access to personalized education data.

Ed Tech tools are mostly cloud-based, which means that the information generated by and about users is stored remotely on centralized servers and controlled by private and non-profit agencies (Kamenetz, 2014). Centralized data can be effective for state- and citywide initiatives. For example, New York City found a discrepancy in the high school curriculum when the data revealed that four out of five students were placed in remedial community college courses after graduation (Kamenetz, 2014). Detailed and comprehensive data exchange across institutions can also help identify students who fall behind in well-performing districts. However, cloud computing is significant for the legal framework because student privacy laws, as they were originally designed, defined educational records as physically maintained by school offices (Daggett, 2008). Cloud storage of records no longer fits this definition.

Ethical Considerations in the Use of Technology in Schools

While laws have an impact on an organization's behavior with data, they are but one factor in overall information sharing practices. In addition to formal mandates, there are influential cultural and institutional factors that impact implementation of privacy safeguards, but they tend to be overlooked during big-picture conversations about technology and privacy (Bennett & Raab, 2006). Current laws continue to give broad discretion to schools in the collection and monitoring of student data. However, Ed Tech tools that promise administrative

relief have also left many districts in the dark about potential threats to student privacy and have raised ethical concerns even when the law is permissive (Yeaman, 2015). A number of well-publicized reports highlighted overbroad surveillance in schools featuring headlines such as "An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning" (Keierleber, 2021), "Surveillance Won't Save Our Kids, Humane Public Policy Can" (Barbour, 2021), and "Under Digital Surveillance: How American Schools Spy on Millions of Kids" (Beckett, 2019). The negative tone of these publications reflects the increased concerns shared by parents toward digital surveillance, despite its legality and school board approvals.

Parents at a Pennsylvania school district, for example, filed a class action lawsuit after the district continuously tracked students at home via school-issued computer cameras without the student's or parents' knowledge (Hill, 2010). The district's surveillance program was within the bounds of its policies and state laws, but legal and computer experts reflected that the policy was "Orwellian" and overreaching (Bender, 2010). The judge ordered an injunction and the parents most likely would have prevailed in the case, but because the school district settled out of court, the controlling jurisprudence on this issue remains silent. The school board has since adopted a policy that narrowly governs the district's access to student computers: "the student's permission must be documented before the remote access is performed" and the district may review student files only if "the District has a reasonable suspicion that the student is violating District rules or policies" (Lower Merion School District, 2011).

By comparison, Technology Use Guidelines in Hawai‘i public schools broadly permit remote-access surveillance: "[d]evices and accounts accessing HIDOE [Hawai‘i Department of Education] Internet and Networks are the property of HIDOE. HIDOE monitors and reserves the right to monitor all such devices, networks, and internet activities by students. Students shall

have no expectation of privacy in their use of HIDOE-owned digital devices" (Hawai'i Department of Education, 2016, para. 4). Under the broad language of this guideline, maintaining ethical boundaries of data privacy remains at the discretion of the school administrators. This may lead to confusion with leadership changes, particularly if parent and community organizations do not have a full understanding of how educational technology impacts children in public schools.

Data practices of state educational agencies have begun to raise concerns and national attention as well. Over 30 education organizations submitted a letter to the Governor of Florida urging him to halt the implementation of a statewide student database to track students who are deemed a threat (Collins & Vance, 2019). Since 2018, Florida has required schools to collect highly sensitive personal student data, including mental health information, as a requirement for public school enrollment (Florida Department of Education, 2018). Insisting that it serves safety interests, Florida began utilizing Ed Tech analytics and algorithms to assess the student data, and in the process raising questions of how schools should balance student safety against student privacy, freedom of movement, and confidential counseling (Herold, 2019; Reddy, 2020).

Finally, lack of transparency has emerged as another issue in ethical use of student data (Parent Coalition for Student Privacy, n.d.). Schools typically contract with Ed Tech companies without parental consent, which is conducive to effective classroom management, but the parents are often left in the dark about the types of information that is being shared without their consent. Federal review of 1,504 school district websites over a period of three years 2018-2021 found that 95% of the districts did not include a data inventory to show the type of information collected about students, and only 6% had district contact information if parents have questions about student privacy (U.S. Department of Education, Student Privacy Policy Office, 2021).

Privacy experts agree that transparency about data collection and use is a first step in effective privacy regulation, and the consumers – in this instance, parents – should not be burdened with complicated technical language in order to understand it (McPhie, 2019).

Data Vulnerabilities in Schools

K-12 districts are also uniquely vulnerable when it comes to cyberattacks. School districts maintain large databases with sensitive information, including medical history, addresses, and social security numbers (Lynch, 2015; Reidenberg et al., 2013), and public schools are under-protected when it comes to network security, lacking resources for advanced technology and up-to-date training (Hobbs, 2017).

A recent increase in data and software breaches suggests that "malicious cyber actors are expected to continue seeking opportunities to exploit the evolving remote learning environment" (Cybersecurity and Infrastructure Security Agency (CISA), 2020, p. 3). Hackers have exposed thousands of records with sensitive student and teacher information, and sometimes have gained access to school security cameras, which prompted the U.S. Department of Education (USDOE) to issue a set of security guidelines (Jones, 2017; Ta & Clayworth, 2017; U.S. Department of Education, 2016). Cyberattacks at schools have caused shutdown of services, daily disruptions, such as students' inability to take exams (Nicosia, 2017) and theft of paychecks (Hobbs, 2017). Cyber thieves also aim to extort money from school districts that have weak data security systems, frequently threatening shaming, bullying, and even violence against students (U.S. Department of Education, 2016).

According to a recent report, 2020 marked a record-breaking year in cyberattacks against schools with an 18% increase from 2019 (Levin, 2021). In August and September, 57% of all ransomware incidents reported to the Multi-State Information Sharing and Analysis Center

involved K-12 schools (CISA, 2020). The move to virtual environments contributed to the increase, but the report also notes that "until school districts have the resources and infrastructure in place to support them in implementing cybersecurity programs, general federal and/or state cybersecurity guidance… is unlikely to be acted upon in a timely manner, if at all" (Levin, 2021, p. 15). The author correctly points out that policies on data protection must be accompanied by allocation of resources and funding at the individual school level.

Ed Tech companies have not been immune to breaches of sensitive data. Potential exposure becomes particularly worrisome as these companies usually serve multiple districts and aggregate records of thousands, sometimes millions of students (Ta & Clayworth, 2017; Wan, 2017). In 2017, the education platform Edmodo, which connects teachers and parents around the globe, was hacked exposing the usernames and passwords of 77 million users (Nicosia, 2017). The information was subsequently put up for sale for $1,000 on the dark web. The FBI warned that cyber attackers "seek to exploit the data-rich environment of student information in schools and education technology (edtech) services… Educational institutions that have outsourced their distance learning tools may have lost visibility into data security measures" (CISA, 2020, p. 4). Private education companies are not subject to student privacy laws because they operate as private vendors rather than educational institutions, which further highlights the failure of the current legal framework to protect student data (DataBreaches, 2016).

Schools' reliance on outside vendors has created additional new challenges for school administrators, such as the need for encryption of data (Wan, 2017). A study by the Center on Law and Information Privacy at Fordham Law School found that 20% of the surveyed school districts failed to have policies on the use of online services and that "school district cloud service agreements generally do not provide for data security and even allow vendors to retain

student information in perpetuity with alarming frequency" (Reidenberg et al., 2013, p. 6). The study reviewed contract agreements in 34 school districts across the country, which collectively covered educational services for over one million students.

Even with added network security measures, there is a constant threat of human error and social engineering as humans are the weakest link in secure computer systems (Orgill et al., 2004). In 2018, the Gadsden School District in New Mexico discovered that 55 high school students in the district had illegally accessed the online platform Edgenuity to change their grades (Bieri, 2018). Administrators' login credentials are particularly at risk as they have access to thousands of confidential student records.

Legislation

Lack of a National Standard for Student Data Privacy

The proliferation of digital data collection prompted enactment of several federal laws that extended information privacy to specific economic sectors, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Children's Online Privacy Protection Act (COPPA) of 1998, and the Gramm-Leach-Bliley Act of 1999 (Solove, 2004). The U.S. privacy legislation is sector-based and dependent on the user's activity, for example, as a patient, or status, for example, under the age of 13, rather than personhood (O'Connor, 2018). In other words, online users outside of the protected sectors and activities have few privacy protections as long as the companies' practices are in line with their stated Terms of Service, which are typically non-negotiable. The new paradigm where private companies gain access and control over sensitive personal information has not been universally regulated, and has led to friction between legal safeguards and the public's concerns for privacy (Penn, 2015).

Student data privacy has been an issue in political circles for the last decade. President Obama announced student data privacy as one of the key issues in his administration (Lestch, 2015). Eight separate student data privacy bills were introduced in the 2015 legislative session both from the Republican and Democratic representatives (Roscorla, 2015). Two acts proposed by President Obama in 2015, *Personal Data Notification and Protection Act* and *Student Data Privacy Act* would have set up a single, federal standard for data protection and would have banned private companies from profiting off student data, respectively (Shear & Singer, 2015). Both acts failed, and we have yet to see national legislation on this issue (Electronic Privacy Information Center (EPIC), n.d.).

A challenge with passing federal legislation on student data privacy is creating exemptions for schools to continue innovative learning and data-driven student improvement goals (Lestch, 2015). Any legal framework designed to protect student privacy must also create pathways for accurate and strategic data collection process to support learners in a meaningful way (Roscorla, 2015). What becomes integral to the legislation is allocation of resources and ongoing training of educators and school officials to ensure safe data handling processes.

Federal Protections for Student Privacy.

Family and Educational Rights and Privacy Act (FERPA).

Often referred to as the Buckley Amendment, FERPA was passed in 1974, well before the widespread use of digital data and record-keeping. The law states that, as a condition of receiving federal funds, schools: 1) may not disclose education records without the consent of the student or parent of a minor; and 2) must provide access to education records to students and parents of minors. It broadly defines education records as materials which: (i) contain information directly related to a student; and (ii) are maintained by an educational agency or

institution or by a person acting for such agency or institution (FERPA, 1974, §99.3). Federal case law has remained largely silent on what is considered an "education record" with only two cases decided by the Supreme Court, though neither one addressed digital data (Elliott et al., 2014).

During the growth of Ed Tech companies, the USDOE favored broad disclosure of student data to private vendors. In 2008, the federal government introduced a FERPA regulation that allowed schools to disclose student data, including PII, to a "contractor, consultant, volunteer, or other party" performing "an institutional service or function for which the agency or institution would otherwise use employees" (FERPA, 2008, 34 C.F.R. § 99.31(a) (1)(i)(B)(1)). This rule was based on the "school official" exception which was part of the original FERPA language (FERPA, 1974). The "school official" exception was traditionally used to give teachers access to student information -- the broadened definition gave discretion to schools and educational agencies to release student data to contracted vendors without parental consent (Bartow et al., 2016; Gross, 2014). There are a number of issues with the use of this exception. First, FERPA mandates only apply to educational institutions and not private companies. Once the information leaves the school, the vendor is free to share and sell student data barring any contractual obligations to the school. Second, the vendor can use data for non-educational purposes as long as at least one of the purposes has a "legitimate educational interest" (Bartow et al., 2016).

Experts suggest that the broadening of definitions jumpstarted the current concerns for student privacy (Gross, 2014). Enforcement and monitoring of FERPA compliance fall under the USDOE's Student Privacy Policy Office (SPPO), but parents or students do not have a right to sue for FERPA violations because the Supreme Court ruled that FERPA law does not grant a

private cause of action (Elliott et al., 2014). A complaint to SPPO is the only remedy available to parents under FERPA.

Other Student Privacy Related Federal Legislation.

Other federal laws that protect student privacy include the Protection of Pupil Rights Amendment (PPRA), Federal Trade Commission Act (FTC Act), Children Online Privacy Protection Act (COPPA), and Children's Internet Protection Act (CIPA) (Student Privacy Compass, n.d.-a). PPRA regulates how schools conduct student surveys and is regulated by the USDOE. Like with FERPA, the responsibility for PPRA compliance falls on the school districts, and during the COVID pandemic, PPRA became increasingly important due to frequent surveying of student mental and emotional health (Vance & Sallay, 2020).

As part of its consumer protection mandate, the FTC Act has emerged as the default legislation to regulate Ed Tech companies directly for unfair or deceitful practices (Federal Trade Commission, 2019; Serwin et al., 2014). In 2003, Gateway Learning Corporation, seller of the learning software "Hooked on Phonics," was charged by the FTC with violating the FTC Act for renting consumers' information, including names, addresses, children's age ranges, to third party advertisers and telemarketers "contrary to explicit promises made in its privacy policy" (Federal Trade Commission, 2004, para. 1). As part of the settlement, Gateway Learning was barred from misrepresenting its use of customer information and from applying new privacy policies to existing customers without their consent.

The FTC's regulation of privacy infringements has several limitations. First, the FTC Act does not protect information privacy as an end goal, but only prohibits misleading practices; thus, companies are free to share as much or as little consumer information as they choose provided they include appropriate disclosures in their policies (Serwin et al., 2014). Second,

consumers rarely know when their information is being sold, which means that finding violations of privacy policies is increasingly difficult among thousands of data collectors, analyzers, and brokers (Chander et al., 2008).

Another important legislation, the Children Online Privacy Protection Act of 1998 (COPPA), limits how online providers collect data for minors under the age of 13 (Reyes et al., 2018). While this act was not intended exclusively for education, it has influenced how educational technology companies develop privacy agreements in order to comply with the law (Gross, 2014). It also impacts how educators set policies on the use of YouTube and other external multimedia in elementary and middle schools (FTC, 2019).

The Children's Internet Protection Act (CIPA) governs how public school districts monitor, filter, set acceptable use policies, and educate students on internet practices in schools (Federal Communications Commission, 2017). Under CIPA, schools are required to use an internet filter, to adopt a policy that addresses hacking and unauthorized disclosure of personal information, i.e. Internet Safety Policy, and to educate students about safe online behavior in order to qualify for discounted telecommunications and internet access rates.

A White House report released in 2014 called for an update to federal legislation on student privacy and a push for digital literacy among students and parents:

> The federal government should ensure that data collected in schools is used for educational purposes and continue to support investment and innovation that raises the level of performance across our schools. To promote this innovation, it should explore how to modernize the privacy regulatory framework under [FERPA] and [COPPA] to ensure two complementary goals: 1) protecting students against their data being shared or used inappropriately, especially when that data is gathered in an educational context, and

2) ensuring that innovation in educational technology, including new approaches and business models, have ample opportunity to flourish. (The White House, Executive Office of the President, 2014)

These ambitious goals have yet to materialize, although the FTC has articulated a more proactive goal of holding Ed Tech companies liable not only for their Terms of Service, but also for pledging any public commitments to protect student data (Ross et al., 2021).

Selected State Laws and Policies

In response to proponents of stronger student privacy standards, individual states have begun to pass legislation on student data privacy, however, often without a consistent, comprehensive reach (Vance, 2016). State laws differ dramatically in the liabilities that are imposed on third-party vendors and enforcement practices, and as a result, the tension between innovation and privacy still persists.

California has been at the forefront of protecting student privacy by passing the Student Online Personal Information Protection Act (SOPIPA) in 2014, the most comprehensive legislation on the issue of student privacy in the U.S. at the time (Future of Privacy Forum (FPF), 2016). SOPIPA prohibits Ed Tech vendors from collecting student data to create a personal profile for non-educational purposes and to generate targeted advertising. However, SOPIPA goes further than simply regulates collection of data; it also governs how the data is used and managed (California Department of Justice, 2016). SOPIPA bans scanning of student information for all non-educational, calls for vendors to use reasonable data encryption methods, mandates deletion of student data when requested by the school or district. The law left open the opportunity for the vendors to use de-identified or aggregated data for the purposes of improving and innovating services.

Home to the largest K-12 student population in the country, California heavily influences privacy practices of Ed Tech companies as many of their products are used in multiple states allowing non-California schools to benefit from increased level of privacy standards (FPF, 2016). SOPIPA became effective in California in 2016 (FPF, 2016), and since then at least 23 states, including Hawai‘i, modeled their student privacy legislation after SOPIPA. Overall, forty states have passed 125 laws addressing student privacy regulation since 2013 (Student Privacy Compass, n.d.-b).

The Hawai‘i state law, also titled SOPIPA, prohibits Ed Tech vendors from storing student data for targeted advertising and from selling student personal information (HRS §302A-499, 2016). These protections do not extend to private schools, nor do they mandate that vendors inform schools as to the type of student information collected and how it is used. As it is currently written, the law does little beyond embracing the minimum standards that already exist for Ed Tech vendors. Although based on California's SOPIPA law, Hawai‘i's SOPIPA provisions are weaker in several areas including allowing targeted advertising as long as the student information is not stored (HRS §302A-499, 2016). The Parent Coalition for Student Privacy, which grades each state on student data privacy legislation, gave Hawai‘i state law a grade of "F" on the issues of data collection transparency and penalties for violation (Parent Coalition for Student Privacy, 2019). Hawai‘i received an overall grade of "D+".

In 2021, Governor of Hawai‘i signed into law the Uniform Employee and Student Online Privacy Protection Act (Online Privacy Protection Act) creating additional protections for student privacy, and this time imposing liability directly on educational institutions (HB125, 2021). The law prohibits schools from accessing student personal online accounts, such as social media or non-school email. While it allows for narrowly tailored exceptions for investigations

and safety, the burden remains on the school to show why access to the content is necessary. Unlike SOPIPA, the new law holds both private and public institutions accountable, and states that schools may not access students' personal accounts even when on school-issued devices.

At the time of this writing, the Hawai'i Department of Education (HIDOE) did not have Board-approved district policies on data governance or student data privacy. The Board has approved *Internet Use* policy in 2015 (Hawai'i Board of Education, 2015, Policy 301-6), which articulates proper use of internet services provided by the district, and the HIDOE distributes to parents *Technology Responsible Use Guidelines* (Hawai'i Department of Education, 2016).

National Trends and Best Practices in Student Data Privacy

While the federal government has recognized the need for legislative overhaul, the current law, at least on the federal level, places the burden of compliance with the district administrators. Their duties include careful review of vendor contracts, establishment of complaint processes, and periodic systemwide audits of student data privacy practices. Individual school districts typically establish data governance offices to oversee proper data collection and sharing practices at the district level. SPPO mandates that all school districts develop a Student Privacy Program, which includes policies, procedures, roles, and responsibilities designed to protect student personal identifiable information (U.S. Department of Education, 2015). School districts must have at least one person with designated privacy protection responsibilities. Furthermore, the USDOE has stated that student privacy programs should involve "users and managers of student information, such as data managers, IT staff, and school administrators" (U.S. Department of Education, 2015, p. 2). To support compliance, numerous resources created by privacy and education nonprofits offer student privacy guidelines for school officials.

The emerging consensus from education advocates suggests that educational data should remain free of targeted advertising when based on a student's profile, or perhaps even free of all advertising (Trainor, 2015). Schools should remain places of learning free from commercial advertisements and consumerism, and most advocates suggest that consent to advertising should not even be an option in K-12 schools (Trainor, 2015). Schools and districts should also provide greater transparency as to "what student information they collect, why they collect it, how they use it, and to whom they disclose it" (U.S. Department of Education, 2014, p. 1).

A nonprofit advocacy group Data Quality Campaign (DQC) has recognized that achieving a sustainable balance between educational innovation and privacy requires a concerted effort from schools, state educational agencies, and the federal government (Data Quality Campaign, 2016). On a local level, educators must make a cultural and institutional shift to think of data not simply as a tool for compliance, but one of empowerment and continuous improvement. At the same time, state and federal regulations must set up a framework for this shift through policies, training, and resources that alleviate regulatory burdens and promote meaningful cross-sector data linkages. DQC supports four policy priorities in safeguarding student data:

1. *Measure what matters*: Be clear about what students must achieve and have the data to ensure that all students are on track to succeed.
2. *Make data use possible*: Provide teachers and leaders the flexibility, training, and support they need to answer their questions and take action.
3. *Be transparent and earn trust*: Ensure that every community understands how its schools and students are doing, why data is valuable, and how it is protected and used.

4. *Guarantee access and protect privacy*: Provide teachers and parents timely information on their students and make sure it is kept safe (Data Quality Campaign, 2016).

Another advocacy organization Parent Coalition for Student Privacy represents parents' voices in policy recommendations. They identified five principles in safeguarding student privacy through policy and legislation: 1) Transparency for parents; 2) No commercial use of data; 3) Minimum standards for data encryption and security; 4) Preservation of data ownership that would prohibit re-disclosure by vendors without consent; and 5) Proper enforcement through fines and private right-of-action for parents/students (Parent Coalition for Student Privacy, n.d.).

An influential model bill released in 2015 by the Foundation for Excellence in Education, which became a model student privacy framework for nine state laws, calls for inclusion of five key areas in student data privacy legislation: appointment of a Chief Privacy Officer at the state educational agency; transparency/governance/security in data collection and management; limitations on data collection and disclosure; alignment of vendor practices with adequate privacy and security controls; and parents' rights to view and download data specific to their child's record (Foundation for Excellence in Education, 2015).

It is important to note that both government and advocacy groups caution against stifling data sharing intended to achieve institutional goals and to improve learning pathways. A number of organizations have produced frameworks and practical guidelines to aid district administrators in proper data collection processes to improve data efficacy and lessen teachers' responsibility for data management (Blair et al., 2015; Grama, 2016). One of the issues associated with data sharing is that "technologists and policymakers are not using the same language to describe data protection outcomes" (Grama, 2016, p. 1). Thus, one of the primary recommendations for

educational data sharing is establishing baseline identifiers of information security protections and privacy standards (Grama, 2016). The data governance structure must also be collaborative, involving data management actors, identified as employees who work with data on a daily basis and understand data life cycles, and school leaders who utilize data for decision-making (Blair et al., 2015). Table 1 below offers a snapshot of key issues and recommendations that have come out from prominent advocacy groups.

Chapter 3 - Table 1

Core Issues for Student Privacy Protections Identified by Advocacy Groups

	ORGANIZATIONS		
	Parent Coalition for Student Privacy	Data Quality Campaign	Foundation for Excellence in Education
Transparency/Data inventory	X	X	X
Data security	X	X	X
Chief Privacy Officer			X
Limitation on the type of data collected		X	X
Limit company/vendor practices	X		X
Parental rights			X
Create training for flexible, supported use of data		X	
Enforcement/private right of action	X		

There is some good news on the horizon. The 2019 *State of EdTech Privacy Report* showed improvements in almost all areas of privacy concerns over the previous year, largely motivated by changes in the law: "Legislative initiatives… created a new narrative that highlighted the privacy shortcomings of big tech and social media companies, which led consumers to look more closely at the privacy practices of the products they use. These factors prompted vendors to update their policies at an unprecedented rate" (Kelly et al., 2019, p. 1). But widespread lack of transparency in how companies are using and sharing student data remains a

big issue. The report evaluated privacy policies of the 150 most popular Ed Tech apps and services and found that only 20% met their minimum standards for privacy safeguards. The majority of the evaluated Ed Tech tools failed to provide clear and adequate description of safeguards and data management practices (Kelly et al., 2019). However, this was a substantial increase from 2018 when only 10% of the apps passed the minimum threshold.

What Happens Next?

The challenges and unanswered questions as to student data privacy remain plentiful: What are districts required to do by law? What *should* the districts do even when the law is silent? What are the expectations of the vendors? What are the rights of students and their parents? Currently, the school districts are driven by compliance rather than the spirit of the law, with little transparency provided to parents and students. We are long overdue for a national framework that will clearly identify the rights and responsibilities of all stakeholders when it comes to educational technology. Below I conclude by outlining a few existing gaps in the current landscape in student data privacy that should become part of a future national framework.

Existing Gaps

Lack of Regular Audits of Existing Practices

One of the persistent gaps in safeguarding student data is lack of regular, comprehensive audit processes on safe data sharing practices and the safety of IT protocols. A legislative audit in Kansas revealed that 69% of the responding school districts "did not have a response plan in the event of cyberattack and 28% had not even installed anti-virus software on all school computers" (Bernard & Ritter, 2021, para. 2). A breach of student data can impact not only schools but also parents' financial records and lead to identity theft, resulting in costly lawsuits

and corrective measures (DataBreaches, 2016). In 2017, the average cost of a data breach in education was $245 per compromised record (Schaffhauser, 2017). Regular audits are an essential step toward building a comprehensive protection framework around student privacy. They equip educational leaders with data for better evidence-based allocation of resources, and create continuity between strategic objectives and implementation.

Defining Student Privacy: Setting Up a National Baseline

Defining student data privacy has proven to be a challenge, but a national baseline for student data privacy, and associated audits, would assist school districts in understanding the minimum measures that need to take place. Best practices guidelines, while helpful, lack enforcement needed for an institutional shift. The national baseline would also equip Ed Tech companies with a set of requirements for their products, although, they may still need to meet individual state laws that have higher standards. Student privacy practices can be thought of as 1) *preventive* - practices that improve training, limit collection of student PII, set up airtight agreements and contracts with external vendors, and articulate internal data sharing limitations, and 2) *responsive* - creation of a breach validation process and a response plan in the event of a cyberattack, identification of an incident response team that includes representatives from leadership, legal, IT, public affairs, and other relevant departments.

Additionally, the existing definitions need to be tightened to match the intent of the law. FERPA's exception to allow 'school officials' access to student information is currently used to define the complex relationship between students, parents, school districts, and vendors. However, this exception has been extended beyond its intended purpose. The 'school official' designation should be limited to teachers and other school staff, and new definitions should be written for the emerging Ed Tech paradigm. In the current virtual learning landscape, there are

often more non-school personnel working for private Ed Tech companies with access to student data than actual school employees (Parent Coalition for Student Privacy, 2019).

Transparency: Including Parents in the Conversation for Stronger Protections

Advocacy groups consider transparency to be one of the core principles of safe student data management, and are pushing back against the districts' lack of accountability when outsourcing educational services. They report that districts lack capacity to respond to parents' requests for transparency "due to the sheer number of educational technology vendors used by a typical school district, school districts' lack of control over these companies, and the historical unwillingness of Ed Tech vendors to turn over student data" (The Student Data Privacy Project, n.d., para. 2). As recommended by USDOE, districts should proactively provide easy-to-understand comprehensive data dictionaries (list of shared data points) to parents on the district's website. Transparency will benefit school administrators and teachers in answering parents' inquiries about student privacy, and will promote innovative use of data without community backlash.

Leadership Buy-In: Policy Should be Meaningful on Paper and in Practice

In designing appropriate policies, districts should take into consideration the gap between *innovation-policy* and *knowledge* practices (Davis, 2014). Because policies are time-consuming endeavors and technological innovation move at a rapid speed, inevitable lag emerges. This dynamic is exacerbated by the lack of technical knowledge among institutional policymakers as to "how identity and privacy are technologically instantiated in any given system… and how identity and privacy are managed generally across many different systems" (Davis, 2014, p. 88). What emerges, and is relevant to future research, is the culture clash between *technology*, which is used to solve problems, and *policymaking*, which regulates such solutions and methods of

problem solving. To create meaningful policy that can regulate yet not stifle technology requires expertise from diverse stakeholders who understand technology, education, and legislative processes. It is also critical to be preemptive in designing such policy before state legislators fill the void with hastily written laws after an injurious data breach or parental backlash.

Conclusion

The relationship between educational technology and student privacy remains complex, however, the conversation is moving in the right direction. Legislation and best practices can lead to a comprehensive framework to effectively balance student privacy and innovation. The gaps identified in this article will contribute to the creation of such framework with participation of policymakers, administrators, teachers, vendors, students, and parents. But ultimately, the decisions and solutions must be centered around students. Each solution must be approached with a foundational question of how it will benefit students both educationally and personally. The emerging efforts and trends on this issue demonstrate a strong bipartisan support from diverse groups to prioritize students and to keep education student-centric.

CHAPTER 4. MANUSCRIPT 2

Balancing Student Privacy and Innovation:

Survey of District Administrators Practices and Perceptions (working title)

Abstract

With advent of educational technology and the Big Data economy, schools must now grapple with unprecedented risks to student data privacy. The onus for these protections falls on the teachers and administrators. District administrators, in particular, are responsible for creation of student privacy policies and procedures that comply with federal and state laws but still allow for data-informed learning opportunities. However, understanding of student privacy among school district administrators remains minimal because of its relatively new emergence, rapid changes in technology, and malicious cyber threats. This study assessed practices and perceptions of student data privacy among 28 district administrators at a single school district. The findings revealed overall positive reactions to both practices and perceptions, but highlighting challenges in communication and need for ongoing training to address knowledge gaps.

Introduction

Technology that can reveal innermost thoughts and motives, or can change basic values and behaviors, must be used judiciously and only by qualified professionals under strictly controlled conditions. Education involves individuals, and educational experimentation is human experimentation. The educator must safeguard the privacy of students and their families (Grayson, 1978, p. 195).

Professor Lawrence Grayson (1978) cautioned not only about the risks of educational technology in its capacity to record and store student information with perpetuity, but he also recognized educators' responsibility to keep the classroom as a place of exploration and discovery. With mass collection of digital student information, increases in cyberattacks, and limited guidance on digital record-keeping, contemporary school administrators are facing complex challenges and have limited research to inform their practices to protect student privacy. At a minimum, school districts must comply with state and federal privacy laws (National Center for Education & Statistics, 2010). However, the legislative mandates are not sufficient to protect against malicious data breaches and cyberattacks (Haduong et al., 2015; Strauss, 2017; Weippl & Min Tjoa, 2005). Moreover, parents and privacy groups are raising concerns about lack of transparency in the collection and use of student data by the schools (Foundation for Excellence in Education, 2015; Parent Coalition for Student Privacy, n.d.). These concerns, threats, and legislative mandates form one side of the scale.

On the other side of the scale, student data offers an opportunity to improve students' academic and social development at individual levels (Future of Privacy Forum, 2015; Mandinach & Gummer, 2021). At the school district level, the administrators must balance nurturing these opportunities with emerging concerns for student data privacy. Often involving multiple administrative branches, the district is tasked with designing policies and procedures that allow for innovative school improvement while remaining in compliance with privacy mandates. Yet, their practices and perceptions are often hindered by insufficient resources, training, and understanding of the relatively new phenomenon of data privacy (Bowers et al., 2019; Consortium for School Networking, 2021; Future of Privacy Forum, 2016).

This tension leads to the exploration in my current research. As an exploratory quantitative research, this study surveyed 28 district-level school administrators to assess their perceptions, practices, and gaps in the knowledge in student data privacy at a single school district. This article constitutes Phase 2 a larger three-phase case study of a school district in Hawai‘i. As a unique state with a single-district educational system, Hawai‘i offers an opportunity to examine student data privacy in a unique setting. This study offers an important step toward advancing research and improving safe and innovative use of student data in K-12.

Supporting Literature

The contemporary practice of mass collection and commercialization of online users personal information has become known as the ‘big data’ economy (Lynch, 2017; Marr, 2016). The companies involved justify their commodification of user data with arguments that users’ subscription to the service is optional and a consent to such collection is given at the time of registration. K-12 education, however, occupies a unique space in the age of ‘big data.’ Because of the compulsory nature of primary education, parents and students, as users, have very little control over the collection of their personal information (Lynch, 2017). Instead, the responsibility to protect student, parent, and even teacher privacy falls on school districts as mandated by relevant laws and district board policies (Future of Privacy Forum, 2016; U.S. Department of Education, Privacy Technical Assistance Center, 2015).

Public school districts and district administrators carry the brunt of the burden for creating, maintaining, and enforcing student data privacy protections (Elliott et al., 2014; Haduong et al., 2015). Student records in K-12 and secondary institutions are afforded privacy protection under the Family and Educational Rights and Privacy Act (FERPA) . All institutions receiving federal education funding are bound by this law, which includes all public schools and

most colleges and universities (FERPA Regulations, 1974). However, FERPA's 1974 privacy framework has not been updated to include comprehensive guidelines for digital data collection and sharing (Elliott et al., 2014), and instead school administrators rely on FERPA exceptions and at times creative interpretations of the law to allow for new uses of technology in the classroom (Chapple, 2019; U.S. Department of Education, Family Policy Compliance Office, 2007). Other federal laws that protect student privacy include the Children Online Privacy Protection Act (COPPA), Federal Trade Commission Act (FTC Act), Children's Internet Protection Act (CIPA), and Protection of Pupil Rights Amendment (PPRA) (Student Privacy Compass, n.d.). The Federal Trade Commission regulates the FTC Act and COPPA, holding private vendors liable for how products and online services are sold to children. PPRA, which regulates how schools conduct student surveys, falls under the purview of the U.S. Department of Education, and the responsibility for compliance falls on the school districts directly. During the COVID-19 pandemic, PPRA became increasingly important due to frequent surveying of student mental and emotional health (Vance & Sallay, 2020).

In Hawai‘i, the state law addressing student privacy is the Student Online Personal Information Protection Act (SOPIPA) (HRS §302A-499, 2016) modeled after an identically titled California law. The law prohibits Ed Tech companies from storing or selling student data for targeted advertising. These protections do not extend to private schools, nor do they mandate that vendors inform the schools as to the type of data they collect. While it is based on California's law, Hawai‘i's SOPIPA is more permissive, allowing targeted advertising to students at "an online location based upon that student's current visit to that location, or in response to that student's request for information or feedback" as long as the student information

is not stored for this purpose (HRS §302A-499, 2016). SOPIPA applies to vendors directly and does not create mandates for the school district.

During the COVID-19 pandemic, the Governor of Hawai‘i signed into law the Uniform Employee and Student Online Privacy Protection Act (Online Privacy Protection Act), which states that schools may not require or request (without a clear voluntary statement) that a student disclose information from their personal online accounts, such as social media or non-school email (HB125, 2021). The law allows for narrowly tailored exceptions related to investigations and safety, but the burden remains on the school to show why access to the content is necessary. Unlike SOPIPA, the new law holds both private and public institutions accountable. Another important provision in the law states that schools may not access students' personal accounts even when students use school-issued devices to log-in. This law may have important consequences for Hawai‘i's public schools whose policy allows for unrestricted monitoring of school-issued devices (Hawai‘i Department of Education, 2016). At the time of this writing, the Hawai‘i Department of Education (HIDOE) did not have a state-wide data governance policy or student data protection policy (State of Hawai‘i Board of Education, n.d.). It is important to note that laws in states with large student population, such as California, receive greater attention and guidance from experts (Future of Privacy Forum, 2016). Hawai‘i law does not have a comparable guideline for educators.

As districts expend more funds on privately-owned Ed Tech tools, concerns for student privacy stretch into the uncharted territories that Grayson (1978) warned about (Bettinger et al., 2020). Using exceptions in FERPA, school districts find a balance between sharing student data with private companies and the value of their products to the schools. One study found that while educational technology delivers some benefit to academic achievement, they actually diminish as

the use of Ed Tech increases: “Substituting too heavily into EdTech might be a mistake because production appears to have a strong diminishing marginal rate of technical substitution” (Bettinger et al., 2020).

Additionally, the COVID-19 pandemic brought an awareness to privacy-related issues that had previously been relegated to specialized IT spaces. The 2021 report on Ed Tech leadership found that cybersecurity and the privacy of student data were the top two technology priorities for school districts nationwide (Cybersecurity and Infrastructure Security Agency (CISA), 2020). Yet, the training associated with data privacy and data breaches remains minimal and largely dependent on the importance the district leadership places on these issues (Mandinach & Cotto, 2021). As breaches of data privacy become increasingly critical to K-12 education and awareness of these issues remains low, this study seeks to contribute to a fuller examination of the phenomenon and the potential implications of the tensions existing within it.

Conceptual Framework

Because of the normative and shifting definitions of privacy, a study examining privacy concerns in education is best grounded in a narrowly-tailored conceptual framework to offset the elusive nature of this term (Dourish & Anderson, 2006; Solove, 2006). This study is framed by a conceptual framework that combines *activity theory* and the *contextual integrity (CI)* framework as articulated by Engeström (1987) and Nissenbaum (2010), respectively. The conceptual model consequently employed in this study combines both theories and serves as a foundational point of inquiry. The framework is also critical in analyzing the findings and understanding their meaning within the selected case study site.

Activity theory offers a suitable framework to examine an activity against the backdrop of its context, actors (subjects), and objectives (or objects) (Nardi, 1996). Activity theory has been

adopted as an influential framework in organizational and system-based examinations of technology (Clemmensen et al., 2016; Korpelainen & Kira, 2013). In educational technology research, activity theory frames studies that examine constructivist learning environments, speech and language therapy, and barriers in technology implementation (Bellamy, 1996; Jonassen & Rohrer-Murphy, 1999; Karakus, 2014; Martin, 2008). More recently, researchers have incorporated activity theory in assessing the impact of data analytics in primary and secondary education (Frontiera, 2019).

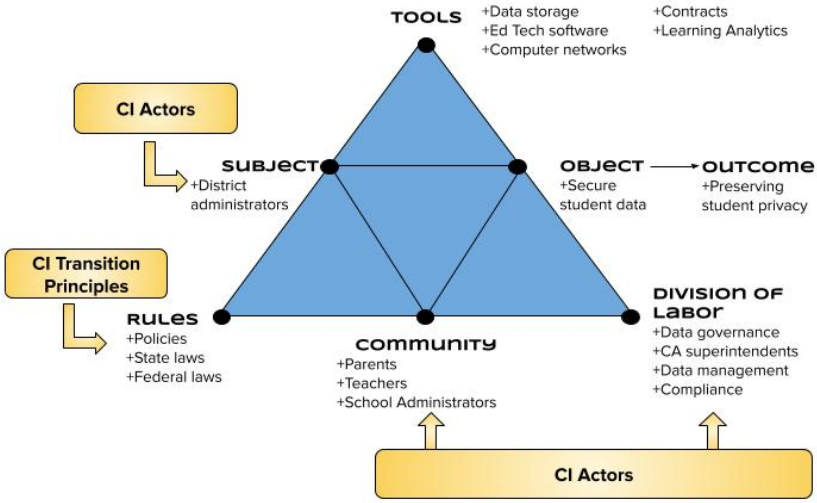
Nissenbaum's (2010) CI framework, like the activity theory, enables researchers to look at a privacy issue within a stipulated context to identify its boundaries through "informational flow," that its "transmission, communication, transfer, distribution, and dissemination" of information (Nissenbaum, 2010, p. 140). Actors, such as people or organizations involved in the transmission of information, are an important contextual element, prompting discussion of who is sending the information, who is receiving it, and about whom the information is transmitted. Other contextual considerations include the transmission principles constraining the flow of information, for example, relevant policies and legislation. Transmission principles encompass both explicit norms, such as laws, and implicit norms, such as practices and procedures that are unique to a specific organization or department.

The conceptual framework combining both theories serves to describe a relationship between district administrators (subjects) and student data privacy (object) within a K-12 public school district (context). Included as mediating elements of the system are the digital tools and data sharing agreements (artifacts), laws and policies (rules), stakeholders such as parents and teachers (community), and the defined roles of the school administrators (division of labor). Reflecting on this through the CI and activity theory lenses, actors, types of information, and

transmission principles, all help cement the students' expectation of privacy (Nissenbaum, 2010). The resulting framework is represented in Figure 1.

Chapter 4 - Figure 1

Conceptual model combining activity theory and CI framework in K-12 school districts



Note: Adapted from the structure of human activity model (Engeström, 1987, p. 78). Reproduced with author's permission.

Methodology

This quantitative exploratory research was conducted using an anonymous online survey with 28 district administrators who were responsible for either securing, monitoring, distributing, interpreting, or managing student data at a single school district. Recognizing that the small number of the participants may signify that the findings are not statistically significant or generalizable, the results are meaningful for the case study because of the unique setting of the site, described in more detail below, and contribute to the overall findings of the three-phase research.

Research Question

This research is based on the following inquiry: What are the perceptions and practices of district-level administrators, especially those with experience and knowledge in data governance, regarding student data privacy?

The research question is informed by gaps in research and the conceptual framework discussed earlier within the selected contextual system (K-12 public school district). The findings from this research are aligned with several elements of the conceptual framework: Subject, Object, Rules, and Community. The research findings deliver answers to the research question, as well as help formulate the context in which subjects are engaged with the activity.

Context

The conceptual framework calls for situating the study within its cultural and historical context. As such, a description of the site becomes critical to understanding the unique organizational structure under which participants regulate student data privacy.

Hawai‘i is home to the only single-district statewide public education system in the country, making it a unique site for exploratory research (Hawai‘i Department of Education (HIDOE), 2021). For purposes of federal reporting and designation, the HIDOE operates both as a State Education Agency (SEA) and a Local Education Agency (LEA) (U.S. Department of Education, 2017). The Superintendent of Education, appointed by the Board of Education, serves as both the Chief State Education Officer and the district superintendent of HIDOE with direct authority over more than 20,000 administrative and teaching personnel (U.S. Department of Education, 2017). Because of its statewide reach, HIDOE is the 10th largest school system in the country with close to 180,000 students and a total of 293 schools, including charter schools

(HIDOE, 2021; U.S. Department of Education, 2017). The typical challenges of managing a large district are exacerbated by the State's geographic distribution across several islands as well as its diversity of cultures and languages.

The HIDOE is divided into seven districts with 15 complex areas that are governed by Complex Area Superintends. The seven 'districts' are so labeled for internal classification purposes and are not considered separate districts for federal reporting. The complex areas operate similarly to LEAs with separate budgets and leadership. HIDOE functions as a tri-level system organized by school level, complex area level, and state/district level. In this study, "district" and "state" are used interchangeably to indicate HIDOE district administration. Because FERPA and other laws hold only federally-recognized LEAs responsible for overseeing student privacy, this research focuses on HIDOE as a single district. As will be discussed in the findings, this unique organizational structure may serve as a barrier for effective student privacy practices because complex areas are not under regulatory pressure to comply, yet they often operate with the autonomy of a school district.

Participant Selection

The participants in the study included district-level administrators who support the district in various capacities. Student privacy issues are cross-departmental and emerge at different levels of district administration, such as, information technology, data governance, and policy and compliance. Because of this organizational structure, the participant list included employees of departments and branches responsible for securing, monitoring, distributing, interpreting, or managing student data.

The sample selected for the study was purposive in order to generate diverse perspectives from complementary but distinct organizational units. I also utilized snowball sampling to

generate social knowledge that is emergent and interactional (Noy, 2008). The selection was focused on participants who are knowledgeable about the particular (Creswell & Plano Clark, 2011; Patton, 2001). After consultation with the HIDOE Data Governance and Analysis Office (DGA), the departments that fell under the selection criteria were: Compliance and Monitoring; Learning and Technology; Curriculum Innovation; Learning Support; Data Governance and Analysis; Policy, Innovation, Planning and Evaluation; Assessment and Accountability; School Transformation Branch; and Information Technology Services. In addition to these departments, the survey was also emailed to institutional analysts whose tasks included monitoring, collection, security, or other work related to student data at the district. These analysts were recommended using snowball sampling by the DGA office. Overall, the estimated number of district administrators who received the email was 76, with 37 participants who either submitted or started the survey. The number of surveys with a complete dataset for this study was 28.

Instrument

The survey instrument used in the study is modeled after a publicly available self-assessment questionnaire created by the Consortium for School Networking (CoSN) and the Trusted Learning Environment (TLE) (Trusted Learning Environment, 2017). This self-assessment for school districts was designed to help a district to assess whether it has reached high standards in policies and procedures for continuous protection of student privacy.

The survey was designed as a cross-sectional questionnaire to assess perceptions and practices of the target population (Creswell, 2014). The survey is composed of 38 questions: 37 are closed-ended questions with 1 open-ended question to capture additional comments and to support the triangulation of data. Of the closed-ended questions, 22 are scaled to measure practices and 13 are scaled to measure perceptions. The final 2 questions collect participants'

background information in alignment with the conceptual framework. Most questions elicit responses on a 5-point scale: 1 (strongly disagree), 2 (somewhat disagree), 3 (neither agree or disagree), 4 (somewhat agree), and 5 (strongly agree). In addition to these five options, questions measuring practices allowed for a 'Don't Know' (DK) option to assess knowledge gaps (Durand & Lambert, 1988). Positive responses (Somewhat Agree or Strongly Agree) represent higher level of compliance and positive perceptions. Questions that received a high mean score indicate that the district is doing well in that area, while questions with a lower mean score suggest that there is room for improvement. The original TLE questionnaire was modified to align with the conceptual framework to measure not only explicit norms of an organization, such as policies, but also to examine implicit ones that represent perceptions, departmental culture, and behavior that are not formally codified or mandated (Nissenbaum, 2011).

Prior to distribution, the survey was pilot-tested with individuals with education or data management expertise to assess the clarity of questions and the dimensions of the survey. The survey was also pilot-tested with a senior level administrator at the selected school district on how well the questions were aligned with the district's organizational structure and internal terminology. The survey was revised after pilot-testing.

A "Don't know" (DK) option was not included in questions measuring perceptions to encourage participants to formulate a meaningful answer based on their experiences or attitudes (Krosnick & Presser, 2010). In contrast, for questions related to school practices, which may require specialized knowledge, the DK option was available to avoid a guessed response and to measure gaps in knowledge among the participants. A single open-ended question was included to capture additional comments and sentiments and to add richness to the survey results (Krosnick & Presser, 2010).

Validity and Reliability

The questionnaire was not previously validated, and despite considerable effort, the search to locate a valid instrument to measure the inquiry was unsuccessful. Some studies have assessed perceptions of data privacy, but these surveys were designed to measure personal thoughts about one's own privacy (Apthorpe et al., 2019; Preibusch, 2013; Shvartzshnaider et al., 2016), or the opinions of privacy experts (Smith, 2016). Instances in which no validated instruments are available, the researcher may design and assess the instrument validity and reliability (Sullivan, 2011). To confirm the validity of the questionnaire, I invited two people with expertise in data management and data analysis to review the instrument. The Cronbach's alpha was run to confirm reliability on the Likert-scaled items after the data were collected, see Table 1. The Cronbach's alpha came back at a strong .914 supporting internal consistency and reliability (Sullivan, 2011).

Chapter 4 - Table 1

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.914	.906	34

Data Collection and Analysis

The anonymous online collection of data was intended to encourage openness that may not be attained in face-to-face conversations. Online surveys also serve a convenient and efficient method for collecting quantitative description of trends, behaviors, or opinions by studying a sample of the population (Creswell, 2014). Qualtrics survey software was used to design the survey and to collect data. The first page of the survey included the informed consent with a checkbox to indicate consent.

The research was approved by the University of Hawai‘i Institutional Review Board (IRB) and the HIDOE prior to data collection. The survey was then distributed via email with 1) an initial invitation to participate, and 2) a reminder notice. The participants were asked to respond within a 10-day period. During pilot testing, the survey was estimated to take no more than 15 minutes to complete. Table 2 presents the timeline for survey distribution and collection.

Chapter 4 - Table 2

Survey Distribution and Response Timeline

Event	Date
Distributed to HIDOE to test for validity and clarity	February 5, 2021
Initial Survey Invitation Email	March 15, 2021
Reminder Survey Email	March 24, 2021
Survey Closing Date	March 25, 2021

After the survey window closed, the data was exported as an Excel spreadsheet with one copy saved as a backup on a password-protected computer and another imported into SPSS. Average time for survey completion was 9 minutes. Approximately, 76 district administrators received the invitation to participate in the survey, and 37 participants either submitted or started the survey. The dataset was reviewed to remove 9 entries that had fewer than 10 responses. The final dataset had 28 (n=28) complete responses. The responses were coded with a 1-5 scale, assigning 1 to ‘Strongly Disagree’ and 5 to ‘Strongly Agree’ as commonly used in Likert scaling (Krosnick & Presser, 2010). Responses marked DK were assigned a distinct number 99 to exclude them from mean and standard deviation calculations (Durand & Lambert, 1988). Analysis of the data included data frequency, measures of central tendency, and variability. Using Excel, I present the findings using tables and graphs for ease of use and access.

Findings

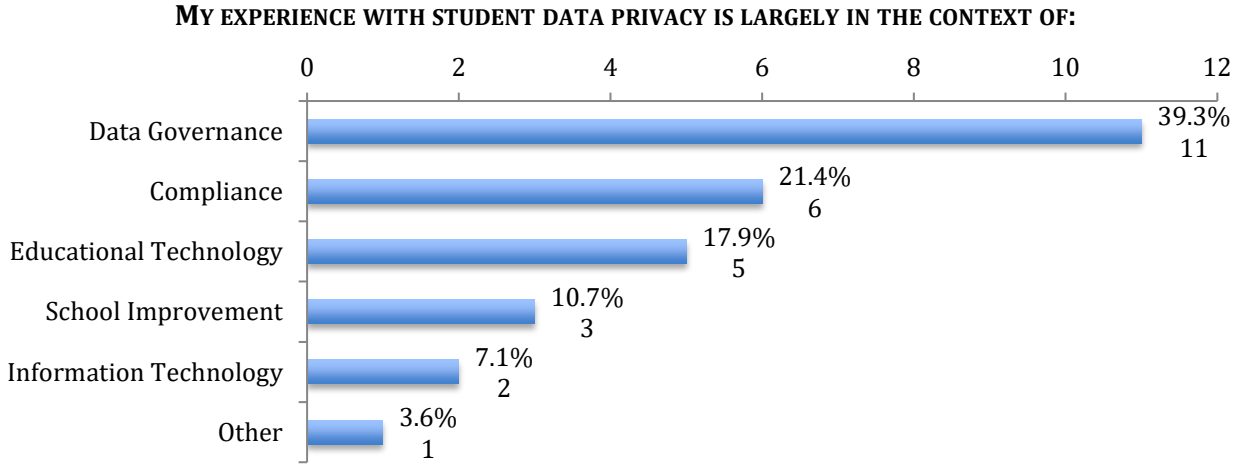
The findings for this research were based on a descriptive statistical analysis identifying trends and "socially important phenomena that have not previously been recognized" (Loeb et al., 2017, p. 1). Descriptive analysis also provides a causal understanding and identifies elements behind relationship variations, and as such was suitable to identify patterns in perceptions and practices in the context of this exploratory study. The following section provides a brief description of the respondents, as well as detailed assessment of Perceptions, and Practices.

Respondents

Respondents represented diverse responsibilities at the district level ranging from data governance, compliance, educational technology, school improvement, and information technology, see Figure 2. The largest representation (39.3%) was among administrators with data governance responsibilities. The information technology sector was underrepresented with only 2 participants. One participant selected 'Other' as their primary role at HIDOE.

Chapter 4 - Figure 2

Survey Participants by Primary Role at The Study Site



The largest grouping of participants had been employed at the District for 15 years or more (45%), while a smaller number (26%) had been at the organization for 0-5 years. Two respondents (7%) preferred not to respond to length of employment. Overall, more than half of the participants had worked with HIDOE for six or more years, as indicated in Table 3. This collective, long-term experience of majority of participants offers a meaningful representation with respect to the practices and implicit norms that exist at the district level.

Chapter 4 - Table 3

Length of employment at HIDOE

	0-5 years	6-15 years	15 or more years	Prefer not to answer
Count	7	6	12	2
%	26%	22%	45%	7%

Perceptions

Participants' perceptions and personal familiarity with student data privacy issues leaned toward the positive with an overall mean of 3.66 (*SD*=1.11). The strongest response was on familiarity with FERPA (*M*=4.57, *SD*=0.69): Almost all respondents indicated that they were somewhat or very familiar with the FERPA law (96%). On the weaker side was the issue of teachers' awareness of student privacy rights (*M*=2.58, *SD*=1.14): Most participants (57%) selected '*Strongly Disagree*' or '*Somewhat Disagree*' when asked if they believed that teachers were aware of the established vetting process.

While FERPA familiarity received a strong response, familiarity with related laws dropped significantly in the following order: Children Online Privacy Protection Act (COPPA) (*M*=3.46, *SD*=1.37); Children's Internet Protection Act (CIPA) (*M*=3.14, *SD*=1.46); Hawai'i Bill SB 2607, Student Online Personal Information Protection Act (*M*=3.00, *SD*=1.57); and Protection of Pupil Rights Amendment (PPRA) (*M*=2.68, *SD*=1.56).

Perceptions of Transparency.

Of interest is the divergence in responses to questions regarding policies for the protection of student data (*M*=4.46, *SD*=0.74) versus those for its transparent use (*M*=4.04, *SD*=0.88) . While both questions received positive perceptions, there was a difference in the degree of agreement with 16 people selecting '*Strongly Agree*' for protection of data and the exact number selecting '*Somewhat Agree*' for transparent use of data, as indicated in Table 4.

Chapter 4 - Table 4

Summary of Survey Responses Regarding Policies and Procedures

School system's policies and procedures set clear expectations for:	Count (%)					Total	M	SD
	Strongly agree	**Somewhat agree**	**Neither agree nor disagree**	**Somewhat disagree**	**Strongly Disagree**			
Protection of student data privacy	16 (57.1%)	10 (35.7%)	1 (3.6%)	1 (3.6%)	0	28 (100%)	4.46	0.74
Transparent use of data	8 (28.6%)	16 (57.1%)	1 (3.6%)	3 (10.7%)	0	28 (100%)	4.04	0.88

Respondents also had a weaker response on the issues of internal transparency. When asked how well informed they were about the type of student data that was collected by online vendors, 46% responded with either neutral or disagreement (*M*=3.39, *SD*=1.07). The less positive reaction on the issue of transparency suggests that there is room for improvement when it comes to transparent use of data, which has been named as one of the key issues in student privacy by parent and privacy advocacy groups (Parent Coalition for Student Privacy, n.d.; U.S. Department of Education, Student Privacy Policy Office, 2021).

Practices

Items that measured practices received above average responses, leaning towards '*Agree*' (M=3.96, SD=0.99). This is moderately higher than the mean of 3.66 for items that measured perceptions; however, items that measured practices included 'Don't know' (DK) responses.

Among responses with the highest mean, suggesting the strongest compliance, were items that addressed the issues of district leadership and working groups. Participants had the most positive response to the existence of a district administrator responsible for data privacy and security policies (Question 5) selecting either '*Somewhat Agree*' (8) or 'S*trongly Agree'* (20). Similarly, 26 responded positively as to the existence of an active data governance committee or a working group (Question 6). However, at the time of data collection, this working group was on hiatus (K. Fukuda, personal communication, 2021), which suggests that either the question was not clear, or the respondents were not aware that the working group was on hiatus. Responses to whether the district had "a documented process to communicate data incidents" (Question 16) also raised an interesting juxtaposition given that it had a high number of DK responses (39%), but respondents with knowledge of the issue had a strong positive response (*M*= 4.47, *SD*=0.62). This suggests that while the district has a process to communicate data incidents, this knowledge was compartmentalized and not widely known across the district offices. Table 5 presents a summary of the strongest responses that measured practices.

Chapter 4 - Table 5

Top Five 'Practices' Responses with the Highest Level of Agreement by Mean

Item	N Valid (Missing/ Don't Know)	*M*	*SD*
Q5. The state office has identified a senior administrator who is responsible for development and implementation of data privacy and data security policies and practices.	28 (0)	4.71	0.46
Q6. The state office has an active data governance committee or a working group.	27 (1)	4.59	0.84
Q15. The school system utilizes a specific role-based process when granting access to educators, staff, and contractors to data and technology systems.	24 (4)	4.54	0.78
Q16. The school system has a documented process in place to communicate data incidents to appropriate stakeholders.	17 (11)	4.47	0.62
Q4. The state office provides transparent and accessible notices regarding the collection and use of student data to the outside community.	28 (0)	4.32	0.72

On the weaker side, the items that had the lowest level of agreement were mostly tied to policies and procedures that take place at the school level, involving teachers and parents. When asked about availability of curriculum to promote internet safety and information literacy (Question 22), 25% of respondents selected 'Somewhat Disagree' or 'Strongly Disagree.' The findings show similar responses to availability of student privacy guides for teachers and availability of student privacy awareness training for parents: Many of the respondents selected DK for this item, but of those that had knowledge of the items, 35% selected either neutral or disagree, see Table 6. These responses highlight the disconnect between the district administrators, who are responsible for creating student privacy safeguards, and the broader community, such as teachers and parents, who benefit from these resources.

Chapter 4 - Table 6

Top Five 'Practices' Responses with the Lowest Level of Agreement by Mean

Item	N Valid (Missing/ Don't Know)	*M*	*SD*
Q22. Schools are required to offer curriculum to promote student information literacy, digital citizenship, and Internet safety.	21 (7)	3.05	1.24
Q25. Teachers are provided with guides for how to clearly answer questions from parents about the collection, use, and protection of student data.	17 (11)	3.06	1.03
Q18. Parents are offered awareness training and resources to learn how to protect children's privacy (ex. a tutorial video on safety of online activities).	18 (10)	3.22	1.26
Q21. Privacy and security of student data is mentioned in training and professional development in all areas of school operations and academics.	26 (2)	3.46	1.33
Q14. The school system has enforceable policies regarding storage of data on local computers, mobile devices, storage devices, and other cloud-related services.	23 (5)	3.52	1.31

Gaps in Knowledge

At the selected school district, respondents were given the DK option on questions that measured practices (rather than perceptions) to assess knowledge gaps among the district administrators. Table 7 highlights questions that received responses with the highest selection of the DK option. These revealed knowledge gaps as to the existence of the following: continuity and recovery plan for data (Question 17); documented process communicating data incidents (Question 16); teacher guides to help respond to questions about student privacy (Question 25); parent awareness training on protecting children's privacy (Question 18); and school curriculum on digital citizenship and internet safety (Question 22). These findings suggest that there is limited cross-departmental communication on IT practices, such as a data recovery plan and incident reporting, and on school-level practices, such as parent training and curriculum.

Chapter 4 - Table 7

Survey Responses with the Highest Number of Missing or "Don't Know" Selections

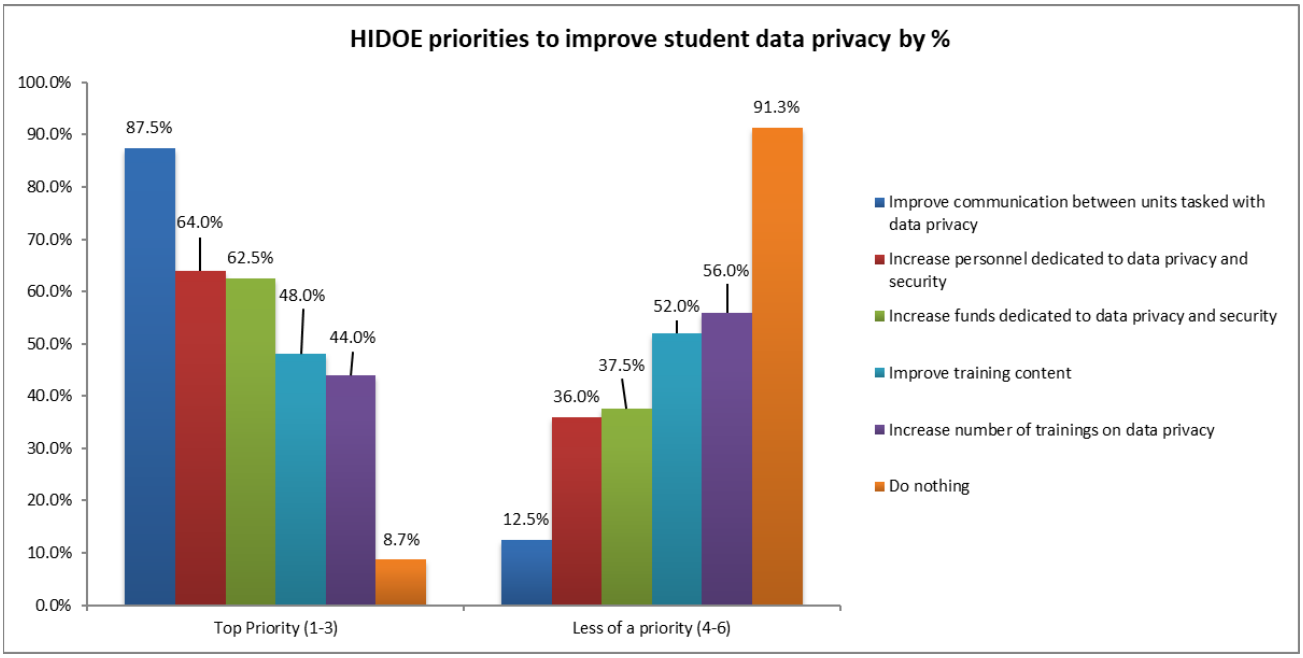
Item	N Valid (Missing/ Don't Know)	*M*	*SD*
Q17. The school system has a continuity and disaster recovery plan for data, which is verified and tested on an established, regular basis.	11 (17)	4.00	0.89
Q16. The school system has a documented process in place to communicate data incidents to appropriate stakeholders.	17 (11)	4.47	0.62
Q25. Teachers are provided with guides for how to clearly answer questions from parents about the collection, use, and protection of student data.	17 (11)	3.06	1.03
Q18. Parents are offered awareness training and resources to learn how to protect children's privacy (ex. a tutorial video on safety of online activities).	18 (10)	3.22	1.26
Q22. Schools are required to offer curriculum to promote student information literacy, digital citizenship, and Internet safety.	21 (7)	3.05	1.24

Identifying Priorities for the District

Finally, the respondents were asked to rank the top priorities for the district to improve student privacy safeguards using the following six options: Improve communication between units tasked with data privacy; Increase personnel dedicated to data privacy and security; Increase funds dedicated to data privacy and security; Increase number of trainings on data privacy; Improve training content; Do nothing. Overwhelmingly, the top priority was given to "improve communication between units" with 87.5% of respondents selecting it as one of their top three choices. Second priority was given to "increase personnel dedicated to data privacy" (64%), with the third priority being to "increase funds" (62.5%). These choices collectively represent both perceptions and practices of administrators based on their years of experience in the district. Figure 3 offers a detailed visualization of the selected priorities.

Chapter 4 - Figure 3

HIDOE Priorities to Improve Data Privacy by Percentage of Respondents



Qualitative Responses to the Survey

The final question in the survey was an open-ended prompt to capture any perceptions and practices that were not revealed otherwise. While these responses did not contribute to the data analysis, they provided additional context for the case study.

Eleven participants responded to the open-ended question. One participant suggested institutionalizing the process of data sharing agreements by adding "a requirement to have student privacy and data sharing included in the procurement process." Three participants gave positive feedback on the work of the DGA office, for example, DGA was "very good about helping educational specialists with data sharing agreements." Two participants responded with less enthusiasm about the DGA office citing insufficient distribution of information, lack of awareness, and the time-consuming process approval process for data sharing agreements. No

comments were made about the role of the IT office. Overall awareness of roles and responsibilities, as well as importance of data privacy was the most frequently cited comment.

Conclusion and Implications

In response to the research question, the findings reveal that the district administrators had above average positive perceptions and practices regarding student privacy at the district level. In the following section, I present the following implications of these findings for the district: need for improvement of cross-departmental (horizontal) and cross-level (vertical) communication, and creation of a strategic training framework I further explore meaning of the data results through the conceptual framework and present the study's limitations.

Implications

Improving Cross-Departmental and Vertical Communication.

Across the surveyed departments, the findings suggest that the district administrators may lack requisite familiarity with IT procedures, such as processes to communicate data incidents and data recovery plans. Responses to IT-related questions had the highest DK incidence: communication of data incidents (11) and data recovery plan (17). In comparison, knowledge of non-IT district processes received relatively low DK responses; for example, inclusion of data privacy clauses in procurement contracts (4 DK) and a vetting process for external vendors (2 DK). These findings are limited by the low number of IT personnel participants (2) responding, but they suggest that IT practices may not be effectively communicated or shared with the non-IT district administrators. Information related to IT practices should be added to future communication on data governance. With the rise of cybersecurity concerns in schools (CISA, 2020), district administrators must be prepared to respond swiftly and uniformly in times of

crises. This may mean addressing cultural and generational hesitancy to gain IT literacy, as well as designing trainings that are both accessible and informative to non-IT personnel.

The knowledge gaps identified in the survey also revealed limited knowledge of practices that take place at the school level. The tri-level organizational system of HIDOE may contribute to this issue. The district/state level leadership defers to complex area superintendents for distribution of guidelines on student privacy. In turn, complex areas, which are burdened with instructional and operational responsibilities, may forego or de-prioritize student privacy training because complex areas are not directly liable for federal regulatory compliance. The middle level of the organization can create a barrier in effective top-down distribution of resources and awareness raising. Designation of a student privacy officer at each complex area will maintain consistent channels of communication across the three levels of organization, and will ensure that the schools' have equity in resources and consistency in messaging.

Additionally, a district website dedicated to student privacy may provide an effective method of communication across organizational barriers and aid in improving transparency. U.S. DOE has recommended utilizing websites for "timely dissemination of information to the school community" (U.S. Department of Education, Student Privacy Policy Office, 2021, p. 1). A website will also allow for up-to-date audience-based distribution of information to teachers, principals, students, and parents, and serve as a central repository of training materials.

Improved communication and increase in personnel dedicated to student privacy also emerged as the top two priorities for the respondents. References to lack of awareness and need for better communication were most frequently referenced in the open-ended question of the survey. These additional data support the implication for the need for effective communication

methods and establishing reliable channels of information distribution through dedicated personnel.

Creating a Strategic Training Framework for Continuous Awareness.

The importance that educators place on FERPA is partly due to the law's longevity and its broad coverage of student records in both K-12 and higher education spheres. However, non-compliance with other laws, such as PPRA, can lead to equally damaging consequences for the districts. The survey respondents' lowered familiarity with PPRA is particularly significant because of the schools' increased use of student surveys to assess mental and emotional wellbeing during COVID-19 (Vance & Sallay, 2020). The lack of familiarity with PPRA is not unique to HIDOE but presents itself as an issue across the country (U.S. Department of Education, Student Privacy Policy Office, 2021). Additionally, non-compliance with Hawai‘i's Online Privacy Protection Act (HB125, 2021) can leave the district open to substantial monetary damages. Unlike FERPA, which only allows for complaints to the U.S. Department of Education, the Online Privacy Protection Act created a private right-of-action for students or parents to sue the district directly.

As such, increased training on relevant state and federal laws should be an important short-term goal for the district. State laws, in particular, are less likely to receive attention in the media, and organizational training becomes the primary means of awareness raising for administrators. As laws and policies constantly evolve and devolve in their importance, the short-term goals for training should be bolstered by a long-term goal to have a professional development framework for administrators that mitigates the tension between changes in the rules and the lag in the administrators' awareness and implementation practices.

Alignment with the Conceptual Framework

The contextual integrity (CI) framework and Activity Theory allow room for tensions and contradictions that arise from the complexity of the human activity system, and these contradictions become "the driving force of change and development in activity systems" (Engeström, 1987, p. 6). The process is iterative – old tensions are resolved while new ones emerge as social norms are transformed by new technology or regulations. In this regard, the complex activity of protecting student privacy is a constant process of transformation and learning for school administrators. In this study, the *subject* (district administrators) is part of a complex system that determines their impact on the *outcome* (protecting student data privacy). As the system components undergo change, for example *Rules*, so do the subject's behavior and the level of importance that is placed on the object. Using the conceptual framework discussed earlier, the results reveal that protecting student privacy is not simply a routine task; instead, it is deeply contextual and culturally normative process that affects a whole system of behaviors.

When examining the survey responses contextually, a discrepancy emerged between the respondents' perceptions toward policies that protect student data and those that promote transparency in the use of data. This tension is aligned with Nissenbaum's (2010) CI framework which highlights the need for an *appropriate* information flow even when the information is secure. Another tension emerged between implicit and explicit norms at the district level. A relatively large number of respondents indicated that they were not aware of a data recovery plan even though those with the knowledge on the topic responded positively. These findings suggest that having processes for data recovery and incident reporting (explicit norms) are weakened if cross-departmental awareness of them (implicit norms) is lacking.

Both activity theory and the CI framework place strong emphasis on *Rules*, or *Transmission Principles*, that constrain the activity at issue. Here, federal and state laws, as well as Board of Education policies, provide critical constraints for district administrators in safeguarding student data. Familiarity with FERPA received strong responses within the survey responses, but familiarity with PPRA and Hawai‘i SOPIPA law was considerably less evident even though, at the time of data collection, PPRA compliance had become critical for COVID-19-related student surveys. As *Tools* change (for example, increased reliance on surveys), the level of importance of certain *Rules* changes (PPRA becomes more important), and consequently, the subject's behavior toward its objective must change as well. However, another tension here is the lag between the transformation and the subject's awareness of this transformation.

The enactment of Hawai‘i's Student Online Privacy Protection Act (HB125, 2021) brings to light another contradiction in the *Rules* element of the activity system. The act is in conflict with the current district policy on the use of technology, which allows HIDOE to monitor student devices and accounts accessing the HIDOE networks with no expectation of privacy (Hawai‘i Department of Education, 2016, section 3). Even though the state law trumps district policies, district administrators are less likely to act on the new law as awareness of new rules takes time to normalize. Instead, administrators are more likely to follow the district's policy posted on the District's website because it is both familiar and well-established. Looking at the Online Privacy Act and the District's technology use policy contextually, the *Rules'* constrain on the activity emerges as both hierarchical and temporal – some rules preempt others because of the familiarity and timing of implicit norms even when explicit norms carry more weight. The context is then

critical in not only resolving the contradiction, but also creating a framework that would address future tensions as they inevitably emerge.

Finally, the findings highlight a disconnect between the district and school-level practices involving teachers, parents, and students (*Community)*. Survey results related to school level indicated the most knowledge gaps; for example, awareness training for parents (10 DK responses), teacher guides for protection of student data (11 DK responses), and student curriculum for information literacy (7 DK responses). Moreover, respondents with knowledge of these practices reported relatively low agreement as to the existence of these practices with the mean scores of 3.22 (*SD*=1.26) for parent training; 3.05 (*SD*=1.24) for student curriculum; and 3.06 (*SD*=1.03) for teacher guides. This suggests a tension between the district and the *Community* element of the activity system which manifests itself in lessened communication about practices at the school level and fewer practices that support student privacy at schools.

Limitations

This study was conducted in the midst of the COVID-19 pandemic, which not only overloaded the capacity of school districts to deliver effective instruction, but also brought a spotlight on the issue of data privacy as schools became reliant almost entirely on privately-owned distance learning platforms. Because student privacy had become a sensitive and at times controversial topic, and because the participating school administrators were operating in a crisis mode, the content of the responses and the response rate may have been limited by these exigent circumstances. Also, the study focused on a single school district that operates as a state educational agency (SEA). It is the only SEA and LEA in the country, and as such, the findings may not be generalizable. Anonymity of the respondents provided both an advantage and limitation to the study. On the one hand, the participants were more likely to provide honest

responses, but the analysis of the responses had to be more general because the practices and perceptions could not be linked to specific roles at the district.

Researcher's Role

I had worked with HIDOE on grant-funded collaborative projects in Spring and Fall of 2020, producing a landscape report on Hawai‘i's computer science education in June 2020. In January-February, 2021, I joined the DGA office of HIDOE on a part-time assignment to assist with data governance tasks at the district. During that time, I did not collect data for this research to avoid any perceived or actual conflict of interest. Some of the information described here regarding the district's data governance practices was gained through personal knowledge and experience.

Although the invitation to participate in the research study was sent after my contract with HIDOE had expired, some of the recipients may have perceived me as an employee and representative of the DGA office, which may have affected their decisions to participate or the responses provided. However, anonymous nature of the survey mitigated this limitation.

Conclusion and Future Research

The findings of this research provide answers to the central research question, namely the practices and perceptions of the district administrators in regards to student privacy protections. Revealing tensions and contradictions through the conceptual framework lens, the study produces a number of meaningful opportunities for future research; for example, cross organizational comparison of student privacy practices across two or more districts; perceptions of student data transparency among parents at the selected study site; and review of the privacy policies of contracted Ed Tech vendors to identify vulnerabilities in the district's vetting process.

On a national scale, a research topic may include an empirical study that compares school data breach incidents between two states with divergent student privacy laws.

As Phase 2 of a larger exploratory case study, this research aims to contribute not only to the growing body of literature on the topic of student data privacy, but also to present meaningful findings within the selected study site. Collectively, the three phases of the study deliver a comprehensive look at the emerging issues on the national level, the district level, and the school level. The results of this study, in combination with Phases 1 and 3, will prove useful to both policymakers and educators, and help design safe and student-centric data sharing practices.

CHAPTER 5. MANUSCRIPT 3

Balancing Student Privacy and Innovation: Assessing Experiences of School Teachers and Technology Coordinators (working title)

Abstract

One of the growing issues in K-12 education is the delicate balance between innovative use and ethical boundaries of educational technology. Educators have come to rely on online learning platforms and their detailed customized assessments; however, the use of educational technology comes with risks of exposure of student personal information, infringements on privacy, and overused surveillance. Using five semi-structured interviews, the study revealed experiences with student data privacy of school personnel who are responsible for technology use in classrooms. The participants also shared existing enablers and barriers toward implementation of data privacy safeguards. The findings suggest that data privacy in schools still carries unresolved issues, such as the need for increased awareness and strategic training across the school district; however, community and designated expert support emerged as strong enablers toward implementation and shared willingness to learn. This article presents qualitative research as part of a larger exploratory case study of a single school district in Hawai‘i.

Introduction

In July of 2019, parents of some 70,000 public school students in Hawai‘i received a letter from the school district stating that their children’s names, addresses, grades, test scores, and other personal information had been exposed to unauthorized access because of improper security protocols (*My Future Hawai‘i Possible Data Exposure FAQ*, 2019). Unfortunately, this is one of thousands of annual incidents as school districts become increasingly vulnerable to data

breaches and cyberattacks (Cybersecurity and Infrastructure Security Agency (CISA), 2020; Doran, 2018; Hobbs, 2017; Levin, 2021). Ubiquitous use of educational technology (Ed Tech) in the classroom generates student digital data and digital footprints with each use (Carmel et al., 2019; Edwards, 2015; Reidenberg et al., 2013). In this complex environment, teachers and technology resource educators emerge as the decision-makers of how Ed Tech is used in schools.

Teachers also rely on thousands of student data points to inform their teaching practices, and much of these data are collected and stored by private vendors. However, the teacher training on responsible use of data and student data privacy has remained stagnant (Mandinach & Cotto, 2021). As teachers increasingly rely on Ed Tech to support instruction, it becomes imperative that teachers and tech support coordinators receive relevant resources that help them implement safe data practices in line with both legislative mandates and best practices. Through five semi-structured interviews with teachers and tech support educators at a single school district in Hawai‘i, this study explores the participants' experiences, as well as existing barriers and enablers, in their understanding and implementation of student data privacy.

The following article presents a final phase in a three-part exploratory case study of a single school district in Hawai‘i. The case study was designed to examine the issue of K-12 student privacy at three levels: an overview of national best practices (Phase 1), survey to assess school district administrators' perceptions and practices (Phase 2), and finally, interviews with teachers and technology support staff at school level (Phase 3). Collectively, the case study offers examination of the increasingly important issue of student privacy from diverse perspectives and provides assessment of existing gaps in practices and implementation.

Supporting Literature

Student Privacy Legislation Offers Limited Protections

Student records are generally afforded privacy protections by federal and state laws, but the primary legislation on this issue, the Family Educational Rights and Privacy Act (FERPA, 1974), has yet to include a comprehensive set of guidelines related to digital records (Elliott et al., 2014). Using FERPA's "school official" exception, schools widely share student data with Ed Tech vendors without parental consent citing that their services serve an educational purpose (Bartow et al., 2016); FERPA, 1974, §1232g(b)).

Two other federal laws play an important role in protecting student privacy: the Protection of Pupil Rights Amendment (PPRA) and the Federal Trade Commission Act (FTC Act) (Feng & Papadopoulos, 2018). PPRA regulates how school districts collect and administer student surveys, mandating that schools seek parental consent before collecting sensitive student information (Reidenberg et al., 2013). Since 2020, PPRA gained traction in the discussions on student privacy because of the increased use of surveys at schools to assess students' emotional and mental health (Vance & Sallay, 2020). Unlike FERPA and PPRA, the FTC Act is governed by the Federal Trade Commission and holds Ed Tech vendors directly liable for unfair or deceitful practices (Serwin et al., 2014). However, the FTC Act does not articulate information privacy as its end goal, and vendors are liable only within the parameters of the company's terms of service. Also, it is difficult to know what information is being tracked for non-educational purposes, which means that violations of privacy policies are likely to go unnoticed (Chander, Gelman, & Radin, 2008).

Absence of comprehensive federal standards for student data protections has led to enactment of laws in 40 states, including Hawai‘i, that grant additional protections to student

privacy (Vance, 2016). But the practices remain inconsistent and piecemeal as each district re-interprets the new legislation with its own taxonomy of terms and best practices (Dey, 2021). Student privacy in Hawai‘i is regulated by federal laws described above and two state laws: Student Online Personal Information Protection (SOPIPA) (HRS §302A-499, 2016), which imposes limitations on Ed Tech companies, and Uniform Employee and Student Online Privacy Protection Act (HB125, 2021), which holds schools liable for unauthorized access to students' social media and personal email accounts. The latter may have important consequences for the schools' policy on technology use which currently allows unrestricted monitoring of school-issued student devices (Hawai‘i Department of Education, 2016). Currently, the Hawai‘i Department of Education (HIDOE) does not have a Board-approved policy on data governance or student data protection.

Creating a Training Framework That Balances Privacy and Innovation

Future of Privacy Forum (FPF) defined student data privacy as "responsible, ethical, and equitable collection, use, sharing, and protection of student data" (Future of Privacy Forum, 2021b, p. 5). A key challenge to setting up uniform federal standards for student data privacy is creating allowances for use of student data in evidence-based academic and socioemotional programs (Lestch, 2015). This is particularly important for struggling schools that focus their efforts on closing the achievement gaps (Lee, 2021). District administrators are tasked with designing student privacy policies, while school principals and vice-principals play an important role in implementation of these policies by modeling best practices and initiating a culture of safety when it comes to student data privacy (Bowers et al., 2019; Lim et al., 2015). But ultimately, student data privacy practices are exercised by teachers in their day-to-day student engagement. A legal framework to protect student privacy must then create pathways for

strategic data collection to support students (Roscorla, 2015) and to train educators and school administrators on safe data use.

Teacher professional development (PD) modules frequently exclude information on student data privacy requirements (Vega & Robb, 2019). Teachers also do not always see the connection between student privacy laws and the safety of Ed Tech products, and may not consider themselves an important part of the student data privacy practices (Center for Democracy & Technology, 2020). Consequently, training materials should include information on teachers' role in privacy compliance (Mandinach & Cotto, 2021). FPF created a 300-page professional development resource using real-life scenarios to help teachers understand student privacy and data ethics issues (Future of Privacy Forum, 2021a).

The Privacy Paradox

Despite increased awareness of risks associated with the use of technology, schools widely accept and welcome Ed Tech tools because of their value and utility in administrative and instructional support (Bettinger et al., 2020; Borthwick et al., 2015). Studies that analyze consumer behavior have found that convenience and immediate benefits often outweighs privacy considerations (Athey et al., 2017; Dinev et al., 2013) even when people express concerns about privacy (Norberg et al., 2007). This so-called "privacy paradox," described as "the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors" (Norbert et al., 2007, p. 100), has been documented with online users. Experiments with consumer behavior suggest that "consumers need to be protected from themselves, above and beyond the protection given by a notice and choice regime, to ensure that small incentives, search costs, or misdirection are not able to slant their choices" (Athey et al., 2017, p. 4). By the same logic, school administrators and teachers are more likely

to engage in 'risky' behavior with technology when presented with immediate benefits, unless there are strict policies and procedures in place to regulate it. Teachers have also reported a lack of awareness of institutional policies and definitions of "digital privacy," even with high use of digital tools (Leatham, 2017).

The Value of Educational Technology

A study by RAND Corporation in late 2020 revealed that, despite thousands of dollars spent on distance learning programs and instructional support software, teachers overwhelmingly reported burnout and insufficient resources during COVID-19 (Diliberti & Kaufman, 2020). Even when schools returned to in-person instruction, the multitude of apps and software adapted during COVID-19 pandemic added to the already heavy workload of technology resource teachers (Anand & Bergen, 2021). While schools struggled to come up with personnel and resources to support teachers during distance learning, the Ed Tech companies reported millions of dollars in revenues and have been exponentially increasing in value since the pandemic: GoGuardian – a popular school monitoring AI program – was recently valued at $1 billion (Anand & Bergen, 2021; Keierleber, 2020). The private Ed Tech companies are in effect being financed by public school funds, but few districts have undertaken comprehensive accounting of how much money is being spent on Ed Tech tools and the impact of this spending on schools' other priorities: "We are spending billions of dollars on technology with almost no information about which tools actually work, where, and why" (Epstein, 2021).

Exacerbating the issue are the tensions that at times emerge between educators' priorities and parent advocacy groups. For example, calls for limited school surveillance may lead to counterarguments from teachers who suggest that tracking students' online allows them to limit unauthorized activities and redirect students to assignments (Anand & Bergen, 2021). Also,

project management and cloud storage software that amass sensitive student information have become instrumental to administrators' responsibilities for accreditation, reporting, and compliance (Frontiera, 2019; Lim et al., 2015; Reidenberg et al., 2013).

Unintended Consequences of Regulating Student Privacy

The recently enacted state laws on student privacy emphasize the need for transparency and limited data collection, but none had created mandates for teacher and administrator training on safe use of data (Vance, 2016). Enactment of new mandates without appropriate training – particularly on unfamiliar issues – poses a risk that the teachers will either disregard the mandate or overcompensate. The laws can create administrative burdens with a detrimental impact on students' educational opportunities (Vance, 2016).

In addition, student privacy laws impose only the minimum standards, which the districts may interpret inconsistently. For example, Chicago Public Schools (CPS) cited the Illinois Student Online Personal Protection Act as the reason for barring access to well-trusted technology programs such as Code.org and Adobe software (Dey, 2021). While other districts in the state continued to use these programs, CPS's interpretation was more restrictive leading to loss of access for students and teachers who relied on the software to design curricula. Students weighed in as well about detrimental impact of the privacy laws on their day-to-day interactions:

> CPS is blocking any further payments to [Student Newspapers Online], which makes publishing tricky... As this situation unfolds, it has become clear to me how bureaucratic decisions from Chicago Public Schools' central office can unintentionally harm students. (Camacho, 2021, para. 4)

In Hawai‘i, principals reported that restrictive interpretation of FERPA resembled a barrier when one school was "blocked from digitally accessing data for students they had taught

during the previous year school" and this restricted access prevented "interaction with data more efficiently" (Frontiera, 2019, p. 118).

Conceptual Framework

This research is informed by a conceptual framework combining *activity theory* and the *contextual integrity (CI)* framework as articulated by Engeström (1987) and Nissenbaum (2010), respectively. Both CI and Activity Theory allow room for tensions and contradictions that arise from the complexity of the human activity system, and these contradictions become "the driving force of change and development" (Engeström, 2015, p. XV). The process is iterative – old tensions are resolved while new ones emerge as social norms are transformed by new technology or regulations. In this regard, protecting student privacy is a constant process of transformation and learning (Kaptelinin, 2005).

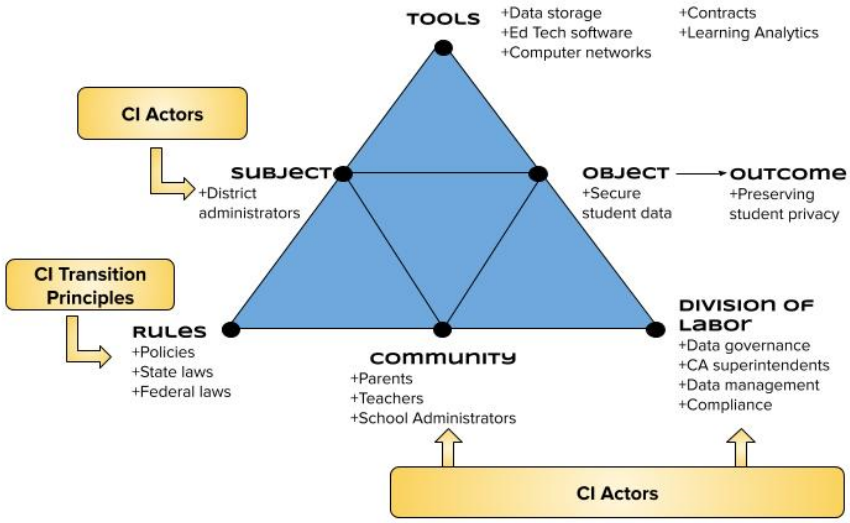
In education context, information flow has both technical and social elements and requires a structural, contextual examination (Bijker, 1997). Students' expectation of privacy is determined by *actors* involved in data transmission, the technology used, and the purpose for which it is shared (Nissenbaum, 2011). The *transmission principles*, articulated by CI, represent elements, such as legislation and policies, that constrain the flow of information. Activity theory further offers a lens to describe the relationship between district administrators (subjects) and student data privacy (object) within a K-12 public school district (context). Included as mediating elements of the system, such as training materials and data sharing agreements (tools), laws and policies (rules), teachers and parents (community), and the defined roles of the school personnel (division of labor).

The conceptual framework combines both theories and serves as a foundational point of inquiry for this research with focus on *Community* and *Division of Labor* elements of the system.

The findings help identify tensions and connect different components of the activity system by examining the experiences of teachers and technology coordinators in the given context. It also connects the findings of the current research and their meaning to other phases of the overarching case study. The resulting conceptual framework is represented in Figure 1.

Chapter 5 - Figure 1

Conceptual model combining activity theory and contextual integrity framework in K-12 school districts



Note: Adapted from the structure of human activity (Engeström, 1987, p. 78). Reproduced with author's permission.

Methodology

This study presents qualitative empirical findings from five interviews with teachers and technology coordinators at HIDOE to assess their experiences with student data privacy. The results contribute to the overarching exploratory case study with focus on a single school district. The current research built on the findings from the previous two phases of the case study and

sought to examine experiences of teachers and technology coordinators who work on student privacy related tasks. The interview questions for this phase of the case study were partly informed by the findings in the previous research phases to have an in-depth understanding of the emerging trends and to solidify the context for the study site.

Research Questions

The following research questions form the basis of the current inquiry:

1) What are the experiences of school-level teachers and administrators regarding effective student data privacy?
2) What are the enablers and barriers to implementation of student data privacy practices in the selected case study district?

The questions are framed by the conceptual model described earlier to look at teachers and school-level personnel as *Community*, or *actors*, of the activity system. This paradigm helps uncover the tensions and connections between *Community*, as the mediating artefact, and other elements of the conceptual framework.

Context and Case Study Site

As the only single-district public education system in the country, the Hawai‘i Department of Education (HIDOE) has many unique attributes that are suitable for an exploratory case study (Hawai‘i Department of Education, 2021). It operates as a State Education Agency (SEA) and a Local Education Agency (LEA) for purposes of federal reporting (U.S. Department of Education, 2017), and it is the only agency in the country that serves both functions. Consequently, the Superintendent of Education, serves as both the Chief State Education Officer and the district superintendent overseeing more than 20,000 administrative

and teaching personnel (U.S. Department of Education, 2017). HIDOE is also the 10th largest school district in the country with almost 180,000 students and a total of 293 schools public and charter schools; however, as a state agency it oversees a relatively small number of students ranking 40th among the states (Hawai‘i Department of Education, 2019; U.S. Department of Education, 2017). Hawai‘i’s geographic distribution across several islands and the State’s cultural diversity contribute to the uniqueness of the school district.

The private school enrollment in the State is relatively high as compared to the rest of the country, and students classified as socioeconomically disadvantaged comprise 47% of Hawai‘i’s public school population (Hawai’i Department of Education, 2021; National Center for Education Statistics, 2015). Analysis of the HIDOE data revealed that the State’s rural areas served a higher percentage of economically disadvantaged students, Table 1. English Language Learners make up 9.2% of public school students which is slightly below the national average of 10.2 percent (National Center for Education Statistics, 2021).

Chapter 5 - Table 1

Economically Disadvantaged HIDOE Students by County in SY2019-20 (Hawai'i Department of Education, 2021, Table 20, p. 13)

	Statewide	Oahu County	Hawai'i County	Maui County	Kauai County
Total student enrollment	179,331	113,703	23,411	21,051	9,289
# of students economically disadvantaged	84,993	49,345	13,479	9,852	4,197
% of students economically disadvantaged	47%	43%	58%*	47%	45%

Note. This table represents analysis of the data reported by HIDOE which defined 'Economically Disadvantaged' as "students whose families meet the income qualifications for the federal free/reduced-cost lunch program [and] an indicator of school-community poverty" (Hawai'i Department of Education, 2021, p. 20).

*The percentage of Hawai'i County economically disadvantaged students is likely to be higher because two complexes in the County did not report data on the percent of economically disadvantaged students.

HIDOE is administratively delineated into seven 'districts' and 15 complex areas. It is critical to keep in mind that HIDOE 'districts' are organizational labels only and are not considered separate districts for federal reporting purposes. Student privacy laws, such as FERPA, apply to federally-designated school districts, or LEAs. Accordingly, this research focuses on HIDOE as a single district. Throughout the interviews, participants referred to district administrators as "state," while I use "district" and "state" interchangeably to mean HIDOE. In this article references to "district office" connote state-level administration of HIDOE.

The 15 complex areas have relative autonomy with separate budgets and leadership. As such, HIDOE functions as a tri-level governance system organized by school level, complex area

level, and state level. As will be discussed in the findings, this unique organizational structure may serve as a barrier for effective student privacy practices because complex areas are not under regulatory pressure to comply with federal and state mandates, yet they often operate with the autonomy of a school district.

The HIDOE Data Governance and Analysis (DGA) office oversees district-wide data sharing and data governance processes, including processes for schools to inquire about the safety of an Ed Tech software and to create a data sharing agreement (DSA) with a vendor. DGA serves as an intermediary to draft and negotiate data sharing agreements with Ed Tech vendors on behalf of the school, complex area, or the state. The DGA's work is limited with only two full-time employees overseeing student privacy and data sharing tasks for the entire district. Schools and complex areas may designate liaisons to collaborate with the DGA office; however, these positions are not mandated or officially designated. The DGA staff are also responsible for statewide trainings on student privacy and research-related data sharing.

Participant Selection

Five participants volunteered to be interviewed for the study. The participants included 2 school teachers and technology coordinators, 2 complex area technology resource teachers, and 1 complex area school renewal specialist (responsible for Ed Tech integration for the complex area). All five participants work on the island of Oʻahu. The sample selected for the study was purposive and snowball to generate social knowledge that is emergent and interactional (Noy, 2008). The selection was focused on participants who are knowledgeable about the particular phenomenon (Creswell & Plano Clark, 2011; Patton, 2001).

The criteria for participation required that the participants: 1) be employed at HIDOE, the selected case study site, and 2) provide support and guidance for educational technology at

school level. The criteria were aligned with the case study to respond to the proposed research questions and to generate overall exploration of student data privacy at the district. Participants were recruited through Hawai‘i Society for Technology in Education (HSTE). School-based participants were responsible for supporting teachers, administrators, and students at their respective schools. Complex area-level participants supported teachers and administrators for the complex area.

In qualitative research, participants are part of the descriptive narrative, and their stories should be associated with identities beyond the anonymity of a code or a number (Seidman, 2006). Finding pseudonyms for participants is a “sensitive task” that needs to take into consideration participants’ identifying attributes (Seidman, 2006, p. 9). For this study, the names of the participants have been replaced by pseudonyms consistent with their gender. Other identifying elements, such as school name or location, are not attributed to them to maintain confidentiality. The pseudonyms used are Carmen, Tasha, Hoku, Kanoe, and Mario.

Instrument and Data Collection

The primary instrument in semi-structured interview research is the researcher (Chenail, 2011). The researcher’s facilitation with the interviewee sets up the flow of communication and prompts allowing for rich data to emerge. When performing as an instrument, the researcher’s role is to construct open-ended questions that “provide openings through which interviewees can contribute their insiders’ perspectives with little or no limitations imposed by more closed-ended questions” (Chenail, 2011).

The University of Hawai‘i Institutional Review Board (IRB) and HIDOE approved the research activities prior to collection of data. Data for this qualitative study was collected through five 60-minute semi-structured interviews in May-June, 2021. The interviews took place

online using Zoom platform. After introduction of the study, participants were asked eight semi-structured questions with clarifying questions in between (Appendix C). The questions were informed by the supporting literature and were open-ended to encourage in-depth participation and elaboration on details relevant to the research questions (Seidman, 2006).

While there are limitations with conducting research in virtual spaces, there are some clear advantages, such as overcoming geographical barriers, convenience, and participants' control over of the interview space (Nehls et al., 2015). Furthermore, at the time of data collection, the University IRB office had imposed limitations on in-person research and HIDOE meetings have been moved to virtual environments due to the global pandemic.

Data Analysis

The audio recordings of the interviews were auto-transcribed using Otter.ai software. I listened to the audio recordings and made corrections to the transcriptions, adding nonverbal cues. Transcriptions were re-read again for accuracy and emergence of themes (Creswell, 2014). Each transcription was subsequently uploaded to NVIVO data analysis software and coded and recoded to reveal emerging themes in alignment with the research questions and conceptual framework. Coding was done in two schemes to correspond with the guiding concerns of the two research questions. First, the responses were coded to identify themes for the experiences of participants in response to Research Question 1. Second coding scheme focused on the reported barriers and enablers to implementation of student data privacy safeguards, in response to Research Question 2. This method of thematic analysis offers a flexible research tool for researchers who are new to qualitative research and generates unanticipated insights (Braun & Clarke, 2006). It is also an appropriate tool for exploratory research as it can be useful in informing policy development. To help relay the richness and meaning of the data, direct

quotations that represented the emerging themes were pulled and included in Findings and Discussion sections (Seidman, 2006).

Findings

The findings organized below provide responses to the two research questions: 1) What are the *experiences* of school-level teachers and administrators regarding effective student data privacy? and 2) What are the *barriers* and *enablers* to implementation of student data privacy practices in the selected case study district? The thematic analyses revealed major themes and sub-themes summarized in Table 2.

Chapter 5 - Table 2

Summary of Thematic Analyses Aligned with the Research Questions

	Themes	Sub-Themes	Sample Codes
Teacher Experiences	Availability and access to training	Preference for types of training	"wish modules were more engaging"
		Timing of the training	"too much information at once"
		Sources of training	"didn't know who to ask"
	Knowledge of student privacy issues	Administrators' role	"admin was supposed to do DSA"
		Privacy not a priority	"guarantee you that's not the case for probably more than 50% of our apps"
		Trust	"use DOE white list"
		Unchartered territory	"we're all learning together"
Enablers	Access to resources	HIDOE problem solving	"department protecting us from doing something dumb"
		Tech coordinators	"every school needs to have technology person"
		Informal communities of practice	"follow Mainland Twitter accounts"
Barriers	Issues with awareness	Lack of awareness	"95% of the staff employed by the DOE will have no idea"
		Communication flow	"no technology coordinator so I don't know if that's part of the problem our school not getting information"
		No stickiness factor	"an email gets buried because you have so many emails from the same person"
	Process	Too restrictive	"a lot of back and forth"
		Decentralized	"nice if at state level they could just see what we're using"

Experiences of School-Level Teachers and Administrators

In response to the first research question - *What are the experiences of school-level teachers and administrators regarding effective student data privacy?* – two major themes emerged from the findings: 1) availability and access to training tools, and 2) knowledge of student privacy issues.

Availability and Access to Training.

Responses related to training generally fell into sub-themes: 1) preferences for types of resources, 2) timing, and 3) sources of training. Teacher training in the district was typically conducted at the start of the school year with hours of videos dedicated to all topics. The key tension that emerged from the current training practice is that the information was too general and too vast. The compliance training, spread over seven asynchronous modules, was quickly forgotten or lacked relevancy until an issue actually emerged. Participants wished for more engaging training materials and better guidance from the state administration. The participants also said they would benefit from having resources that they could tap into as needed; for example, videos that they could send to parents about protecting student privacy and flow charts with step-by-step processes for purchasing and using a new app (online application):

> Some of us teachers had suggested if there's more information put out, or maybe even like a flowchart if you want to use an app or some kind of online platform ‘what do you do first before you just do it’ because I think that the teachers don't know. If they could at least tell us what's the first step ‘do you go to your principal do you go to DGA?’ I still haven't seen anything. (Tasha)

Other teachers mentioned that the timing of the training was inconsistent. Some videos distributed in the beginning of the year did not always reach the teachers in time. Because the

state training was distributed to complex areas and not directly to teachers, at times there was a bottleneck in distribution to the schools. Carmen said that after speaking with someone at the state office, she learned that the "resource teachers [were] told they should only be sharing information with complexes… And then a complex resource teacher should be sharing it with the schools." She continued: "it's a tri-level thing." She became aware of some videos that were not distributed to her school:

> So, I said 'How were we supposed to see these, because I had never seen those before.' [Administrator] said their office created it and shared it with the complex. Complex is supposed to share it with the schools. Well, our complex teacher didn't share that with us till January and I knew about it in August. (Carmen)

Overall, the participants' comments suggest that student privacy training was available but its effectiveness was undermined by timing and lack of an engaging design. There was also expressed interest in user-friendly sources of information after the training, such as one-page flow charts, and greater clarity as to where the teachers could seek more information.

Knowledge of Student Privacy Issues.

In discussing their understanding of student privacy, participants expressed a number of diverse experiences that can be categorized into four sub-themes: 1) the role of administrators, 2) student privacy not being a priority, 3) trust in the district's vetting process, and 4) unchartered territory for everyone.

Role of Administrators.

School administrators, such as principals and vice-principals, emerged as key influencers of student privacy enforcement in schools. First, school administrators must allocate funding for a technology coordinator, who would then be responsible for keeping teachers informed about

Ed Tech use. Second, administrators must be signatories to DSAs for the use of new software or program.

Participants were aware that they had to seek school administrator's approval before using new program in the classroom. This was reiterated in the *2020 Digital Device and Application Guidance for Distance Learning* which was brief, accessible, and it clearly stated that "teachers must seek administrator approval before selecting any online application for the classroom" (Hawai'i Department of Education, 2020). However, this safeguard was effective only if the school administrators understood the approval process and were supportive of the heightened student privacy protections. Otherwise, administrators' lack of buy-in became a hindrance and the responsibility shifted onto the teachers:

> If our admin didn't care, then I should be, 'well, I don't care.' You know what I mean? So that becomes the teacher's responsibility, like 'Is this something I should be using with them? I'm going to have to find out, the admin is not going to help me.' So, the burden becomes on you because you care about it. (Tasha)

She later also added that the teachers should still have a certain degree of awareness because teachers are still responsible for students' safety to a certain extent.

Not a Priority.

Student privacy not being a priority emerged as a sub-theme because the participants felt that school personnel did not have a full understanding of the connection between Ed Tech use and student privacy. I asked Mario, based on his experience working both at schools and complex areas, whether more training would raise this awareness:

> You know, as much as I would love to say training would help, it's a people problem. Unless the teachers really care about that, they're not going to do it… long story short, if

> we add any additional hoops for them to have tools to teach the students - for example, if we have to run everything by, let's say, a data privacy [group] - they're going to see it as a thing that they can just bypass. And I don't know of a good way to fix that, honestly. (Mario)

Hoku had a similar response saying that some of the terminology, such as data sharing agreements and "AG showstoppers" (Attorney General requirements for all state contracts), was foreign to principals and teachers, and there was no tangible urgency in going through the vetting process: "You might be the most techie person at your complex area. But that doesn't mean you've ever heard of data governance" (Hoku). Even when teachers knew of the DGA vetting process, teachers continued to use Ed Tech tools in the classroom without a data sharing agreement because there was no tangible, well-understood consequence to bypassing the process:

> I did, at one point, try to go through data governance... But it was kind of a lot of back and forth. So sorry, give up. The process got better. But I gave up. I totally gave up, like I'm not doing this. And so that was just one [software]. (Tasha)

When asked what she meant by "gave up," Tasha responded that she still used the software in her classroom but without going through the DGA process.

Trust in the District's Safeguards.

The lack of priority could also be attributable to the trust that the teachers placed in the district's monitoring and vetting of the Ed Tech. All five interviewees commented said they appreciated the reasons for protecting student privacy and wished there were more protections but outside of their responsibilities; for example:

> If in a theoretical situation, where we have rules and regulations and laws that protected privacy in general… and we didn't have to worry about those things it would make

everyone's life a little easier… if we the teachers wouldn't have to worry about it. Organizations have to administer, that will make things a little bit more standardized, you know what I mean? It gives us an idea of what we're dealing with. (Mario)

The divergence in responses occurred when participants were asked about their role in the process. Complex area resource teachers saw themselves as accountable for knowing the mandates related to student privacy. There was a sentiment that, even when it was not their primary responsibility, they are responsible for providing accurate information to the teachers across the complex area: "It's not truly ultimately my responsibility… people will come to me for those answers before they go to State because I'm more readily available to them than the three people at the state that, you know, handle 256 public schools, right? So, that's a lot harder for them" (Hoku).

Teachers at school-level, on the other hand, had less urgency in having an in-depth knowledge of the student privacy mandates. While they would have liked to know about app safety, they trusted in the "whitelisted" apps that were posted on the District's website. It was "time-consuming" and "cumbersome" to go through the DSA process, so it was easier to use what was approved. For example, Tasha had a working relationship with a representative from Apple school management program and downloaded apps that were available through the Apple operating system. She trusted that if the school had a contract with Apple, all apps available on the Apple's site were safe to use. When asked if she had looked at the app privacy policies or confirmed that the app was approved for use, she replied "I found out after that it really should have been admin, and if a data sharing agreement was needed they were supposed to. But I think because our admin was not familiar with it, I don't think that was happening" (Tasha).

Unchartered Territory.

Finally, the participants revealed that the experiences in student data privacy was an unchartered territory for everyone: “We are all wizards in training” (Carmen). There was also a lot of collective learning and willingness – but not time – to learn. The move to virtual learning during the COVID-19 pandemic sped up some of the learning and awareness that may have taken longer otherwise. One teacher reported that she learns from her students every day when she talks to them about digital citizenship: “As I'm teaching the children, I'm also teaching the teachers and a lot of times the students and the teachers will be teaching me. We're all learning together now” (Tasha). She reported that even when she attended training on data sharing agreements, “it really seemed like [the presenters] were truly trying to understand it themselves. As they were telling us about it, they're just still trying to understand it” (Tasha).

Enablers for Effective Safeguards of Student Privacy

In response the second research question - What are the enablers and barriers to implementation of student data privacy practices in the selected case study district? – I divide this section into two parts organized by enablers and barriers, outlining first themes that emerged as enablers.

Access to Resources.

Participants were grateful for the resources they could access when the prescribed pathways, such as school administrators, were not available. The sub-themes that emerged for Resources were: problem solving by the State Office, technology coordinators, and informal communities of practice.

State Problem Solving.

Some enablers for effective student privacy practices emerged during the COVID-19 pandemic. There was increased training on the use of technology. More direct communication from the State Office to practitioners was positively received as well. Kanoe spoke of "practitioner forums" that were organized during the pandemic which improved the State's typical flow of communication: "Normally, they put everything through the CAS [Complex Area Superintendents]. The AS [Assistant Superintendents] go to CAS meetings, okay, but the CAS have way too much information bottlenecking through them so it doesn't get out to anyone else." The practitioner forums, which had guest speakers, allowed complex area specialists to hear directly from the decision-makers and to learn of challenges that other complex areas were facing:

> We really needed more forums like these in the CAS structure and then it ended… Sometimes there are lulls where we really only have information that's coming from the CAS and it's just too much pressure, it's too much information to put on one person. It's not possible for them to get all the details of all the projects and to know what questions to ask. That doesn't really set anybody up for success. So, when they have practitioner forums where people who are practicing and using can ask directly to people who are decision makers, I think that really helps. (Kanoe)

State support for student privacy emerged from unexpected places. Carmen's teacher group purchased Padlet program but were told "they couldn't use it" because of potential student privacy issues. After two months of negotiating, Carmen said that a video was created for teachers on the proper use of Padlet, after which they could use the program. She believed the video was made by the Office of Talent Management: "They problem-solved for us."

All respondents were familiar with the DGA office, and three respondents had direct contact with the personnel responsible for creating data sharing agreements. They saw the office and its personnel as experts on student data privacy and deferred to their expertise. Even when the process appeared cumbersome, there was understanding why certain barriers existed. For example, Kanoe mentioned that she understood why she needed to provide rationale for sharing student information with a vendor:

> Sometimes in a good way DGA cut stuff like, 'I really don't think you need this XYZ… to accomplish this goal' and then when we went back and forth, the company was like 'You're right. We don't need that.' We were able to trim it down to just be essentials.

She said that even after getting approvals for 9 different apps, she did not see herself as an expert because it came to her desk only once or twice a year, and she did not "feel super confident" to tell the vendor what was problematic about their terms of service. Kanoe added that "as things change or get updated, we could be saying something wrong or be misinformed. I think it is nice when we get more support from our State office in this area so that it is really in their expertise and wheelhouse."

Technology Coordinators.

Another major resource for teachers were technology coordinators and technology resource teachers across the District. Participants reported relying on people more often than on training modules to ask questions and to seek collaborative solutions. Many of the people were labeled as "techie" by their schools or complex areas and became the default go-to person for any technology-related questions. Carmen was the first person I interviewed and she suggested "you're going to find, if anyone is interviewing with you, that it's usually one person, doing all of [technology] if it's a public school." Technology coordinators would also be invited to complex

area meetings where they would learn new information and pass it down to other teachers. They built relationships with the State and other complex area technology resource teachers during trainings. However, not every school had a designated technology coordinator. Tasha recalled "if the admin is not comfortable with technology or thinks it's not a priority, then it won't be… [They] prioritize that non-classroom position to something else." Carmen, who was a technology coordinator and a teacher, expressed a wish for having a full-time technology coordinator but quickly added that it is not likely to be a priority because of funding: "I love doing the teaching part. If there was another person doing the technology, can help with the devices, that would be so beautiful. I really don't think that is possible. I mean, we're having a hard time funding our library."

Kanoe concurred that it was important to have technology coordinator designation at each school and that this designee could become the student privacy expert at the school:

> I can't really imagine [student privacy] being a full-time job, but I could see our tech coordinators being people who at the school level are really strong at it and our point person as assigned to us, becoming even more of a champion of the work and being involved… They would be more likely to see things happening when schools are not actually checking on it.

This last point she made was critical to understanding the potential breakdown between district-level policies and school-level practices without a designated person responsible for student privacy at school level.

Informal communities of practice.

Community support was mostly informal and its robustness dependent on the participant's school and community. Two participants relied on Twitter posts by educators

outside of Hawai‘i who shared information on new apps and best practices. Carmen stated that most of the information on Twitter did not touch on student privacy, but at times, she would see a related post. On the other hand, Hawai‘i-based informal communities provided more feedback on safe practices and vetting of online applications. During COVID-19, technology needs became too overwhelming for a single person, so Carmen found support in her own school:

> It was a big effort of a lot of people, even though I'm in that one role with technology… So grateful that everyone stepped in to help. And the teachers were having to help too, because they were the ones having to unplug the cord and having to bundle up the technology devices and get ready for the kids… So yeah, out of necessity.

There was a sentiment of good fortune, when people stepped in to assist. It was not expected and was seen as a volunteer effort. Carmen also suggested she did not expect administrative support from the State: "We're so lucky that everyone stepped in… volunteered their services. They said, 'Hey, how can I help?' If it's not that kind of [helpful] climate at a school, the people at this kind of position would be sinking."

Participants who were members of the HSTE consulted with other members and reached out to teachers outside of their complex area. Overall, there was positive feedback about the support and willingness to help among other teachers and technology coordinators: "I'll ask other teachers, like '[name redacted] have you heard of this is? Is this something we can use? Do we need a DSA?' There are certain things, like [name redacted] said if [students] have to log in with their name or some kind of identifiable thing… That's why *we* wanted a flow chart because, how would you know you need to get a DSA?" (Tasha). I highlight "we" in this segment of the interview because Tasha's response implied a discussion took place among several people, and they collectively came up with a solution that would be useful to them as practitioners.

Barriers to Effective Implementation

Participants identified a number of barriers during the interviews that could be synthesized into two major themes: 1) awareness issues and 2) process.

Awareness Issues.

The sub-themes for awareness were similar to the findings identified in teachers' experiences on knowledge of student privacy. Namely, the respondents suggested that lack of awareness, poor communication flow, and no stickiness factor were barriers to successful implementation of student privacy.

Lack of awareness about student privacy was a major barrier to implementation. Under the current system, the burden of safeguarding student privacy at schools lies primarily with the principals. The teachers are expected to seek approval from principals or their designee before using new technology in the classroom. As discussed in the previous sections, teachers did perceive that the responsibility for ensuring safety of Ed Tech should be primarily on the administration. However, Hoku estimated than close to half of all Ed Tech in use in the District has not been properly vetted because of lack of awareness among the principals:

> You will get principals that say just go ahead and buy it… But the principal doesn't realize by saying that they're taking on that liability. They've not looked at the privacy laws, they've not looked at the terms of use, the teacher didn't bother explaining it to the principal, because they just want to use it because it's got this awesome feature" (Hoku).

The tri-level governance system can lead to additional hurdles in communication and up-to-date awareness among school-level personnel. The guidelines from the District Office do not always get communicated to the schools directly but instead flow through complex area administration. This can create inconsistent distribution because a complex area may disseminate

information instantly or wait for complex area-wide meetings. Moreover, when an app is approved for one complex area, the approval does not get communicated to other complex areas, so each school or complex area has to go through its own vetting process. When asked about the impact of the current HIDOE organizational structure, Mario stated:

> I think bypassing the complex area [helps], because if we're going to do one for a certain complex area… and another complex area wants to do it and might not know that it already exists or it's already being done with a third-party vendor. So, if it's centralized, then at least we have eyes on everything, and then we can say okay, this has already been done. Here's a template and we can add that on, or we can make the process more streamlined for anybody who wants to do something with the specific company.

When information did reach the teachers, there was a problem of stickiness. Either overwhelmed by an influx of information ("an email gets buried, because you have so many emails from the same person") or not remembering the pathway to get to the correct information ("I got it from that meeting. I don't know how else to get it"), respondents felt that the information did not always stick and needed access to the information in a way that would be intuitive. Tasha said that the updates about student privacy were usually shared at faculty meetings without a written memo. She said that at her school "we have been asking for a while about some kind of handbook that has procedures about different things, because otherwise it's all just word of mouth" (Tasha). When asked if she knew whether a guidebook existed at district level, she shook her head to indicate 'no'.

Process.

The process for introducing and vetting Ed Tech in the classroom was reported to be restrictive and lacking centralized authority. Respondents knew of the DGA's role but said it was

not clear who was responsible for data privacy at complex area or school level. Respondents wished for more centralized processes. Mario, because of his close work with the District's IT office, stated that even when the policies were developed at district level, the schools still operated independently under their internal norms: "The DOE structure is unusual in the sense that schools are sort of *little silos, autonomous*, so they kind of generate their own policies and procedures... I think I would do away with our sort of federated model in the DOE, the fact that schools are kind of autonomous that leads to problems" (Mario). He continued that the IT systems are secure enough, but the safeguards ultimately depend on the exercise of professional judgement among teachers and administrators. There is a lot of confusion and "duplication of effort across all the schools," and it becomes difficult to reach and train every teacher on something as nuanced as data privacy: "People get the wrong message and they're not really, truly understanding what they need to do… that that kind of stuff is hard to, I guess, lock down, again, because it's so decentralized" (Mario).

Carmen expressed similar sentiments saying that giving schools too much autonomy without centralized processes puts unnecessary administrative burdens on the schools:

> It would really be nice if at the state level, not the school level, if there was a place that they could just see what we're using and handle getting the okay for us, that would be really helpful. Then you cover the mass of schools instead of each individual school having to get that… That would be wonderful. Because now, you know, having to change this to that to make it work. Yeah, it just, it's not worth it."

These responses suggest that schools may prefer to have less autonomy and more direct guidance on issues that are not familiar to school administrators or require specialized expertise, such as student privacy.

The process was further encumbered by limited resources at the district office. With only two people in the DGA office receiving and processing requests for data sharing agreements, the teachers perceived the process as slow. When asked if the current district offices had the capacity to handle requests from individual schools in an efficient way, Mario responded:

> No, I don't think a lot of our state offices or branches have that capacity. It's just in general, again with the structure of the DOE how it is, a lot of the money ends up going towards the schools and becomes more federated. Because of that we're running very lean on higher levels and so we're going to talk, you know, human resources, or any other sort of resources. It's a little light… that's kind of my sense of it.

The slowness of the process could stem from the numerous departments that may be involved in approving a single data sharing agreement. Kanoe gave an example of a DSA that took 8 months to complete involving "the vendor, the complex area, DGA, OITS [Information Technology Office], then also [name redacted] office got involved…, and then the AG's office." She continued that without a project management software, all communication was happening by email causing her to lose track of the up-to-date version of documents and which departments had not issued their approval yet: "There were six different offices involved that were touching this. Sometimes the DSAs are separate from the memoranda of agreement and sometimes they're combined, so there was a lot of people." Kanoe suggested having an online project tracking software and clear time frames for approvals: "if we can manage expectations, it causes a lot less stress."

Even as processes improve, the institutional memory persists, particularly at school level where teachers rely on informal communities to confirm or dispel effective practices. If a teacher has a negative experience going through the DGA vetting process, they will likely remember and

be impacted by that experience when deciding on app adoption in the future. Negative experiences are also more likely to be recalled. When asked how they viewed an ideal process, respondents were more likely to bring examples of negative experiences that were frustrating rather than positive experiences that worked well.

Discussion

In response to the study's research questions, the findings suggest that the participants' experiences included limited but growing knowledge of student data privacy. The responses also highlighted the need for effective training (Research Question 1). The existing barriers can similarly be traced to limited awareness and decentralized processes. However, strong community support and expertise of the district office personnel are promising enablers toward design of student privacy safeguards (Research Question 2). Below is an in-depth discussion of the implications and their meaning within the conceptual framework.

Increasing Awareness of Ed Tech with Focus on Student Needs

The findings suggest that the current processes for data privacy at the district are driven largely by compliance:

> The state put out these training modules that the teachers were supposed to watch, but you know a lot of them didn't… When admin says 'State says we have to look at this, or we have to do this,' the teacher is like 'Comply'… Those modules, we just have to sign a paper, 'Yes, I watched this. Yes, I watched this.'" (Tasha)

Despite the training, all five participants stated that they either witnessed teachers using Ed Tech without a vetting process, or have done it themselves because of the time and effort it required to go through a DSA. This highlights the tension in implementation of district policies.

While the district appears to comply with the relevant laws, an audit is likely to reveal gaps between policies and classroom practices. One of the shifts that needs happen is increased awareness of how Ed Tech impacts students rather than the current focus on compliance. Applying the student-centric learning model (Christensen et al., 2008), the District would begin its inquiry from ground up – looking at the students' best interests and subsequently designing policies that capture those needs.

Hoku suggests that in a student-centric model the first point of inquiry for Ed Tech adoption should be the purpose of the tool. Before the DSA process, the teachers should be asked what learning objective they wish to achieve. A technology coordinator can then assist with identifying an app that fulfills that objective:

> Downloading an app is not innovation. Just because you've downloaded an app does not mean you have made yourself more innovative. I said 'What are you trying to do?' Because if you have several apps that do the same thing, how much are you driving those parents crazy? You're making them download all these apps just to be able to attend school. (Hoku)

Furthermore, the autonomy granted to schools can add administrative burdens and confusion. When teachers are presented with options instead of clear guidance, the focus becomes on experimentation rather than teaching: "I give you a list of 35 apps that are approved, and guess what's going to happen tomorrow? You're going to use 35 apps and you're going to try to see what you can do with them all" (Hoku). The hidden costs of Ed Tech fall on students and parents as they struggle to keep track of the overwhelming number of new programs and login information with minimal value added to academic improvement. The Ed Tech vetting process must then include a *value* assessment to confirm that the use of the program is in fact innovative.

At times teachers' interests may not be in alignment with students' interests. Using the conceptual framework discussed above, it is important to recognize that the school *community* involves multiple stakeholders: "The general triangle that we typically talk about. Student, parent and teacher" (Hoku). He continued that if we only focus on the teachers, we miss important considerations of other members of the community. A student data privacy framework with a focus on student needs will also advance the District's compliance goals by staying ahead of potential liabilities. As all *community* members, including parents and students, gain awareness of and agency over student data, a two-way communication process would provide valuable feedback to the District on the emerging tensions before they reach non-compliance violations.

Some of the current elements of the process are already student-centric and should remain. For example, during the vetting process DGA reviewed what type of data would be collected by the Ed Tech app and sent inquiries to the initiating school or complex area to confirm that the shared data is connected to the purpose of the app. This created an added step in the process but fulfilled the District's obligation that only necessary student data would be shared with the vendor.

Creating Strategic Student Data Privacy Training and Resources

Strategically designed training should take into consideration not only the *content* of the material but also its *effectiveness.* Respondents reflected positively on incorporating time-saving methods of delivery, a propensity for persistency (stickiness), and ease of access to information after the training. Effectiveness of the training may also depend on how frequently this information is used. For issues that involve specialized expertise and infrequent occurrence, such as student data privacy, it becomes important to train teachers *how to find* information when it is needed in addition to knowing the information.

Suggestions for time-saving delivery methods included a step-by-step flowchart on how to introduce new technology in the classroom (Carmen; Hoku; Kanoe). A flowchart is a time-saving resource for teachers who have little time to explore hefty manuals; for example, Data Privacy Agreement Flowchart (Utah State Board of Education, 2020) and Resource Request Workflow (Rockingham County Public Schools, n.d.-b) are one-page summaries for educators who have gone through training but may need a refresher when they wish to utilize Ed Tech in the classroom.

For improved stickiness, Tasha suggested applying proven engagement tools to professional development sessions:

> Maybe if admin had made it more fun, or we watched it together. You know how teachers have to teach online and engage students? If they had done that with us during the modules, we learned together and people engaged in the chat blogs.

Such engagement strategies must account for the audience's existing skills, knowledge, and experience (UC San Diego, 2021). One of the pitfalls of workplace training is the emphasis on 'telling' and not enough opportunities to apply what is learned. FPF developed training student data privacy scenarios for teachers to address this gap (Future of Privacy Forum, 2021a). These scenarios help create persistent connection between classroom experience and student privacy. They also clarify consequences of failing to follow proper safeguards.

Additionally, easy access to information post training is key to ongoing implementation of student privacy mandates. As Kanoe mentioned, student data privacy issues do not come up frequently. Consequently, the teachers will resort to easily accessible resources to refresh their recollection rather than attempt to remember what they learned in their training. Tasha recalled that the State maintained a spreadsheet with "whitelisted apps" but did not remember where she

could find it after the training. Because the current written resources are too few or not intuitively accessibly, teachers reach out to their communities of practice whom they perceive to be experts on the topic. One option for easy information access is a dedicated student privacy website that offers resources for all stakeholders – parents, teachers, and administrators. For example, Academic Technology Menu website (Denver Public Schools, n.d.), Data Security and Privacy website (Rockingham County Public Schools, n.d.-a), and Student Data Privacy website (Utah State Board of Education, n.d.) serve as comprehensive publicly-viewable sources of information for the district or state.

The findings that revealed bottlenecking of information are not surprising considering the enormous workload of other responsibilities assigned to principals and complex area superintendents. When designing a strategic training framework, the District should consider the audience's capacity for information distribution and information retention. This may first require identifying barriers at distribution points. Hoku suggested creating a task force comprising multiple levels of school hierarchy:

> A group that incorporates state, complex area, school, and teacher level. And school level has multiple levels: tech coordinators, teachers, and admin. And they need to listen first… to get everybody on the same page speaking the same language before you can even start to make change… right now, there are about 1000 different myths and misconceptions out there about everything.

The long-term impact of strategically designed training is multifaceted and will lead to alleviating many of the current barriers to implementation. First, creating training videos for parents will contribute to transparency and will ease the schools' administrative burden to explain consent forms and image release forms to parents. Second, written and easily accessible

information for teachers will ease the burden of "techie" employees who are frequently sought after as informal sources of information and who have become the de facto experts in student data privacy. Finally, maintaining a publicly viewable list of district-approved apps with valid DSAs is consistent with best practices identified by the U.S. DOE's recommendation for transparency (U.S. Department of Education, Privacy Technical Assistance Center, 2014).

Alignment with the Conceptual Framework

The findings from semistructured interviews contribute to *Community* and *Division of Labor* components of the conceptual framework. These elements impact and are impacted by the *Subject* (district administrators) component. In a K-12 context, teachers and school administrators play a critical role in fulfilling the district's objective to protect student data privacy. Respondents indicated that district administrators were both an enabling element (serving as resource) and a barrier (cumbersome DSA process).

The tensions in *Division of Labor* emerged between the district-level and school-level communication due to the tri-level governance system. Mediated artefacts, such as resources and training (*Tools)*, must be strengthened in order to support distribution of information from the district across the complex areas and to the schools. This implication is supported by findings in the previous phase of the case study, which revealed that district administrators had limited knowledge of student data practices in schools.

Limitations

This study was conducted during the COVID-19 pandemic, which overloaded the capacity of technology coordinators and resource teachers and brought to light the issue of data privacy as schools came to rely almost entirely on distance learning platforms. Student privacy

became a sensitive and at times controversial topic in schools and many of the teachers had been overwhelmed with the barrage of technology requirements imposed on them. As such, the responses during the interviews were skewed by the experiences of technology use during the pandemic rather than in general.

Also, majority of the participants were part of the HSTE and had greater exposure to understanding Ed Tech because of the affiliation with the group. All five were employed by schools or complex areas in the urban Honolulu County, and the data did not reflect experiences of neighbor island teachers. The study focused on a single school district that also operates as a state educational agency (SEA). It is the only single SEA and LEA in the country, and as such the findings may not be generalizable. As the only researcher for the case study, I brought personal assumptions and biases into the interview when guiding the discussion and when coding responses. My biases were influenced by the reviewed literature on the subject, experience working with HIDOE, and findings from the previous phases of the study. To account for biases, I kept a journal detailing personal reflections that emerged during research.

In professional capacity, I had worked with the HIDOE DGA Office on a short-term project in 2021, during which I did not collect data for the case study research to avoid any perceived or actual conflict of interest. Some of the information described here was gained through personal knowledge and experience, and has contributed to my understanding of the district as a case study. Although the invitations to participate in the research study were sent after my contract with HIDOE had expired, some of the participants may have perceived me as an employee and representative of the DGA office, which may have affected their decisions to participate or the responses they provided.

Future Research and Conclusion

This study supports future research in examination of student data privacy at schools, with particular focus on: impact of training on teacher awareness; comparison of training delivery models; usability and effectiveness of student privacy websites; and perceptions of parents in student data privacy issues. On a regional level, future research might include a comparison of HIDOE complex areas in their capacity to support Ed Tech use in schools. Such research will be useful for practitioners, policymakers, and the District.

The current research contributes to Phase 3 of the exploratory case study and provides answers to the research questions articulated above. This phase offers more granular, focused examination of student data privacy at the selected school district from the perspective of teachers and technology coordinators. Participant interviews generated rich data for school-level understanding of privacy issues. As a new phenomenon, data privacy in schools still carries unresolved concerns, but the overall responses among the participants suggested willingness to learn and to become better protectors of student privacy when appropriate supports were in place. These implications are critical to the comprehensive examination of the case study, supporting or dispelling previous research phases.

CHAPTER 6. DISCUSSION AND CONCLUSION

Introduction

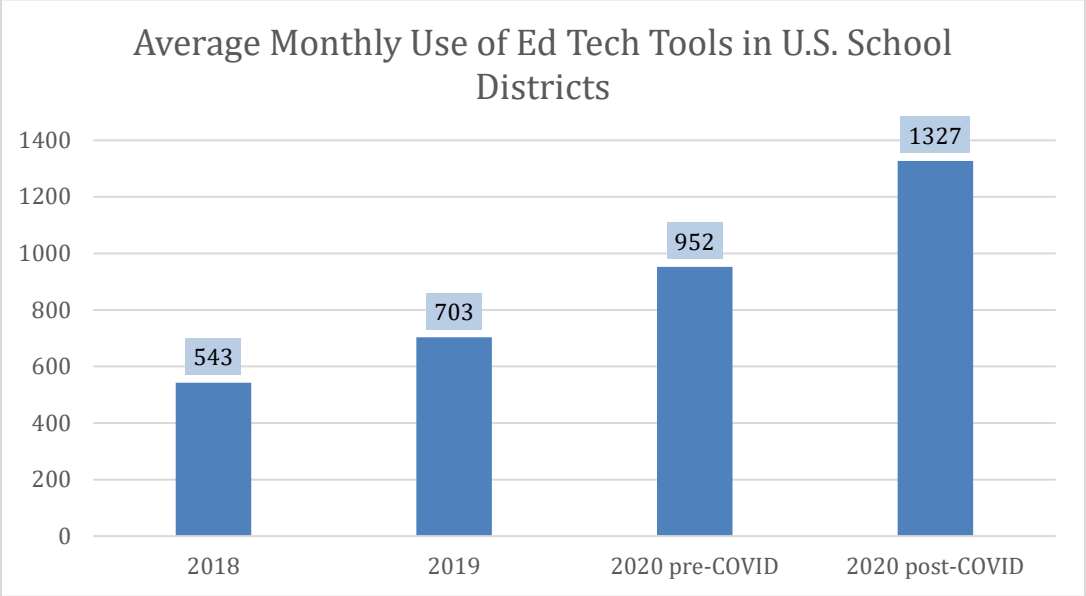
The purpose of this exploratory case study was to examine practices related to student data privacy and educational technology in a single K-12 school district. The case study offers an insight into this emerging phenomenon in three phases using literature review, a quantitative survey analysis, and qualitative semi-structured interviews, presented as three manuscripts in Chapters 3-5. In this final chapter, I summarize the findings of the three phases and articulate the collective implications that link the three manuscripts. I also discuss contributions to theory and practice, concluding with limitations and recommendations for future research.

Literature Update

I began researching the issue of student data privacy in 2018 when the conversation on the topic existed largely in the context of law, information technology, and higher education (Cavoukian, 2011; Daggett, 2008; Ifenthaler & Schumacher, 2016; Miller et al., 2012; Park & Vance, 2021; Rubel & Jones, 2016). Since then, the use of educational technology in K-12 skyrocketed to record levels prompting an urgent need for guidelines on student privacy and data breaches (Catalano, 2021; Cybersecurity and Infrastructure Security Agency, 2020). In one year, driven by the move to virtual learning during COVID-19, average school district's monthly use of Ed Tech went from 703 to 1327 (Rectanus, 2020). Overall, since 2018 the number of Ed Tech tools in school districts almost tripled, Figure 1.

Figure 6

Average Monthly Use of Ed Tech Tools in U.S. School Districts (Catalano, 2021)



As the use of Ed Tech in public schools continues to grow, the discussion of student data privacy has gained momentum in popular and academic publications; however, the number of empirical studies on this issue remain small (Bernard & Ritter, 2021; Center for Democracy & Technology, 2020; Consortium for School Networking, 2021; Regan & Jesse, 2019; Slade et al., 2019; Vu et al., 2019).

The data privacy concerns in K-12 environments are driven by unauthorized use of student data by private Ed Tech companies (Kelly et al., 2021), lack of transparency on student data use (U.S. Department of Education, Student Privacy Policy Office, 2021), districts' non-compliance with privacy laws (Reyes et al., 2018), and cyberattacks on student records by malicious actors who exploit vulnerabilities in network systems (Cybersecurity and Infrastructure Security Agency, 2020; Regan & Jesse, 2019). Numerous state laws have been enacted in the last three years, including Hawai'i's Student Online Privacy Act (HB125, 2021), but the federal standards have not kept up with regulating student data collection and use by

private companies (Bartow et al., 2016). While there has been a shift toward privacy awareness in recent years, parents still largely accept the culture of digital trust in schools' collection and management of sensitive student data (Abraham et al., 2019).

Methodologies

This exploratory, interpretive case study (Merriam, 1988) was conducted in three phases to gain a comprehensive look at the selected school district, to understand the policies and regulations that guide its student data management practices, and to assess the district's current practices from a perspective of diverse district-level and school-level personnel. While there are a number of other issues in student data privacy, such as the use of student data by law enforcement and immigration officials (American Civil Liberties Union, 2019; Bellows, 2019; Reddy, 2020), the monitoring of student social media and emails (Beckett, 2019; Hankerson et al., 2021; Vickery, 2015), and ethical implications of learning analytics (MacCarthy, 2014; Willis et al., 2016), this study had a specific focus on the impact of Ed Tech on student privacy in public schools. The case study site, HIDOE, is uniquely positioned as the only statewide school district in the country that operates both as a state and local educational agency, providing an apt setting for an in-depth exploration.

The research design was purposely designed to explore sequentially from broad to narrow context to inform each subsequent phase of the study. Phase 1 (Chapter 3) assessed the overall national trends and best practices using a literature and legislation review on the topic. These findings helped define the broad national context. Phase 2 (Chapter 4) narrowed the focus on the selected school district and the district administrators' perceptions and practices of student data privacy using an anonymous online survey. Phase 3 (Chapter 5) delved even deeper to assess the

experiences of school-level personnel using semi-structured interviews with teachers and technology coordinators.

Major Findings

Manuscript 1 (Chapter 3)

Phase 1 of the research focused on a review of publications and legislation related to student data privacy and educational technology aiming to contextualize, give background information, and situate the case study in the larger paradigm (Eisenhardt, 1989). It addressed Research Question #1 of the case study: *What are the current trends in student data privacy as evidenced by school district policies and legislation related to student data governance?*

The resulting manuscript (Chapter 3) revealed that parent groups and privacy advocates had strong concerns about lack of transparency in student data use and data security (Data Quality Campaign, 2016; Foundation for Excellence in Education, 2015; Parent Coalition for Student Privacy, 2019). Because federal laws fail to provide comprehensive standards and protections to address these concerns, states such as California, Utah, Oklahoma, have attempted to address them through state legislation. However, both government and advocacy groups caution against swinging the protection pendulum too far resulting in stifling data-driven academic interventions (Blair et al., 2015). Other best practices emerged as well: Setting limits on the collection and use of student data by private companies; appointment of chief data officer for the school district; expanding parental rights; creation of safe data use training; and establishment of a private right of action in data privacy breaches.

The implications from the literature review revealed a number of existing gaps that remain unaddressed in the current student data privacy frameworks. First, while schools use

dozens and sometimes hundreds of different Ed Tech tools (Catalano, 2021), school districts rarely engage in *regular audits* of Ed Tech use, such as evaluating the risk of data breaches and unauthorized use of Ed Tech. Audits would equip district administrators with the information needed for appropriate allocation of resources and timely strategic interventions. Second, school districts need standardized *national definitions and baseline* for student data privacy. Such standards would help maintain consistent safeguards across each school district and place the onus of meeting these standards on the Ed Tech providers. They would also tighten the increasingly overbroad definitions adopted from FERPA. Third, *transparency* in data use remains an urgent concern for parents but has not been met by most school districts (U.S. Department of Education, Student Privacy Policy Office, 2021). Addressing transparency concerns is an important preemptive step in balancing innovation and privacy. Finally, *meaningful student data privacy policies* should be impactful both on paper and in practice. Technology will continue to evolve faster than policy enactments. Consequently, meaningful policy will require expertise from technology, legal, and education experts who can anticipate short-term changes. Inclusive stakeholder engagement will also prevent hastily written laws that lead to detrimental impact on innovative uses of data.

Manuscript 2 (Chapter 4)

The phase 2 of the case study used quantitative survey data to measure practices and perceptions of the district-level administrators at the selected school district. Using responses from 28 HIDOE administrators, the survey addressed Research Question #2 of the case study: *What are the perceptions and practices of district-level administrators, especially those with experience and knowledge in data governance, regarding student data privacy?*

The participants were employees of HIDOE at different levels of district administration. The selection was purposive to include employees of departments and branches responsible for securing, monitoring, distributing, interpreting, or managing student data. The anonymous online survey was conducted entirely online with 37 closed-ended questions and 1 open-ended question.

The collected data revealed participants' perceptions and practices of the student data privacy at the district. Participants' *perceptions* and personal familiarity with student data privacy issues leaned toward the positive. However, familiarity with student privacy laws was inconsistent with participants being most familiar with FERPA and least familiar with Hawai‘i SOPIPA law. Participants had a slightly less positive response on the issue of transparency, although the mean remained above average.

Survey questions that measured *practices* at the district also received above average positive response. Among items with the highest mean, suggesting the strongest compliance, were questions that addressed the issues of district leadership and administration. However, items that assessed existing policies and procedures at the school level, involving teachers and parents, received the least positive responses. The survey also measured gaps in knowledge among the respondents to understand their awareness of the issues (Krosnick & Presser, 2010). These revealed limited awareness of IT-related practices, such as processes for data recovery and incident reporting, and of practices that take place at school level, such as parent training and teacher guides. Participants overwhelmingly selected "improved communication among units" and "increase in personnel dedicated to data privacy" as top two priorities to improve student data privacy at the district.

The implications emerging from the survey suggest an urgent need to improve both vertical and horizontal communication processes across the school district, and to create a

district-wide strategic framework for student privacy. First, *improved communication* across the district-level units would provide administrators with up-to-date information, particularly in light of increased data breaches in school districts (Bernard & Ritter, 2021). Second, the district is in need of a *strategic student data privacy framework* that would incorporate policies, clear guidelines, training, and continuous awareness raising for all stakeholders, including teachers, parents, and administrators.

Manuscript 3 (Chapter 5)

Finally, the last phase of the research sought to understand student data privacy issues at school level through semi-structured interviews with teachers and personnel who are responsible for educational technology use in schools. This Phase 3 addressed Research Questions #3 and #4 of the case study: *What are the experiences of school-level teachers and administrators regarding effective student data privacy?* and *What are the enablers and barriers to implementation of student data privacy practices in the selected case study district?*

Five semi-structured interviews were conducted with HIDOE personnel who are employed at schools and complex areas in Honolulu County. The interviews were qualitatively analyzed and thematically coded to represent participants' experiences and existing enablers/barriers to student data privacy. Two major themes emerged addressing participants' experiences: 1) availability and access to training and 2) knowledge of student of student privacy issues. The sub-themes suggested that the training resources were not always timely or consistent across all schools. Participants also experienced student privacy as a learning process and reported they trusted in the district's vetting of the Ed Tech used in the classrooms.

The interviews further provided insight on the *enablers* of successful implementation of student privacy, citing reliance on tech coordinators, strong community support, and expertise of

the district office personnel. However, a number of *barriers* persisted, such as lack of awareness of student privacy and the onerous process for safeguarding student data. Participants suggested that lack of awareness and poor communication flow had a negative impact on implementation. When the information did reach them, it lacked 'stickiness.' The existing process for introducing and vetting Ed Tech tools was onerous and decentralized, which led to inconsistent implementation.

The findings from Phase 3 imply limited but growing knowledge of student data privacy at school level, with two major implications: 1) There is a need to improve awareness of the relationship between Ed Tech and student privacy focusing on student needs, and 2) student data privacy training and resources should be strategic to meet the needs of the audience.

Connecting the Findings

Connecting the findings from the three phases – in how they complement and diverge from one another – is a critical step in developing a deep understanding of the "contemporary phenomenon within its real-life context" in a single setting (Yin, 2014, p. 13). With multiple units of analysis, this research presents an example of an embedded case study with subunits – phases – that contribute to the overarching inquiry and to theory (Yin, 2014). While each phase of the research was described in an individual manuscript, collectively, the three manuscripts offer an in-depth view of the selected school district and its implementation of student data privacy policies. The section below identifies the common threads.

Transparency

Call for greater transparency in how schools and Ed Tech companies use student data was on the forefront of national conversations. This was supported by recommendations from non-

profit organizations (Data Quality Campaign, 2016), enactment of state laws (Colorado State Legislature, 2020), and federal best practices guidelines (U.S. Department of Education, Student Privacy Policy Office, 2021), urging or mandating that school districts publicize which companies are collecting student data and the type of data collected. Yet, the findings from Phases 2 and Phases 3 did not suggest that the need for transparency was a critical issue in the selected school district. Participants in Phase 2 reported that the district's policies and procedures on transparency were slightly less clear than on other items, but the overall mean score of 4.04 on this item was still positive suggesting that participants "somewhat agree" with the district's transparent use of data. Findings in Phase 3 was even more stark as transparency did not emerge as a major theme or sub-theme during the interviews. One participant hesitantly suggested that explanatory videos would be relevant for parents but was not convinced that this would become a priority: "If [HIDOE] was giving all these papers to the parents to sign, maybe a little introduction video that explains some of these important points, like the time the child is safe and 'what am I signing?' I don't know if that would be helpful or even possible, but yeah, that's fantasy item" (Carmen). Otherwise, improving transparency in data use did not emerge as an important issue in the selected site.

This divergence can further be seen in the absence of the local state laws that prioritize transparency. Unlike laws enacted in Utah, Colorado, and California, the two Hawai'i state laws that address student privacy did not mandate that educational institutions reveal to parents what type of student data are collected and how the data are shared (California Department of Justice, Privacy Enforcement and Protection Unit, 2016; Colorado State Legislature, 2020; HRS §302A-499, 2016; HB125, 2021; Student Privacy and Data Protection, 2016). Collectively, the findings suggest that there is little push from parents and education advocacy groups for stronger

transparency practices in Hawai‘i, and there is a disconnect between the national conversation and HIDOE on this issue.

Training

Unlike the issue of transparency, training emerged as a critical need in all three phases of the research. This is not surprising considering that concerns for student data privacy are relatively new and that the skyrocketed proliferation of Ed Tech in the classrooms caught both policymakers and educators unprepared (Bartow et al., 2016; Kamenetz, 2014). Because educator preparation programs typically do not offer training on safe data use (Mandinach & Cotto, 2021), the districts carry the responsibility to train teachers and administrators on student data privacy. Increased educator training on data use was recommended as one of the best practices by national advocacy groups (Data Quality Campaign, 2016).

At the selected school district, the findings were similar but more nuanced. Additional training was important at every level of school governance, but in order for it to be effective, the content and delivery needed to be based on the audience needs rather than on compliance. Parents would benefit from brief videos that accompany required forms. Teachers also preferred time-saving and engaging training materials that covers information relevant to their duties. Because issues with student data privacy do not occur frequently at school level, it became important that the school-level personnel knew *how to access* information when needed rather than be well-versed on all related policies. On the other hand, district administrators who are responsible for data management and policy implementation need to stay continuously up-to-date and trained on new developments as technology-related mandates will inevitably continue to evolve (Bennett & Raab, 2006; Davis, 2014).

Communication

Phases 2 and 3 revealed the need for improved communication across the district. This was not a major concern in Phase 1, suggesting that the issue is specific to the selected school district. The district's unique tri-level governance structure may be contributing to the inconsistent flow of information. As Phase 2 findings suggest, the district administrators had limited knowledge of school-level practices, and correspondingly, school-level personnel did not always receive timely and coordinated information from the district (Phase 3). The complex areas serve as intermediaries between the district and the schools; thus, the schools may not all be receiving information consistently and at the same time.

Timely information was particular important in vetting Ed Tech because teachers plan lessons around Ed Tech apps and supplemental online materials. The current process for vetting Ed Tech was reported to be time-consuming and administratively burdensome. In her interview, Kanoe referred to at least six different offices that were involved in a single data sharing agreement resulting in an 8-months delay. Improvement in communication was also named as the top priority in student data privacy by district administrators (Phase 2). This may involve investing in effective communication tools, such as project management software or a website, and creating modes of communication that are more use-friendly, such as flowcharts and videos.

Conceptual Framework

The conceptual framework – combining Activity Theory (Engeström, 1987) and the contextual integrity framework (Nissenbaum, 2010) – allows for a contextual assessment of all three phases of the case study as a single activity within a system. It allows for the emergence of tensions and contradictions between components of the activity system, as well as the importance

of relationships within it. The framework plays a particular critical role in Phase 2 of the case study because of its focus on the subjects of the activity system – district-level administrators. The findings revealed a mediated interaction in how the district administrators (*Subject)* secure student data when using educational technology (*Object)* in order to protect student privacy (*Outcome*). A number of mediating factors, represented as *Tools*, *Community, Division of Labor,* and *Rules,* emerged in this activity suggesting a strong relationship between the elements of the conceptual framework within a system – K-12 district. The contextual integrity (CI) framework offers a lens to assess privacy implications in the use and sharing of student data in the context of K-12 education.

Using the *Rules* element, Phase 1 findings helped situate the study within the contextual norms that either support or hinder the district administrators' activity of protecting student privacy. The current federal and state compliance standards enable the district administrators to set policies toward student data privacy. However, lack of transparency in data use and gaps in national standards have a negative impact because they do not provide sufficient guidelines. Similarly, the findings in Phase 1 support the CI framework hypothesis that *Transmission Principles* play a significant role in the expectation of privacy. As parents increasingly demand transparency in data use, privacy does become dependent on the appropriateness of information sharing in addition to its security. Interestingly, Phase 1 findings also revealed a direct relationship between *Rules* and *Community* because parental demand for greater transparency represents *Community's* impact on *Rules* and subsequently on the activity as a whole.

Phase 2 explored the core inquiry of the conceptual framework as the district administrators - *Subject* of the activity – shared their practices and perceptions that affect student privacy in the selected school district. The gaps in knowledge revealed tensions between *Subject*

and *Community* as administrators reported limited knowledge of school-level practices. These tensions also emerged in Phase 3 where the participants reported communication issues, which resulted in inconsistent practices in the classrooms. The findings in Phase 2 suggested inconsistent awareness of *Rules* as administrators were familiar with some laws but not others. Here, the CI framework contributes to understanding the findings as a tension between implicit and explicit norms at the district level. A relatively large number of district administrators indicated that they were not aware of a data recovery plan. The CI framework helped to identify that having processes for data recovery and incident reporting (explicit norms) were weakened if cross-departmental awareness of them (implicit norms) was lacking.

As for *Tools,* the district administrators utilized data sharing agreements (DSAs) to ensure that the data was collected and used safely by Ed Tech vendors. DSA was a useful tool to protect student privacy as long as the process was effective. The same was true for communication tools, such as flowcharts and training materials. Again, the findings suggested a direct relationship between *Tools* and *Community*. While DSAs were created and administered by the district administrators, the utility of DSAs was dependent on whether the school-level personnel consistently used them in the classrooms.

In Phase 3, the participants represented *Community* and *Division of Labor* elements of the conceptual framework. The findings revealed a significant interrelationship between school-level personnel (*Community)* and the district administrators (*Subject*), specifically the importance of training and communication between these two elements. When examined through *Division of Labor* lens, the Phase 3 findings also highlighted how the role of the school-level personnel impacted the activity. There was divergence in the individual responsibility for safeguarding student privacy at school level. Teachers and technologists at the schools perceived

administrators to carry greater responsibility for ensuring compliance, and reported disproportionate burden when administrators did not fulfill this role.

Overall, the conceptual framework situated the case study within the context of the selected school district and connected the distinct findings as part of a comprehensive system with tensions and contradictions across diverse elements of the district.

Contribution to Theory

The case study and the three manuscripts have meaningful theoretical implications in the field of student data privacy. The theoretical frameworks utilized in this study helped position and examine student data privacy in K-12 as part of an interactive system driven by internal and external forces. When examining the phenomenon through the Activity Theory (Engeström, 1987), it becomes apparent that the district administrators' practices in protecting student data privacy is not a linear process but instead are impacted by a number of dynamic transitions in the system. The elements of the activity theory – *Subject, Object, Community, Tools, Rules,* and *Division of Labor* – do not exist as unchanging, separate entities, and must be characterized by transformations that occur between them within a given context. For the human activity studied in this case study the tensions between the studied elements of the system emerged as the chief sources of change and influence in how this activity will continue to transform. The findings also help identify additional subunits of a system, such as a direct relationship between mediated factors. For example, I found that the *Tools* created by the district administrators needed to be aligned with teachers' needs (*Community*) in order to be effective. This presents an additional implication for the Activity Theory, namely that the object-oriented action is impacted by a direct relationship between the mediated factors.

The contextual integrity (CI) framework has been an influential lens in understanding privacy in the context of digital technology (Apthorpe et al., 2019; Benthall et al., 2017; Shvartzshnaider et al., 2016). This case study contributed to CI's expansion into the field of educational technology, which has been under researched in the academic circles. The findings in support of greater transparency and clear communication are aligned with the CI's emphases on context and *Transmission Principles* that allow for appropriate flow of information.

It is important to highlight that this conceptual framework was appropriate for the case study because of its focus on exploration and description of the phenomenon. The framework may carry less relevance in predictive or experiential research.

Contribution to Practice

The results of the study offer relevant information on the emerging but critical issue of student data privacy in the use of Ed Tech. As revealed by the case study, the effectiveness of laws and policies on this issue are tied closely to implementation at all levels of the school district. In examining school administrators' perceptions and practices as part of an activity system, the study brings to the surface some of the existing barriers to implementation. Furthermore, because issues with data privacy in Ed Tech outpace academic research on the topic, this research will contribute to the urgent need in creating a broad comprehensive framework focused on student-needs rather than on technology.

As the case study is situated in Hawai‘i, the findings and the manuscripts deliver an in-depth analysis of the HIDOE's current practices and persistent issues. Manuscript 3, in particular, reveals rich data in understanding barriers and enablers to student data privacy implementation in public schools. District administrators who are tasked with ensuring safe use of Ed Tech in Hawai‘i public schools can utilize these findings for future policy development.

Similarly, this dissertation may contribute to state legislative reforms to protect privacy of students given Hawai‘i’s unique statewide tri-district school system. As evidenced by other state laws and numerous proposals for a federal overhaul of FERPA, schools in Hawai‘i are likely to face new mandates and updates to its existing policies in the years to come.

Finally, the case study has a strong connection to the field of educational technology and will contribute to practitioners who design and utilize Ed Tech both in Hawai‘i and in other states. The study highlighted the importance of understanding state laws in addition to FERPA because each state may impose additional mandates on Ed Tech use beyond the federal standards. Based on the growing call for transparency, the findings also anticipate that instructional designers and educational technologists will face greater scrutiny in the use and collection of student data, and will need to work closely with school administrators in creating appropriate procedures.

Limitations

The scope of the case study was limited to allow for practical and meaningful exploration at the selected site, and may not be generalizable to other context because the data will be associated with a single school system (Merriam, 1988). The data collected at the school district site may have lacked full transparency because confidentiality of the district could not be attained as the HIDOE is the only school district in the state. Further, the analyses of data may not be indicative of the most up-to-date practices if the policies are amended after the data collection stage. Similarly, both federal and state laws shift rapidly in the field of technology, and subsequent security threats and the Covid-19 epidemic will likely have a dramatic impact on how educators and key stakeholders implement future policies related to student data privacy. By the time this dissertation enters the University’s ScholarSpace repository, the research may

already be obsolete. Also, the questions posed to participants may have alerted them to the gaps in practices and led to proactive changes before the dissertation is published.

This study was conducted in the midst of the COVID-19 pandemic, which not only overloaded the capacity of school districts to deliver effective instruction, but also brought a spotlight on the issue of student privacy as schools became reliant almost entirely on privately-owned distance learning platforms. Because student privacy became a sensitive and at times controversial topic and because participants were operating in a crisis mode, the content of the responses and the response rate may have been influenced by these exigent circumstances.

For Phase 2, participants district administrators had close working relationships with one another and may have refrained from speaking openly about departmental concerns. Small number of participants also affected statistical significance of the quantitative data analysis (Creswell, 2014). Anonymity of the respondents in Phase 2 provided both an advantage and limitation to the study. On the one hand, the participants were more likely to provide honest responses, but the analysis of the responses had to be more general because the practices and perceptions could not be linked to specific roles at the district to protect anonymity.

During the Phase 3 interviews, data collection was impacted by personal bias, reflected in the tone and questions asked (Creswell, 2014). As the only researcher for the case study, I brought personal assumptions and biases into the interview when guiding the discussion and when coding responses. My biases were also influenced by the reviewed literature on the subject, experience working with HIDOE, and findings from the previous phases of the study. Furthermore, the small sampling of participants made the findings less generalizable to the district since all of the interviewees worked in urban Honolulu County and the data did not reflect experiences of neighbor island teachers. Also, majority of the participants were part of the

Hawai‘i Society for Technology in Education (HSTE) and had greater understanding of Ed Tech than the general population.

In professional capacity, I had worked with the HIDOE on a short-term assignment prior to data collection and some of the participants may have perceived me as an employee and representative of the DGA office. This would have affected their decisions to participate or the responses they provided.

Recommendations for Future Research

Revealing tensions and contradictions through the conceptual framework lens, the study lends itself to a number of meaningful opportunities for future research. Broad policy-based inquiries may include a cross organizational comparison of student privacy policies across two or more districts, or an empirical study that compares school data breach incidents between states with different student privacy laws. The selected school district would benefit from greater exploration of *Community* aspect of the system, examining perceptions of student data transparency among parents at the selected study site. Similarly, assessment of school principals' role in vetting Ed Tech would provide further insight into the activity system.

District administrators would benefit from an in-depth review of policies and procedures of the contracted Ed Tech vendors to identify vulnerabilities in the districts' vetting process. Though not directly related to student privacy, the district would also benefit from a financial audit of the Ed Tech expenditures across the district, ideally leading to removal of duplicated services and limiting unnecessary exposure to student data.

Conclusions and Summary

Issues that affect educators' decisions in protecting student data privacy are uniquely complex and compounded by shifting legislation, cultural norms, and advancements in technology. Vendors' data collection and security standards, parental consent, transparency in the data use, data ownership, data sharing agreements, and legal compliance are just some of the emerging concerns that impact the use of educational technology in public schools. At the same time, data has become integral to academic and social programming in K-12 and has contributed to a number of innovative interventions. Because school districts must navigate multiple stakeholder interests and tensions, it was important to assess the practices of a K-12 school district through a holistic case study research design.

The research presented by this dissertation provides some insight into the current landscape of student data privacy at the selected school district. It identified the context that influenced district administrators' decisions, revealing the importance for continuous training across the organization, clear communication, and improved processes for vetting of new technology. The case study also contributed to the emerging theoretical understanding of privacy in the digital age and provided practitioners with data to inform future policy development and implementation. Finally, the key contribution of this research was to define how educational technology can be used safely to support student needs and innovative learning.

REFERENCES

Abraham, Sims, Daultrey, S., Buff, A., & Fealey, A. (2019). How Digital Trust Drives Culture Change—ProQuest. *MIT Sloan Management Reivew*, *60*(3), 1–8.

American Civil Liberties Union. (2019). *Cops and no counselors: How the lack of school mental health staff is harming students*. https://www.aclu.org/report/cops-and-no-counselors

Anand, P., & Bergen, M. (2021, October 27). Big teacher is watching: How AI spyware took over schools. *Bloomberg*. https://www.bloomberg.com/news/features/2021-10-28/how-goguardian-ai-spyware-took-over-schools-student-devices-during-covid

Apthorpe, N., Varghese, S., & Feamster, N. (2019). Evaluating the contextual integrity of privacy regulation: Parents' IoT toy privacy norms versus COPPA. *Computers and Society*, 18. https://www.usenix.org/system/files/sec19fall_apthorpe_prepub.pdf

Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. *National Bureau of Economic Research*, *Working Paper 23488*. https://www.nber.org/papers/w23488

Barbour, I. (2021, September 17). *Surveillance won't save our kids, humane public policy can*. Student Privacy Compass. https://studentprivacycompass.org/surveillance-wont-save-our-kids-humane-public-policy-can/

Bartow, A., Beckstrom, R., Bennett, C., Borgman, C. L., Citron, D., Davies, S., Donohue, L., Dwork, C., Farber, D., Fischer, A., Flaherty, D., Hurley, D., Ito, J., Kerr, I., Larsen, C., Lewis, H., Lysyanskaya, A., Minow, M., Molina, P., … Association, Y. A. L. S. (2016). *Coalition Petition to the U.S. Department of Education to Amend 34 CFR Part 99 to Establish a Data Security Rule*. https://alair.ala.org/handle/11213/5970

Beckett, L. (2019, October 22). Under digital surveillance: How American schools spy on millions of kids. *The Guardian*. https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle

Bellamy, R. K. E. (1996). Designing educational technology: Computer mediated change. In B. Nardi (Ed.), *Context and consciousness: Activity theory and human-computer interaction* (pp. 123–146). MIT Press.

Bellows, L. (2019). Immigration enforcement and student achievement in the wake of secure communities. *AERA Open*, *5*(4), 2332858419884891. https://doi.org/10.1177/2332858419884891

Bender, W. (2010, February 19). Spying on L. Merion students sparks probes by FBI. *The Philadelphia Inquirer*. https://www.inquirer.com/philly/hp/news_update/20100220_Spying_on_L__Merion_students_sparks_probes_by_FBI__Montco_detectives.html

Bennett, C. J., & Raab, C. (2006). *The governance of privacy: Policy instruments in global perspective*. The MIT Press.

Benthall, S., Gürses, S., & Nissenbaum, H. (2017). Contextual Integrity through the Lens of Computer Science. *Foundations and Trends® in Privacy and Security*, *2*(1), 1–69. https://doi.org/10.1561/3300000016

Bernard, K., & Ritter, S. (2021, October 8). Audit finds Kansas schools unprepared for a cyberattack. What is the risk? *The Kansas City Star*. https://www.kansascity.com/news/local/education/article254838942.html

Bettinger, E., Fairlie, R., Kapuza, A., Kardanova, E., Loyalka, P., & Zakharov, A. (2020). *Does EdTech substitute for traditional learning? Experimental estimates of the educational*

production function (No. W26967). National Bureau of Economic Research. https://doi.org/10.3386/w26967

Bieri, K. (2018, May 17). *District officials remain tight-lipped in the wake of Gadsden High cheating scandal*. KVIA. https://www.kvia.com/news/education/district-officials-remain-tight-lipped-in-the-wake-of-gadsden-high-cheating-scandal/742250976

Bijker, W. E. (1997). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. MIT Press.

Blair, D., Briner, K., Hopkins, B., Fary, M., Dani, V., & Kelly, M. (2015). The compelling case for data governance. *EDUCAUSE Center for Analysis and Research (ECAR), EDUCAUSE Working Group*, 7.

Borthwick, A. C., Anderson, C. L., Finsness, E. S., & Foulger, T. S. (2015). Special article personal wearable technologies in education: Value or villain? *Journal of Digital Learning in Teacher Education*, *31*(3), 85–92. https://doi.org/10.1080/21532974.2015.1021982

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Bowers, A., Bang, A., Pan, Y., & Graves, K. (2019). *Education Leadership Data Analytics (ELDA): A white paper report on the 2018 ELDA summit* (ELDA-TC-2019-01). Columbia University Teacher's College. https://files.eric.ed.gov/fulltext/ED602366.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brenan, M. (2018). *Cybercrimes Remain Most Worrisome to Americans*. Gallup. https://news.gallup.com/poll/244676/cybercrimes-remain-worrisome-americans.aspx

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.

California Department of Justice, Privacy Enforcement and Protection Unit. (2016). *Ready for school: Recommendations for the ed tech industry to protect the privacy of student data*. https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ready-for-school-1116.pdf

Student Online Personal Information Protection Act, (2014). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

Camacho, M. (2021, November 5). *I'm a student journalist. A new privacy law is interfering with Chicago's high school newspapers.* Chalkbeat Chicago. https://chicago.chalkbeat.org/2021/11/5/22765913/student-newspapers-chicago-soppa

Carmel, Y. H., Olsher, S., Elkin-Koren, N., & Yerushalmy, M. (2019). eTextbooks: Challenges to pedagogy, law, and policy. In Y. Kali, A. Baram-Tsabari, & A. M. Schejter (Eds.), *Learning In a Networked Society: Spontaneous and Designed Technology Enhanced Learning Communities* (pp. 177–199). Springer International Publishing. https://doi.org/10.1007/978-3-030-14610-8_10

Catalano, F. (2021, January 11). Surveys find districts are using more edtech tools—And teachers are bearing the costs. *EdSurge*. https://www.edsurge.com/news/2021-01-11-surveys-find-districts-are-using-more-edtech-tools-and-teachers-are-bearing-the-costs

Cavaye, A. L. M. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal*, *6*(3), 227–242. https://doi.org/10.1111/j.1365-2575.1996.tb00015.x

Cavoukian, A. (2011). *Privacy by Design: The 7 foundational principles*. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Center for Democracy & Technology. (2020). *Teacher, parent, and student views on education data, technology, and student privacy*. https://cdt.org/wp-content/uploads/2020/10/CDT-student-privacy-parents-teachers-students-research-slides.pdf

Chander, A., Gelman, L., & Radin, M. J. (Eds.). (2008). *Securing privacy in the internet age*. Stanford Law Books.

Chapple, M. (2019). Understanding FERPA: How K–12 schools can update their data privacy approach. *EdTech Magazine*. https://edtechmagazine.com/k12/article/2019/09/understanding-ferpa-how-k-12-schools-can-update-their-data-privacy-approach-perfcon

Chen, A. (2015, November 6). The ever-growing ed-tech market. *The Atlantic*. https://www.theatlantic.com/education/archive/2015/11/quantifying-classroom-tech-market/414244/

Chenail, R. J. (2011). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *The Qualitative Report*, *16*(1), 255–262.

Christensen, C., Johnson, C. W., & Horn, M. B. (2008). *Disrupting class: How disruptive innovation will change the way the world learns* (1st edition). McGraw-Hill.

Clemmensen, T., Kaptelinin, V., & Nardi, B. (2016). Making HCI theory work: An analysis of the use of activity theory in HCI research. *Behaviour & Information Technology*, *35*(8), 608–627. https://doi.org/10.1080/0144929X.2016.1175507

Collins, S., & Vance, A. (2019, July 9). 33 organizations send letter to Florida Governor Desantis. *Student Privacy Compass*. https://studentprivacycompass.org/letterdesantis/

Colorado State Legislature. (2020). *Student data transparency and security act*. https://www.cde.state.co.us/dataprivacyandsecurity/crs22-16-101

Consortium for School Networking. (2021). *2020 State of EdTech leadership survey report*. https://www.cosn.org/focus-areas/leadership-vision/state-edtech-leadership

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (Second edition). SAGE Publications.

Cybersecurity and Infrastructure Security Agency. (2020). *Cyber actors target K-12 distance learning education to cause disruptions and steal data* (No. AA20-345A). https://us-cert.cisa.gov/sites/default/files/publications/AA20-345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf

Daggett, L. M. (2008). FERPA in the twenty-first century: Failure to effectively regulate privacy for all students. *Catholic University Law Review*, *58*, 57.

Darke, P., Shanks, G. G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism. *Inf. Syst. J.*, *8*, 273–290. https://doi.org/10.1046/j.1365-2575.1998.00040.x

Data Quality Campaign. (2016). *Roadmap to safeguarding student data: Key focus areas for state education agencies*. https://dataqualitycampaign.org/wp-content/uploads/2016/03/DQC-roadmap-safeguarding-data-June24.pdf

DataBreaches. (2016, June 7). Info on international students and hosting families exposed in misconfigured database. *DataBreaches.Net*. https://www.databreaches.net/info-on-international-students-and-hosting-families-exposed-in-misconfigured-database/

Davis, K. (2014). Bridging the Innovation-Policy Gap. *SAIS Review of International Affairs*, *34*(1), 87–92. https://doi.org/10.1353/sais.2014.0015

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003

Dearnley, C. (2005). A reflection on the use of semi-structured interviews. *Nurse Researcher*, *13*(1), 19–28. https://doi.org/10.7748/nr2005.07.13.1.19.c5997

DeBaryshe, B. D., Scott, K. G., & Gauci, K. T. (2020). Hawai'i early childhood homelessness needs assessment. *University of Hawai'i Center on the Family*. http://www.hawaiihealthmatters.org/content/sites/hawaii/ECHomelessNeeds_2020.pdf

Denver Public Schools. (n.d.). *Academic Technology Menu*. Retrieved November 13, 2021, from http://atm.dpsk12.org/

Dey, S. (2021, November 1). CPS teachers 'blindsided' after access to popular classroom software yanked due to new student privacy law. *Chicago Sun-Times*. https://chicago.suntimes.com/education/2021/11/1/22749383/cps-soppa-student-online-personal-protection-act-students-data-privacy-public-schools-adobe

Diliberti, M. K., & Kaufman, J. H. (2020). *Will this school year be another casualty of the pandemic?: Key findings from the American educator panels Fall 2020 COVID-19 surveys*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA168-4.html

Dinev, T., Xu, H., Smith, J., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*. https://doi.org/10.1057/ejis.2012.23

Doran, E. (2018, October 30). Central New York schools struggle with ongoing cyberattacks. *Government Technology*. https://www.govtech.com/security/Central-New-York-Schools-Struggle-with-Ongoing-Cyberattacks.html

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, *21*(3), 319–342. https://doi.org/10.1207/s15327051hci2103_2

Durand, R. M., & Lambert, Z. V. (1988). Don't know responses in surveys: Analyses and interpretational consequences. *Journal of Business Research*, *16*(2), 169–188. https://doi.org/10.1016/0148-2963(88)90040-9

Edwards, R. (2015). Software and the hidden curriculum in digital education. *Pedagogy, Culture & Society*, *23*(2), 265–279. https://doi.org/10.1080/14681366.2014.977809

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532–550. JSTOR. https://doi.org/10.2307/258557

Electronic Privacy Information Center (EPIC). (n.d.). *State student privacy policy*. https://epic.org/state-policy/student-privacy/

Elements of a New Ethical Framework for Big Data Research. (2018, June 21). Berkman Klein Center. https://cyber.harvard.edu/node/99428

Elliott, T. L., Fatemi, D., & Wasan, S. (2014). Student privacy rights—History, Owasso, and FERPA. *Journal of Higher Education Theory & Practice*, *14*(4), 34–47.

Encyclopedia Britannica. (2020). *Hawaii: State*. https://www.britannica.com/place/Hawaii-state

Engeström, Y. (1987). *Learning by expanding: An activity-theoretical approach to developmental research*. Orienta-Konsultit. https://doi.org/10.1017/CBO9781139814744

Engeström, Y. (2015). *Learning by Expanding* (2nd ed.). Cambridge University Press.

Engeström, Y., Miettinen, R., & Punamäki, R.-L. (1999). *Perspectives on Activity Theory*. Cambridge University Press.

Epstein, B. (2021, March). *We have no clue how much the U.S. spends on edtech. But it's at least 2x what many of us thought.* https://www.linkedin.com/pulse/we-have-clue-how-much-us-spends-edtech-its-least-2x-what-bart-epstein/

Family Educational Rights and Privacy Act Regulations, 34 C.F.R. § 99 (1974). https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=78804d024b2215bc22206622cec9f8af&mc=true&n=pt34.1.99&r=PART&ty=HTML

Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974). http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title20-section1232g&num=0&edition=prelim

Federal Communications Commission (FCC). (2017, September). *Children's Internet Protection Act (CIPA)*. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Federal Trade Commission. (2004, July 7). *Gateway Learning Settles FTC Privacy Charges*. Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges

Federal Trade Commission. (2019, September 3). *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*. Federal Trade Commission.

https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

Feng, K., & Papadopoulos, S. (2018). Student (K-12) data protection in the digital age: A comparative study. *Comparative and International Law Journal of Southern Africa*, *51*(2), 261–287.

Florida Department of Education. (2018). *DOE bill summary of SB 7026*. http://www.fldoe.org/core/fileparse.php/12031/urlt/SB-7026-Public-Safety.pdf

Foundation for Excellence in Education. (2015). *Protecting K-12 student privacy in a digital age*. https://files.eric.ed.gov/fulltext/ED576766.pdf

Frontiera, C. S. (2019). *A mixed methods study of principals' experience using data analytic tools in Hawai'i* [Thesis, University of Hawai'i at Manoa]. http://scholarspace.manoa.hawaii.edu/handle/10125/63201

Future of Privacy Forum. (2015). *Parental support for technology and data use in schools*. https://fpf.org/wp-content/uploads/2015/11/Beyond-the-Fear-Factor_Sept2015.pdf

Future of Privacy Forum. (2016). *FPF guide to protecting student data under SOPIPA: For K-12 school administrators and ed tech vendors*. https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf

Future of Privacy Forum. (2020). *Issues K-12 Education*. https://fpf.org/issues/k-12-education/

Future of Privacy Forum. (2021a). *Student Data Privacy and Data Ethics Scenarios*. https://studentprivacycompass.org/wp-content/uploads/2021/10/Student-Data-Privacy-Scenarios_Combined.pdf

Future of Privacy Forum. (2021b, October 5). Student privacy primer. *Student Privacy Compass*. https://studentprivacycompass.org/resource/student-privacy-primer/

Garfinkel, S. (2001). *Database nation: The death of privacy in the 21st century*. O'Reilly Media.

Grama, J. L. (2016). *Understanding information security and privacy in postsecondary education data systems*. EDUCAUSE. https://sites.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy.pdf

Grayson, L. P. (1978). Education, technology, and individual privacy. *Educational Communication and Technology*, *26*(3), 195–206.

Gross, A. (2014, May 7). A brief history of education's big data debate. *Education Dive*. https://www.educationdive.com/news/a-brief-history-of-educations-big-data-debate/258602/

Haduong, P., Wood, Z., Cortesi, S., Plunkett, L., Ritvo, D., & Gasser, U. (2015). Student privacy: The next frontier-emerging & future privacy issues in K-12 learning environments. *Berkman Center Research Publication No. 2015-12*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2638022

Hankerson, D. L., Venzke, C., Laird, E., Grant-Chapman, H., & Thakur, D. (2021). *Online and observed: Student privacy implications of school issued devices and student activity monitoring software*. Center for Democracy & Technology. https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-andstudent-activity-monitoring-software/

Hawai‘i Appleseed Center for Law and Economic Justice. (2016). *The State of Poverty in Hawai‘i* (p. 28).

Hawai‘i Board of Education. (2015). *Internet use*. https://boe.hawaii.gov/policies/Board%20Policies/Internet%20Use.pdf

Hawai‘i Department of Education. (2016). *Technology responsible use guidelines*. https://www.hawaiipublicschools.org/DOE%20Forms/FRL/TRUG.pdf

Hawai‘i Department of Education. (2019). *Department announces 2019-20 enrollment figures for public and charter schools*. http://www.hawaiipublicschools.org/ConnectWithUs/MediaRoom/PressReleases/Pages/2019-20-enrollment.aspx

Hawai‘i Department of Education. (2020). *Digital device and application guidance for distance learning*. https://drive.google.com/file/d/1x0gWL6t-AeQBMGHpE2qiLTbUtvA5ggq3/view

Hawai’i Department of Education. (2021). *2020 Hawai‘i Department of Education Data Book*. http://arch.k12.hi.us/reports/hidoe-data-book

Student Online Personal Information Protection Act, §302A-499 (2016). https://www.capitol.hawaii.gov/hrscurrent/vol05_ch0261-0319/HRS0302A/HRS_0302A-0499.htm

HB125, Hawai’i Uniform Employee and Student Online Privacy Protection Act, (2021). https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=HB&billnumber=125&year=2021

Heath, J. (2014). Contemporary privacy theory contributions to learning analytics. *Journal of Learning Analytics*, *1*(1), 140–149. https://doi.org/10.18608/jla.2014.11.8

Herold, B. (2019, May 30). Florida plan for a huge database to stop school shootings hits delays, legal questions. *Education Week*. https://www.edweek.org/ew/articles/2019/05/30/florida-plan-for-a-huge-database-to.html

Hess, F. M., & Eden, M. (2017). The Every Student Succeeds Act: What it means for schools, systems, and states. In *Harvard Education Press*. Harvard Education Press.

Hill, K. (2010, October 11). Lower Merion School District and Blake Robbins Reach a Settlement in Spycamgate. *Forbes*. https://www.forbes.com/sites/kashmirhill/2010/10/11/lower-merion-school-district-and-blake-robbins-reach-a-settlement-in-spycamgate/#552c9fdf2c60

Hobbs, T. D. (2017, October 23). Hackers target nation's schools. *The Wall Street Journal*. https://www.wsj.com/articles/hackers-target-nations-schools-1508751002

Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, *64*(5), 923–938. https://doi.org/10.1007/s11423-016-9477-y

Jonassen, D. H., & Rohrer-Murphy, L. (1999). Activity theory as a framework for designing constructivist learning environments. *Educational Technology Research and Development*, *47*(1), 61–79. https://doi.org/10.1007/BF02299477

Jones, K. M. L., Thomson, J., & Arnold, K. (2014). Questions of data ownership on campus. *EDUCAUSE Review*. https://er.educause.edu/articles/2014/8/questions-of-data-ownership-on-campus

Jones, R. (2017, September 19). Hackers lock down entire school district with threats: "We are savage creatures." *Gizmodo*. https://gizmodo.com/hackers-lock-down-entire-school-district-with-threats-1818542996

Jones, S. J. (2012). Technology review: The possibilities of learning analytics to improve learner-centered decision-making. *Community College Enterprise*, *18*(1). https://link.galegroup.com/apps/doc/A290733902/AONE?sid=lms

Kamenetz, A. (2014, April 28). What parents need to know about big data and student privacy. *National Public Radio*. https://www.npr.org/sections/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy

Kaptelinin, V. (2005). The object of activity: Making sense of the sense-maker. *Mind, Culture, and Activity*, *12*(1), 4–18. https://doi.org/10.1207/s15327884mca1201_2

Karakus, T. (2014). Practices and potential of activity theory for educational technology research. In J. M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of Research on Educational Communications and Technology* (pp. 151–160). Springer. https://doi.org/10.1007/978-1-4614-3185-5_13

Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. *IEEE Security Privacy*, *7*(4), 61–64. https://doi.org/10.1109/MSP.2009.87

Keierleber, M. (2020, October). 'Don't get gaggled': Minneapolis school district spends big on student surveillance tool. *The 74*. https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating-its-police-contract/

Keierleber, M. (2021, September). An inside look at the spy tech that followed kids home for remote learning—And now won't leave. *The 74*. https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/

Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). *2019 state of EdTech privacy report*. Common Sense Media. https://privacy.commonsense.org/content/resource/state-of-edtech-2019/cs-2019-state-of-edtech-privacy-report.pdf

Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). *2021 state of kids' privacy*. Common Sense. https://www.commonsensemedia.org/sites/default/files/research/report/common-sense-2021-state-of-kids-privacy.pdf

Korpelainen, E., & Kira, M. (2013). Systems approach for analysing problems in IT system adoption at work. *Behaviour & Information Technology*, *32*(3), 247–262. https://doi.org/10.1080/0144929X.2011.624638

Krosnick, J., & Presser, S. (2010). Question and questionnaire design. In P. V. Marsden & J. D. Wright (Eds.), *Handbook of survey research* (Second edition, pp. 263–313). Emerald.

Larson, E. (1992). *The naked consumer: How our private lives become public commodities*. Penguin Books.

Lee, S. (2021, November 1). How one school's academic turnaround helped it weather the pandemic. *Honolulu Civil Beat*. https://www.civilbeat.org/2021/11/how-one-schools-academic-turnaround-helped-it-weather-the-pandemic/

Lestch, C. (2015, February 5). Obama finds bipartisan backing for student data privacy pitch. *FedScoop*. https://web.archive.org/web/20150309021250/http://fedscoop.com/bipartisan-bill-on-obamas-student-data-privacy-proposal-to-be-unveiled

Levin, D. A. (2021). *The state of K-12 cybersecurity: 2020 year in review* (p. 25). K-12 Cybersecurity Resource Center. https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf

Lim, N., Grönlund, Å., & Andersson, A. (2015). Cloud computing: The beliefs and perceptions of Swedish school principals. *Computers & Education*, *84*, 90–100. https://doi.org/10.1016/j.compedu.2015.01.009

Lindh, M., & Nolin, J. (2016). Information we collect: Surveillance and privacy in the implementation of Google Apps for Education. *European Educational Research Journal*, *15*(6), 644–663. https://doi.org/10.1177/1474904116654917

Linos, K., & Carlson, M. (2017). Qualitative Methods for Law Review Writing Symposium: Developing Best Practices for Legal Analysis. *University of Chicago Law Review*, *84*(1), 213–238.

Loeb, S., Dynarski, S., McFarland, D., Morris, P., Reardon, S., & Reber, S. (2017). *Descriptive analysis in education: A guide for researchers* (NCEE 2017–4023). Washington, DC: U.S. Department of Education, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance. https://files.eric.ed.gov/fulltext/ED573325.pdf

Lower Merion School District. (2011). *Policy 137: District-issued laptops*. https://resources.finalsite.net/images/v1611931606/lmsdorg/dy9fgquokmi2b4ot9hkr/Policy_P137.pdf

Lynch, C. F. (2017). Who prophets from big data in education? New insights and new challenges. *Theory and Research in Education*, *15*(3), 249–271. https://doi.org/10.1177/1477878517738448

Lynch, T. L. (2015). Soft(a)ware in the English Classroom: Mustard Seeds and Information Feeds: A Short History of Students as Data. *The English Journal*, *105*(1), 96–98.

MacCarthy, M. (2014). Student privacy: Harm and context. *The International Review of Information Ethics*, *21*, 11–24. https://doi.org/10.29173/irie366

Mandinach, E. B., & Gummer, E. S. (2021). *The ethical use of data in education: Promoting responsible policies and practices*. Teachers College Press.

Mandinach, E., & Cotto, J. (2021). The case for including data privacy and data ethics in educator preparation programs. *Student Privacy Compass*. https://studentprivacycompass.org/resource/case-data-privacy-ethics/

Marr, B. (2016, January 13). Big data facts: How many companies are really making money from their data? *Forbes*. https://www.forbes.com/sites/bernardmarr/2016/01/13/big-data-60-of-companies-are-making-money-from-it-are-you/

Martin, D. (2008). A new paradigm to inform inter-professional learning for integrating speech and language provision into secondary schools: A socio-cultural activity theory approach. *Child Language Teaching and Therapy*, *24*(2), 173–192. https://doi.org/10.1177/0265659008090293

McPhie, E. (2019, June). Transparency about data collection is a needed first step of privacy regulation, panelists say at FTC event. *Broadband Breakfast*. http://broadbandbreakfast.com/2019/06/transparency-about-data-collection-is-a-needed-first-step-of-privacy-regulation-panelist-say-at-ftc-event/

Merriam, S. B. (1988). *Case Study Research in Education: A Qualitative Approach* (1 edition). Jossey-Bass.

Merriam, S. B., & Tisdell, E. (2015). *Qualitative Research: A Guide to Design and Implementation, 4th Edition | Wiley*. https://www.wiley.com/en-us/Qualitative+Research%3A+A+Guide+to+Design+and+Implementation%2C+4th+Edition-p-9781119003618

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*, *14*(5), 53–55.

My Future Hawai'i Possible Data Exposure FAQ. (2019, September 6). Hawai'i P-20. http://www.p20hawaii.org/graduationalliancefaq/

Nardi, B. A. (1996). Activity theory and human-computer interaction. In B. A. Nardi (Ed.), *Context and consciousness: Activity theory and human-computer interaction* (pp. 4–8). MIT Press.

National Center for Education & Statistics. (2010). Data stewardship: Managing personally identifiable information in electronic student education records. *SLDS Technical Brief*, *2*. https://nces.ed.gov/pubs2011/2011602.pdf

National Center for Education Statistics. (2015). *LEA Summary of Selected Facts;* https://ocrdata.ed.gov/Page?t=d&eid=29005&syk=8&pid=2278#

National Center for Education Statistics. (2021, May). *English language learners in public schools*. https://nces.ed.gov/programs/coe/indicator/cgf

National Forum on Education Statistics. (2016). *Forum Guide to Education Data Privacy* ((NFES 2016-096); p. 83).

Nehls, K., Smith, B., & Schneider. (2015). *Video-Conferencing Interviews as a Data Collection Method* (pp. 140–157). https://doi.org/10.4018/978-1-4666-6493-7.ch006

Nicosia, M. (2017, May 17). *77 million Edmodo users Are Hacked as Widespread Cyberattacks Hit the Ed Tech World*. https://www.the74million.org/article/77-million-edmodo-users-are-hacked-as-widespread-cyber-attacks-hit-the-ed-tech-world/

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law*, *20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Noy, C. (2008). Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of Social Research Methodology*, *11*(4), 327–344. https://doi.org/10.1080/13645570701401305

O'Connor, N. (2018, January 30). Reforming the U.S. Approach to Data Protection and Privacy. *Council on Foreign Relations*. https://www.cfr.org/report/reforming-us-approach-data-protection

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *Proceedings of the 5th Conference on Information Technology Education*, 177–181. https://doi.org/10.1145/1029533.1029577

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, 29.

Parent Coalition for Student Privacy. (n.d.). *Five principles to protect student privacy*. Retrieved October 10, 2021, from https://studentprivacymatters.org/five-principles-to-protect-study-privacy/

Parent Coalition for Student Privacy. (2019). *2019 State student privacy report card*. https://www.studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf

Park, J., & Vance, A. (2021). *College students' attitudes toward data privacy*. 17.

Patton, M. Q. (2001). *Qualitative research & evaluation methods* (3rd ed.). SAGE Publications.

Penn, M. (2015). *Views from around the globe: 2nd Annual Report on How Personal Technology is Changing our Lives*. Microsoft. https://blogs.microsoft.com/blog/2015/01/19/views-around-globe-2nd-annual-report-personal-technology-changing-lives/

Podesta, J. (2014, May 1). *Findings of the Big Data and Privacy Working Group Review*. The White House. https://obamawhitehouse.archives.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, *71*(12), 1133–1143. https://doi.org/10.1016/j.ijhcs.2013.09.002

Rectanus, K. (2020, December 17). *3 take-aways from the latest analysis of digital learning equity gaps across educators and students in U.S. districts*. https://www.linkedin.com/pulse/3-take-aways-from-latest-analysis-digital-learning-us-karl

Reddy, A. (2020, December 18). *The Trouble With Pasco County's Predictive Policing Program*. Student Privacy Compass. https://studentprivacycompass.org/pasco/

Regan, P. M., & Jesse, J. (2019). Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology*, *21*(3), 167–179. https://doi.org/10.1007/s10676-018-9492-2

Reidenberg, J., Russell, N. C., Kovnot, J., Norton, T. B., Cloutier, R., & Alvarado, D. (2013). Privacy and cloud computing in public schools. *Center on Law and Information Policy*, *2*, 93.

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018). "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies*, *2018*(3), 63–83. https://doi.org/10.1515/popets-2018-0021

Richards, N., & Hartzog, W. (2016). Privacy's trust gap: A review book review. *Yale Law Journal*, *126*, 1180–1224.

Rockingham County Public Schools. (n.d.-a). *Data security and privacy*. Retrieved November 13, 2021, from https://www.rcps.net/en-US/data-security-and-privacy-9f2a150b

Rockingham County Public Schools. (n.d.-b). *Digital resource requests*. Retrieved November 13, 2021, from https://rcps.schoolblocks.com/en-US/digital-resource-requests-966a2d37

Roscorla, T. (2015, July 28). The lowdown on federal student data privacy legislation of 2015. *Government Technology*. https://www.govtech.com/education/k-12/The-Lowdown-on-Federal-Student-Data-Privacy-Legislation-of-2015.html

Rosen, J. (2011). *The unwanted gaze: The destruction of privacy in America*. Knopf Doubleday Publishing Group.

Ross, T., Kim, C., & Rohde, K. (2021, September 18). Protecting student data privacy in the digital age. *The Regulatory Review*. https://www.theregreview.org/2021/09/18/saturday-seminar-protecting-student-data-privacy-in-digital-age/

Rubel, A., & Jones, K. M. L. (2016). Student privacy in learning analytics: An information ethics perspective. *The Information Society*, *32*(2), 143–159. https://doi.org/10.1080/01972243.2016.1130502

Schaffhauser, D. (2017, July). Average cost per record of US data breach in ed: $245. *Campus Technology*. https://campustechnology.com/articles/2017/07/18/average-cost-per-record-of-us-data-breach-in-ed-245.aspx

Seidman, I. (2006). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (3rd ed.). Teachers College Press.

Selwyn, N. (2013). *Distrusting educational technology: Critical questions for changing times*. Routledge. https://doi.org/10.4324/9781315886350

Serwin, A. B., McLaughlin, P., & Tomaszewski, J. (2014). *Privacy, security and information management: An overview*. American Bar Association.

Shear, M. D., & Singer, N. (2015, January 11). Obama to call for laws covering data hacking and student privacy. *The New York Times*. https://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html

Shvartzshnaider, Y., Tong, S., Wies, T., Kift, P., Nissenbaum, H., Subramanian, L., & Mittal, P. (2016). Learning privacy expectations by crowdsourcing contextual informational norms. *Association for the Advancement of Artificial Intelligence*, 10.

Slade, S., Prinsloo, P., & Khalil, M. (2019). Learning analytics at the intersections of student trust, disclosure and benefit. *Proceedings of the 9th International Conference on Learning Analytics & Knowledge*, 235–244. https://doi.org/10.1145/3303772.3303796

Smith, J. (2016). *Exploring the complexities of private sector influence: The case of student data privacy policy* [Doctoral dissertation, University of Southern California]. ProQuest.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York University. http://choicereviews.org/review/10.5860/CHOICE.42-5512

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. JSTOR. https://doi.org/10.2307/40041279

Solove, D. J., & Schwartz, P. (2018). *Information privacy law* (6th Ed). Wolters Kluwer Law & Business.

Stake, R. E. (1995). *The Art of Case Study Research*. SAGE.

State of Hawai‘i Board of Education. (n.d.). *Policies and framework*. Retrieved May 1, 2020, from http://boe.hawaii.gov/policies/Pages/default.aspx

Stewart, D. W., & Shamdasani, P. N. (2014). *Focus Groups: Theory and Practice*. SAGE Publications.

Strauss, V. (2017, September 5). Parents cite student privacy concerns with popular online education platform. *Washington Post*. https://www.washingtonpost.com/news/answer-sheet/wp/2017/08/30/parents-cite-student-privacy-concerns-with-popular-online-education-platform/?utm_term=.c7cbb4dd77d9

Student Data Privacy Consortium. (n.d.). *About the Consortium*. Retrieved May 2, 2020, from https://privacy.a4l.org/privacy-community/

Student Privacy Compass. (n.d.-a). *State student privacy laws*. Student Privacy Compass. Retrieved November 6, 2021, from https://studentprivacycompass.org/state-laws/

Student Privacy Compass. (n.d.b). *Student privacy laws*. https://studentprivacycompass.org/audiences/lawyers/

Sullivan, G. M. (2011). A primer on the validity of assessment instruments. *Journal of Graduate Medical Education*, *3*(2), 119–120. https://doi.org/10.4300/JGME-D-11-00075.1

Ta, L., & Clayworth, J. (2017, October 5). "Dark Overlord" hackers posted stolen student info, Johnston officials say. *Des Moines Register*. https://www.desmoinesregister.com/story/news/crime-and-courts/2017/10/05/dark-overlord-hacker-johnston-schools-threats/735950001/

The Student Data Privacy Project. (n.d.). Retrieved October 9, 2021, from https://www.studentdataprivacyproject.com/takeaction

The White House, Executive Office of the President. (2014). *Big data: Seizing opportunities, preserving values*. https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

Trainor, S. (2015). Student data privacy is cloudy today, clearer tomorrow. *Phi Delta Kappan*, *96*(5), 13–18. https://doi.org/10.1177/0031721715569463

Trusted Learning Environment. (n.d.). *About the Seal*. Retrieved April 30, 2020, from https://trustedlearning.org/about-the-seal/

Trusted Learning Environment. (2017). *TLE self-assessment*. https://trustedlearning.org/resources/

UC San Diego. (2021). *How to design training*. https://blink.ucsd.edu/HR/training/instructor/tools/training.html#1.-Identify-the-need-for-traini

United Health Foundation. (2019). *Hawai'i 2019 State Summary Report*. America's Health Rankings. https://www.americashealthrankings.org/learn/reports/2019-annual-report/state-summaries-hawaii

University of Hawai'i News. (2019, September 6). *Investigation finds no evidence of data removal, My Future Hawai'i turned off*. https://www.hawaii.edu/news/article.php?aId=10179

U.S. Census Bureau. (2010). *U.S. Census Bureau QuickFacts*. https://www.census.gov/quickfacts/fact/table/US/PST045219

U.S. Department of Education. (2008, December 17). *Dear colleague letter about Family Educational Rights and Privacy Act (FERPA) final regulations* [Letters (Correspondence); Policy Guidance]. https://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht12-17-08.html

U.S. Department of Education. (2016). *Cyber advisory: New type of cyber extortion/threat attack*. U.S. Department of Education.

U.S. Department of Education. (2017). *Hawai'i Consolidated State Plan* (OMB No. 1810-0576). https://www2.ed.gov/admins/lead/account/stateplan17/hiconsolidatedstateplanfinal.pdf

U.S. Department of Education, Family Policy Compliance Office. (2007). *Turnitin letter to the Catholic University of America*. 2.

U.S. Department of Education, Privacy Technical Assistance Center. (2014a). *Protecting student privacy while using online educational services: Requirements and best practices*. U.S. Department of Education. https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

U.S. Department of Education, Privacy Technical Assistance Center. (2014b). *Transparency best practices for schools and districts*. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LEA%20Transparency%20Best%20Practices%20final.pdf

U.S. Department of Education, Privacy Technical Assistance Center. (2015a). *Checklist for developing school district privacy programs*. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Checklist_District_Privacy_Program_0.pdf

U.S. Department of Education, Privacy Technical Assistance Center. (2015b). *Data Governance Checklist*. 5.

U.S. Department of Education, Student Privacy Policy Office. (2021). *Local education agency website student privacy transparency reviews: Combined three-year report summary* (p. 16). https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LEA_Year1-3_CombinedReport%20Summary_Final.pdf

Utah State Board of Education. (n.d.). *Student data privacy*. Retrieved November 13, 2021, from https://schools.utah.gov/studentdataprivacy

Utah State Board of Education. (2020, April 6). *DPA flowchart*. https://schools.utah.gov/file/86fa6d45-958e-49da-b0e0-a0caa81bd683

Student Privacy and Data Protection, H.B. 358 (2016). https://le.utah.gov/xcode/Title53E/Chapter9/53E-9-P3.html

Van Eijk, R., & Zanfir-Fortuna, G. (2021, February). Understanding interconnected local and global data flows. *Future of Privacy Forum*. https://fpf.org/blog/understanding-the-retail-data-ecosystem-and-edtech-data-flows/

Vance, A. (2016a). Data privacy laws follow lead of Oklahoma and California. *National Association of State Boards of Education*, 4.

Vance, A. (2016b). Data privacy laws follow lead of Oklahoma and California. *State Education Standard*, *16*(2), 25.

Vance, A., & Sallay, D. (2020, March). FAQs: The Protection of Pupil Rights Amendment. *Student Privacy Compass*. https://studentprivacycompass.org/faqs-ppra/

Vega, V., & Robb, M. B. (2019). *2019 the Common Sense census: Inside the 21st-century classroom*. Common Sense Media. https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom_1.pdf

Vickery, J. R. (2015). 'I don't have anything to hide, but … ': The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, *18*(3), 281–294. https://doi.org/10.1080/1369118X.2014.989251

Vu, P., Adkins, M., & Henderson, S. (2019). Aware, but don't really care: Student perspectives on privacy and data collection in online courses. *Journal of Open, Flexible and Distance Learning*, *23*(2), 42–51. https://doi.org/10.3316/informit.980808045440057

Walt, G., & Gilson, L. (1994). Reforming the health sector in developing countries: The central role of policy analysis. *Health Policy and Planning*, *9*(4), 353–370. https://doi.org/10.1093/heapol/9.4.353

Wan, T. (2017, April 20). *Schoolzilla 'File Configuration Error' Exposes data for more than 1.3m students*. EdSurge News. https://www.edsurge.com/news/2017-04-20-schoolzilla-file-configuration-error-exposes-data-for-more-than-1-3m-students-staff

Warren, S. D., & Brandeis, L. D. (1890). Right to Privacy. *Harvard Law Review*, *4*, 193–220.

Watters, A. (2013, October 17). *Student data is the new oil: MOOCs, metaphor, and money*. Hack Education. http://hackeducation.com/2013/10/17/student-data-is-the-new-oil

Weippl, E. R., & Min Tjoa, A. (2005). Privacy in e-learning: Anonymity, pseudonyms and authenticated usage. *Interactive Technology and Smart Education*, *2*(4), 247–256. https://doi.org/10.1108/17415650580000048

Willis, J. E., Slade, S., & Prinsloo, P. (2016). Ethical oversight of student data in learning analytics: A typology derived from a cross-continental, cross-institutional perspective. *Educational Technology Research and Development*, *64*(5), 881–901. https://doi.org/10.1007/s11423-016-9463-4

Yeaman, A. R. J. (2015). If it was illegal, the technology wouldn't allow it. *TechTrends*, *59*(3), 11–12. https://doi.org/10.1007/s11528-015-0846-x

Yin, R. K. (2014). *Case Study Research: Design and Methods* (5th ed.). SAGE.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1 edition). PublicAffairs.

APPENDIX A. Permission to use Activity Theory diagram

UNIVERSITY of HAWAI'I SYSTEM

Minara Mordecai <minara@hawaii.edu>

Permission to use Activity Theory diagram in PhD dissertation

Engeström, Yrjö H M <yrjo.engestrom@helsinki.fi> Mon, Oct 18, 2021 at 6:29 AM
To: Minara Mordecai <minara@hawaii.edu>

Dear Minara, I hereby give you permission to use the diagram mentioned below in your message.

Best regards,

Yrjö Engeström
[Quoted text hidden]

APPENDIX B. Consent form and survey questions

Research Study: Student Data Privacy in K-12

Start of Block: Informed Consent

Welcome to my research study! My name is Minara Mordecai and you are invited to take part in a research study titled "*Student Data in the 21st Century: Balancing Privacy and Innovation*." I am a Ph.D. student at the UH Mānoa, College of Education. This project is part of the requirements for earning my doctoral degree in Learning Design and Technology. In addition to its academic purpose, this study is rooted in my commitment to public education, fairness, and student privacy, and I hope to contribute to understanding of student privacy issues in K-12 in Hawai'i.

I have been approved to conduct the study by both the University of Hawai'i IRB Office and the HIDOE Data Governance Office (approval letters) (link to dissertation website).

What am I being asked to do? If you participate in this project, you will be asked to fill out an anonymous 15-minute online survey.

Taking part in this study is your choice. Your participation in this project is completely voluntary. You may stop participating at any time. If you stop being in the study, there will be no penalty or loss to you.

Why is this study being done? The purpose of my project is to evaluate perceptions and practices regarding student data privacy by state administrators at HIDOE. The survey is a part of a larger case study research to understand the policies and regulations that guide K-12 student data sharing, and to assess current practices in a single school district from a perspective of diverse administrators. I am asking you to participate because you have worked closely with compliance, collection, management, governance, or security of student data.

What will happen if I decide to take part in this study? You will be asked to respond to an anonymous survey with 30 multiple-choice and 1 open-ended question. The survey includes

questions such as, "I believe the state office has up to date policies and regulations addressing data privacy compliance requirements (Agree or Disagree on 1-4 scale)."

How long is the survey? It should take approximately 15 minutes.

What are the risks and benefits of taking part in this study? I believe there is little risk to you for participating in this research project. You may become uncomfortable answering any of the survey questions, in which case you can skip the question or take a break. You can also stop taking the survey or withdraw from the project altogether by not submitting the survey. You may review the questions to the survey before submission at the survey link below. There will be no direct benefit to you for participating in this survey. The results of this project may help improve understanding, practices, and future safeguards for student privacy at HIDOE.

Confidentiality and Privacy: I will not ask you for any personal information, such as your name or address. Please do not include any personal information in your survey responses. I will keep all study data secure on a password protected computer. Only my University of Hawai'i advisor and I will have access to the information. Other agencies that have legal permission have the right to review research records. The University of Hawai'i Human Studies Program has the right to review research records for this study. De-identified findings and the final dissertation will be published and available for you to review.

Compensation: You will not receive compensation for participating in this research project.

Timeline and Future Research Studies: The study will take place during SY 20-21. No identifiers will be collected or reported. Even after removing identifiers, the data from this study will not be used or distributed for future research studies.

Questions: If you have any questions about this study, please email me at minara@hawaii.edu. You may also contact my dissertation advisor, Dr. Seungoh Paek, at spaek@hawaii.edu. You may contact the UH Human Studies Program at 808.956.5007 or uhirb@hawaii.edu to discuss problems, concerns and questions, obtain information, or offer input with an informed individual who is unaffiliated with the specific research protocol. Please visit http://go.hawaii.edu/jRd for more information on your rights as a research participant. You may download or print a PDF copy of the consent form for your reference. I invite you to email me if you would like to receive aggregated results of this survey.

Please respond to this survey by **March 25**. Mahalo for your support and participation!

By clicking the button below, you acknowledge:

Your participation in the study is voluntary. You are 18 years of age. You are aware that you may choose to terminate your participation at any time for any reason.

- ○ I consent, begin the study (1)
- ○ I do not consent, I do not wish to participate (2)

End of Block: Informed Consent

Start of Block: Block 1

Please select the response that best reflects your understanding or perception of each statement.

* *This survey was based on the Consortium for School Networking (CoSN) policies and procedures checklist for the Trusted Learning Environment (TLE) seal.*

Q1 I believe our school system has up-to-date policies and regulations addressing data privacy compliance requirements.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q2 I believe the actions and decisions of the senior administrators reflect support of data privacy and security practices.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q3 I believe the school system's policies and procedures set clear expectations for:

	Strongly agree (1)	Somewhat agree (2)	Neither agree nor disagree (3)	Somewhat disagree (4)	Strongly disagree (5)
Protection of student data privacy (6)	○	○	○	○	○
Transparent use of data (7)	○	○	○	○	○

Q4 The state office provides transparent and accessible notices regarding the collection and use of student data to the outside community (ex. annual parent notification regarding student information privacy).

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q5 The state office has identified a senior administrator who is responsible for development and implementation of data privacy and data security policies and practices.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)
- ○ I don't know (6)

Q6 The state office has an active Data Governance committee or a working group.

- ○ Strongly agree (46)
- ○ Somewhat agree (47)
- ○ Neither agree nor disagree (48)
- ○ Somewhat disagree (49)
- ○ Strongly disagree (50)
- ○ I don't know (51)

Q7 I believe the school system ensures adequate resources are available to meet data privacy and security needs.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q8 The school system has implemented a vetting process for external vendors for data privacy and security (ex. external vendor = Google Classroom).

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)
- ○ I don't know (6)

Q9
I believe the school system regularly educates its employees about the importance of the use of the established vetting process for online services.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q10 The school system provides employees with sufficient resources that facilitate student data privacy and data security (ex. template contract language and data sharing agreements).

- Strongly agree (1)
- Somewhat agree (2)
- Neither agree nor disagree (3)
- Somewhat disagree (4)
- Strongly disagree (5)
- I don't know (6)

Q11 The school system ensures that all procurement contracts that deal with student data include enforceable data privacy and security requirements.

- Strongly agree (1)
- Somewhat agree (2)
- Neither agree nor disagree (3)
- Somewhat disagree (4)
- Strongly disagree (5)
- I don't know (6)

Q12
The school system website includes its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.

- ○ Strongly agree (11)
- ○ Somewhat agree (12)
- ○ Neither agree nor disagree (13)
- ○ Somewhat disagree (14)
- ○ Strongly disagree (15)
- ○ I don't know (16)

Q13 The school system data privacy policies include information about the following:

	Strongly agree (76)	Somewhat agree (77)	Neither agree nor disagree (78)	Somewhat disagree (79)	Strongly disagree (80)	I don't know (81)
Data retention period for student records (6)	○	○	○	○	○	○
Data transmission (7)	○	○	○	○	○	○
Technical protocols (8)	○	○	○	○	○	○
Methods and controls to limit access (9)	○	○	○	○	○	○

Q14 The school system has enforceable policies regarding storage of data on local computers, mobile devices, storage devices, and other cloud-related services.

- Strongly agree (1)
- Somewhat agree (2)
- Neither agree nor disagree (3)
- Somewhat disagree (4)
- Strongly disagree (5)
- I don't know (6)

Q15
The school system utilizes a specific role-based process when granting access to educators, staff, and contractors to data and technology systems.

- Strongly agree (6)
- Somewhat agree (7)
- Neither agree nor disagree (8)
- Somewhat disagree (9)
- Strongly disagree (10)
- I don't know (11)

Q16
The school system has a documented process in place to communicate data incidents to appropriate stakeholders.

- ○ Strongly agree (11)
- ○ Somewhat agree (12)
- ○ Neither agree nor disagree (13)
- ○ Somewhat disagree (14)
- ○ Strongly disagree (15)
- ○ I don't know (16)

Q17
The school system has a continuity and disaster recovery plan for data, which is verified and tested on an established, regular basis.

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q18 Parents are offered awareness training and resources to learn how to protect children's privacy (ex. a tutorial video on safety of online activities).

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q19 **State office employees** participate in annual student data privacy training related to applicable federal and/or state laws.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q20 All **school-level personnel** participate in annual student data privacy training related to applicable federal and/or state laws.

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q21 Privacy and security of student data is mentioned in training and professional development in all areas of school operations and academics.

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q22 Schools are required to offer curriculum to promote student information literacy, digital citizenship, and Internet safety.

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q23 In general, I believe teachers are aware of the established process for vetting external vendors when they wish to introduce a new app in the classroom.

- ○ Strongly agree (13)
- ○ Somewhat agree (14)
- ○ Neither agree nor disagree (15)
- ○ Somewhat disagree (16)
- ○ Strongly disagree (17)
- ○ I don't know (18)

Q24 Teachers are asked to model appropriate use and protection of student data for their students.

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q25 Teachers are provided with guides for how to clearly answer questions from parents about the collection, use, and protection of student data.

- ○ Strongly agree (6)
- ○ Somewhat agree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat disagree (9)
- ○ Strongly disagree (10)
- ○ I don't know (11)

Q26 I feel well informed about the type of data collected about our students by the external online vendors.

- ○ Strongly agree (1)
- ○ Somewhat agree (2)
- ○ Neither agree nor disagree (3)
- ○ Somewhat disagree (4)
- ○ Strongly disagree (5)

Q27 I am familiar in the requirements of the following laws:

	Very familiar (1)	Somewhat familiar (2)	Neutral (3)	Know a little (4)	Not familiar at all (5)
Family and Educational Rights and Privacy Act (FERPA) (6)	○	○	○	○	○
Children's Online Privacy Protection Act (COPPA) (7)	○	○	○	○	○
Children’s Internet Protection Act (CIPA) (8)	○	○	○	○	○
Protection of Pupil Rights Amendment (PPRA) (9)	○	○	○	○	○
Hawai'I Bill SB 2607: Student Online Personal Information Protection Act (11)	○	○	○	○	○
(10)	○	○	○	○	○

Q28 HIDOE should prioritize the following to improve student data privacy (with 1 as top priority):
_____ Improve communication between units tasked with data privacy (6)
_____ Increase personnel dedicated to data privacy and security (7)
_____ Increase funds dedicated to data privacy and security (8)
_____ Increase number of trainings on data privacy (9)
_____ Improve training content (10)
_____ Do nothing (11)

Q29 My experience with student data privacy is largely in the context of (select best answer):

- ○ Compliance (1)
- ○ Educational Technology (2)
- ○ Information Technology (3)
- ○ Data Governance (4)
- ○ School Improvement (7)
- ○ Other (5) _____
- ○ Prefer not to answer (6)

Q30 I have been employed at HIDOE for (optional):

- ○ 0-5 years (1)
- ○ 6-15 years (2)
- ○ 15 or more years (3)
- ○ Prefer not to answer (6)

Q31 Please share any additional comments about the current practices or your perceptions related to student data privacy at HIDOE.

_____

End of Block: Block 1

APPENDIX C. Phase 3: Interview Consent Form, Invitations, and Protocol

1. Interview consent form (electronic distribution)

Aloha! My name is Minara Mordecai and you are invited to take part in a research study titled "*Student Data Privacy in K-12*." I am a graduate student at the University of Hawai'i at Mānoa in the Department of Learning Design and Technology. This project is part of the requirements for earning my graduate degree.

What am I being asked to do?
You are asked to participate in a one-on-one online interview with me to talk about your shared experiences in regards to protecting student data privacy at your schools. The interview will be confidential, take place **online**, and will last no longer than 60 minutes. I am inviting you to participate because your work as an educator may require management of student data or ensuring protection of student records when working with outside vendors.

Taking part in this study is your choice.
Your participation in this project is completely voluntary. You may stop participating at any time. If you stop being in the study, there will be no penalty or loss to you.

Why is this study being done?
The purpose of the interview is to understand your experiences, challenges, and successes in safeguarding student data privacy. The interview is a part of a larger case study research to understand the policies and regulations that guide K-12 student data sharing, and to assess current practices in a single school district from a perspective of diverse administrators.

What will happen if I decide to take part in this study?
The interview will be guided by approximately 6 open-ended questions and will last about 50-60 minutes. Interview will include questions such as, "In your experience, what have been some of the challenges in protecting student records when working with outside vendors?"

With your permission, I will audio-record the interview so that I can later transcribe it and analyze the responses. This recording will only be used for transcribing and will not be part of final data.

What are the risks and benefits of taking part in this study?
I believe there is little risk to you in participating in this research project. You may become stressed or uncomfortable answering any of the questions or discussing topics during the interview. If you do become stressed or uncomfortable, you can skip the question or take a break. You can also stop participating at any time.

There will be no direct benefit to you for participating in this interview. The results of this project may help improve practices and policies in regards to student data privacy.

Privacy and Confidentiality: All interviews will remain confidential. When I report the results of my research project, I will not use your name. I will not use any other personal information that

can identify you. I will use pseudonyms (not your real name) and report my findings in a way that protects your privacy and confidentiality to the extent allowed by law.

I will keep all study data secure on a password protected computer. After I successfully defend my dissertation, I will erase or destroy the audio-recordings.

Only my University of Hawai'i advisor and I will have access to the information. Other agencies that have legal permission have the right to review research records. The University of Hawai'i Human Studies Program has the right to review research records for this study.

Compensation:
You will not receive any compensation for participating in this project.

Questions:
If you have any questions about this study, please email me at minara@hawaii.edu. You may also contact my dissertation advisor, Dr. Seungoh Paek, at spaek@hawaii.edu. You may contact the UH Human Studies Program at 808.956.5007 or uhirb@hawaii.edu. to discuss problems, concerns and questions; obtain information; or offer input with an informed individual who is unaffiliated with the specific research protocol. Please visit http://go.hawaii.edu/jRd for more information on your rights as a research participant.

Please select one of the following:

I consent to be audio-recorded for the interview portion of this research. The recording will be used for transcription only (optional)

☐ Yes

☐ No

Signature(s) for Consent:

I give permission to join the research project titled *Student Data Privacy in K-12.*

Name of Participant	**Signature of the Person Obtaining Consent**
Participant's Signature	
	Date

Keep a copy of the informed consent for your records and reference.

2. **Email invitation to participate**

Subject: Invitation to Participate in an Interview

Dear _____,

My name is Minara Mordecai and I invite you to take part in a research study "Student Data Privacy in K-12." I am a PhD student at the University of Hawai'i at Mānoa, College of Education. My research seeks to **evaluate perceptions and practices related to student data privacy** among K-12 educators. I invite you to participate in an **online interview** as part of my study. This research will be part of the requirements for earning my doctorate degree and has been approved by the HIDOE Data Governance Office (see link below).

Student data privacy has become a critically important topic for school administrators. Driven by the COVID-19 pandemic and distance learning, ed tech tools are now a necessity in every classroom, but their use has raised questions as to the protection of student privacy particularly with outside vendors. Educators face questions such as: Can a vendor track student's online activity without parental consent? Can teachers give up data rights when they agree to Terms of Service? These issues are of particular importance for public schools because of privacy constraints imposed by FERPA. Schools are faced with the delicate balance between innovation and privacy.

What you are being asked to do:
I will be conducting online interviews with administrators and educators with the goal of understanding your shared experiences in regards to safeguarding student data privacy. **To participate, please fill out this Doodle form [link] and indicate your availability.** I will follow up with the final date and a Zoom link information. **All participation in this study is voluntary and confidential**. Any personally identifiable information will not be part of the published research.

I appreciate and value your busy schedule during these challenging times. Your time commitment in this study will be **60 minutes or less**. Should you have any questions about this study, I invite you to read my dissertation proposal at: http://go.hawaii.edu/JU2. I hope the results of this research will become useful to Hawai'i educators in understanding the challenges of protecting privacy of student records in the digital era. Please feel free to email me or my faculty advisor, Dr. Seungoh Paek, spaek@hawaii.edu, for additional information.

HIDOE Research Approval Letter: http://go.hawaii.edu/JUG
Consent Form Notification: Attached.

Thank you so much for your support,

Minara Mordecai
PhD Candidate, Learning Design and Technology
University of Hawai'i at Mānoa/Ke Kulanui o Hawai'i ma Mānoa

Faculty advisor: Dr. Seungoh Paek, spaek@hawaii.edu

3. Email follow-up

Subject: Link to participate in an online interview on student data privacy

Dear _____,

Thank you for agreeing to participate in an interview for my study on student data privacy. To confirm, I have scheduled your interview for [date, time]. The Zoom link to connect to the interview is listed below.

Interview Session link: [Zoom link]

The attached consent form [link to consent form collected electronically via Google Forms] provides information about your rights as a participant. Please review, type your name, and submit before the interview.

I will use UH-licensed Zoom account for the interviews. Please let me know if you need assistance using this software, or prefer an alternative web conferencing service.

I look forward to speaking with you soon.

Mahalo,

Minara Mordecai
PhD Candidate, Learning Design and Technology
University of Hawai'i at Manoa/Ke Kulanui o Hawai'i ma Mānoa
Faculty advisor: Dr. Seungoh Paek, spaek@hawaii.edu

4. Interview protocol

Aloha _____,

Thank you so much for joining me for this interview. I'm Minara Mordecai and I am a graduate student at the University of Hawai'i at Mānoa in the Department of Learning Design and Technology. Last year I worked with HIDOE in preparation of the Computer Science Landscape Report and the Statewide CTE Needs Assessment report. I have worked in higher education for the past 13 years. I occasionally teach as a lecturer at the College of Education. I have a law degree and I am currently completing a PhD degree. As you know, I am conducting research to gather practices, perceptions, and shared experiences of K-12 educators when it comes to protecting student data privacy. This interview will last 50-60 minutes. I will facilitate the discussion with open-ended questions. I encourage you to provide additional information that you think is relevant.

To reiterate, I will not use names or other information that may identify you in my dissertation. You may stop and withdraw your consent at any point of this interview. [optional] *You indicated that you agree to audio recording of this interview for transcription purposes only. I will not share the recording publicly and will delete it after my dissertation is approved*.

1) I'd like to begin with your current responsibilities as an educator. Could you describe how you interact with student data in your day to day operations?

2) Do you work with outside vendors who gain access to student records?

- If yes, what is your process for vetting the vendors and ensuring protection of student records

3) I conducted an anonymous survey among state-level administrators at HIDOE, which revealed that the top priorities in improving student data privacy are: [state top priorities from the survey results]. Do you agree with that? If not, what would you say are the priorities in your school or complex area?

4) What resources do you rely on in assessing whether classroom technology infringes on student privacy?

5) As educators, how do you and your colleagues support each other when it comes to student privacy?

6) What have been some of the barriers in safeguarding student data? How would you help eliminate these?

Thank you so much for your time and thoughtful responses. I will be happy to share my dissertation results with you if you're interested, please email me at minara@hawaii.edu. Also, don't hesitate to contact me if you have any questions. Mahalo!

APPENDIX D. Research Approval Letters

UNIVERSITY of HAWAI'I® MĀNOA

Office of Research Compliance
Human Studies Program

DATE:	August 28, 2020
TO:	Paek, Seungoh, University of Hawaii at Manoa, Department of Learning Design and Technology Mordecai, Minara, University of Hawaii at Manoa, Department of Learning Design and Technology
FROM:	Rivera, Victoria, Dir, Ofc of Rsch Compliance, Social&Behav Exempt
PROTOCOL TITLE:	Student Data Privacy in K-12
FUNDING SOURCE:	None
PROTOCOL NUMBER:	2020-00440
APPROVAL DATE:	August 28, 2020

NOTICE OF APPROVAL FOR HUMAN RESEARCH

This letter is your record of the Human Studies Program approval of this study as exempt.

On August 28, 2020, the University of Hawaii (UH) Human Studies Program approved this study as exempt from federal regulations pertaining to the protection of human research participants. The authority for the exemption applicable to your study is documented in the Code of Federal Regulations at 45 CFR 46.104(d) 2.

Exempt studies are subject to the ethical principles articulated in The Belmont Report, found at the OHRP Website www.hhs.gov/ohrp/humansubjects/guidance/belmont.html.

Exempt studies do not require regular continuing review by the Human Studies Program. However, if you propose to modify your study, you must receive approval from the Human Studies Program prior to implementing any changes. You can submit your proposed changes via the UH eProtocol application. The Human Studies Program may review the exempt status at that time and request an application for approval as non-exempt research.

In order to protect the confidentiality of research participants, we encourage you to destroy private information which can be linked to the identities of individuals as soon as it is reasonable to do so. Signed consent forms, as applicable to your study, should be maintained for at least the duration of your project.

This approval does not expire. However, please notify the Human Studies Program when your study is complete. Upon notification, we will close our files pertaining to your study.

If you have any questions relating to the protection of human research participants, please contact the Human Studies Program by phone at 956-5007 or email uhirb@hawaii.edu. We wish you success in carrying out your research project.

UH Human Studies Program, Office of Research Compliance
Office of the Vice President for Research and Innovation, University of Hawai'i, System
2425 Campus Road, Sinclair 10, Honolulu HI 96822
Phone: 808.956.5007 • Email: uhirb@hawaii.edu
https://www.hawaii.edu/researchcompliance/human-studies
An Equal Opportunity & Affirmative Action Institution

UNIVERSITY of HAWAI'I® MĀNOA

Office of Research Compliance
Human Studies Program

DATE:	April 27, 2021
TO:	Paek, Seungoh, University of Hawaii at Manoa, Department of Learning Design and Technology Mordecai, Minara, University of Hawaii at Manoa, Department of Learning Design and Technology
FROM:	Rivera, Victoria, Dir, Ofc of Rsch Compliance, Social&Behav Exempt
PROTOCOL TITLE:	Student Data Privacy in K-12
FUNDING SOURCE:	Graduate Student Organization (GSO)
PROTOCOL NUMBER:	2020-00440
	Approval Date: April 27, 2021 Expiration Date: August 27, 2070

NOTICE OF APPROVAL FOR HUMAN RESEARCH

This letter is your record of the Human Studies Program approval of this study as exempt.

On April 27, 2021, the request for IRB approval of changes to your exempt project noted above has been reviewed and approved. The proposed amendments will be added into your current project file. The proposed changes do not alter the exempt status of your project. The authority for the exemption applicable to your study is documented in the Code of Federal Regulations at 45 CFR 46.101(b) 2.

This approval does not expire. However, please notify the Human Studies Program when your study is complete. Upon notification, we will close our files pertaining to your study.

If you have any questions relating to the protection of human research participants, please contact the Human Studies Program by phone at 956-5007 or email uhirb@hawaii.edu. We wish you success in carrying out your research project.

DAVID Y. IGE
GOVERNOR

DR. CHRISTINA M. KISHIMOTO
SUPERINTENDENT

STATE OF HAWAI`I
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAI`I 96804

OFFICE OF THE SUPERINTENDENT

February 22, 2021

Ms. Minara Mordecai
3448 Oahu Ave
Honolulu, HI 96822

Re: Research Application Decision

Dear Ms. Mordecai:

I am pleased to approve your Hawaii State Department of Education (HIDOE) research application for the study "Student Data Privacy in K12" (Application #2020016).

This approval will expire July 31, 2021. If you require additional time to complete your study, you must submit a request for an extension or another application before this approval expires. If you intend to make changes to your project, you must submit the change request to the Data Governance and Analysis Branch prior to implementing the change. These changes include but are not limited to (1) any changes that require approval from your Institutional Review Board and (2) any changes that are in conflict with or not included in this approval letter. Significant changes may need to be reviewed by the Research Review Committee at their next scheduled meeting. If changes are approved, a modified approval letter will be issued to the researcher and affiliated state/district office staff.

As described in your application, the objective of your study is:

- To understand the policies and regulations that guide K-12 student data management practices and to assess current practices in a single school district from a perspective of diverse system-level and school-level administrators.

You must present this letter to the appropriate HIDOE administrator(s) upon invitation to participate in your research.

You have also indicated that you will be inviting the following individuals to participate in your study:

- A representative from the Data Governance and Analysis Branch (DGA)
- Select HIDOE personnel
- All Complex Area Superintendents or their designees

The DGA representative who participates in your study will be involved in the following activities:

- A brief interview with the researcher

Select HIDOE personnel who participates in your study will be involved in the following activities:

- Complete an online anonymous survey that will be emailed to them.

Complex Area Superintendents or their designees who participate in your study will be involved in the following activities:

- Participants will be emailed an invitation to participate in one of three on-line focus groups.
- Participants may participate in multiple focus groups if they choose to.
- Each focus groups will be 60-90 minutes in duration.
- The focus groups and will ask participants about their data management practices in a K-12 setting focus group.

You will also collect the following data about select HIDOE personnel:

- Survey results

You will also collect the following data about Complex Area Superintendents or their designees:

- Transcription of on-line focus group

As you proceed with your study, please be aware of the following:

- The participation of HIDOE schools, offices, students, and personnel in your study is strictly voluntary.
- All study activities must take place at dates, times, and locations agreed upon by the administrators of the participating HIDOE schools and offices.
- Any compensation provided to HIDOE personnel for participation in your study must be for activities completed outside of instructional and work hours and must be in compliance with the Hawaii State Ethics Code. Any questions about this topic should be referred to the Data Governance and Analysis Branch.
- You are required to conduct your study in accordance with both the conditions of approval described in this letter and the document "Affirmation and Acknowledgement of the Processes, Procedures, and Conditions for Conducting Research in the Hawaii State Department of Education" (the "Affirmation Form for Researchers"). See Attachment 1.
- You are responsible for ensuring that all individuals involved in this study — both those affiliated with your organization and those contracted by your organization and affiliated with external entities or vendors — adhere to all of the conditions of my approval, including those detailed in this letter and those stipulated by the Affirmation Form for Researchers.

Should you have any questions about the above, please contact Ke‘ala Fukuda, HIDOE Data Governance and Analysis Branch, at DOEresearch@k12.hi.us or at (808) 784-6061.

Best wishes for a successful study. We look forward to receiving your findings and recommendations.

Sincerely,

Rodney Luke
Assistant Superintendent

RL:jh
Attachment: Affirmation Form

c: Data Governance and Analysis Branch