It's Inappropriate Because You Can See It- Regulating, Pruning, and Understanding Revealed Thinking in Education

Dr. Stephanie A Sadownik [iD][1]

[1]Curriculum, Teaching and Learning, University of Toronto, Canada

Abstract

Qualitative data from a two-year study provides school administration and technology staff understandings and challenges with their use of surveillance in their role. School administration and technology staff offer their understandings of their need to conduct privacy impact assessments (PIA) when student personally identifiable data may be collected, stored or disseminated to 3ʳᵈ parties. Connections between advancements of privacy in electronic health records and recordkeeping of student confidential information is discussed as it relates to storing of confidential data and the inappropriateness of an all-access pass for employees.

Keywords: At-risk students; Data-driven Decision Making; Tracking

[1][iD] https://orcid.org/0000-0002-1520-7261

Introduction

The ability of a teacher or student to hold inappropriate information on their own device while on school grounds raises the question of the appropriateness of surveillance by educational institutions for bring your own devices (BYODs). Personally identifiable medical information is filed with education records in schools and may be used by multiple stakeholders to develop individual education plans and accommodations for students. Many school districts utilize sophisticated technology to secure confidential information and to identify possible threats. Of particular interest is the use of surveillance guised under the insider threat model, typically used in business as a way of controlling the leaking of documents to outsiders and controlling the communication of trade secrets or espionage (Huth, 2013). Surveillance may be used for punitive reasons to report negative messaging in personal communication, hate or the accessing of inappropriate websites instead of controlling the dissemination of confidential information such as identified students with behaviour or medical conditions that need to be provided to guest teachers. "Being mindful of the purpose and extent of monitoring is a theme discussed in privacy guidelines" (ibid, p. 370).

In the United States, "Computer Emergency Readiness Team (CERT) is sponsored by the Department of Homeland Security. It researches technical and behavioral aspects of insider threats. We maintain a case database of malicious insider threat incidents, typically sabotage, fraud, theft of intellectual property, and espionage" (Huth, 2013, p. 368). While studies comparing Australia and Slovenia's implementation of Electronic Health Records noted legal liabilities for the improper handling of protected information (Cripps et al., 2011; Dixon, 2007). "It was found that the strategic, organizational and human challenges are usually more difficult to master than technical aspects (Deutsch et al., 2010 as cited by Cripps et al., 2011, p. 132).

The network has the ability to identify non-school district technology and devices and offers an alternative school wireless fidelity (Wi-Fi) connection that limits the access of the user to confidential and secure documents. The network provides access to the internet but cannot connect to SMART boards or other school owned technology on site. This accords school districts the ability to safeguard the school community from information that is not regulated by the school, or devices not owned by the school and therefore unavailable for threat assessments.

Confidential information stored on secure networks in school settings are inaccessible by Bring Your Own Device (BYOD) devices not owned by the school district and remain secure. However, as is normally the case, human error is the cause for most privacy breaches. Visitors to the schools, most often teachers on call/substitute teachers are also given access to confidential information related to students in classes and this information can be provided on lesson plans that are printed off or emailed out. This was noted by researchers in China who noted that in hospitals or health care settings users who were unable to exchange patient clinical information electronically, distributed "paper copies of their clinical information" (Lei et al., 2013, p. 8).

A gap exists in the literature to identify the extent to which school districts have trained staff and students on privacy concerns related to Bring Your Own Device (BYOD) policies as well as clear indications of what constitutes inappropriate use. Also lacking is any clear sense of the variability that may exist, particularly along the lines of marginalized and vulnerable populations. Nor has much research addressed the specific methods of surveillance (ie, for adherence to policy), consequences for any violations of policy, and implications for teachers' careers or students' academic futures. Thus, there is a need for research to understand:

Protocol #: 00038180
Protocol Title: Bring Your Own Devices in Education: Issues of Surveillance of Vulnerable and Marginalized Populations

Research of Schools and Boards at the institutional level:

- How do schools and boards define the security of personal information within a network of BYODs? What are the policies and mechanisms of assurance?
- In what ways do educational institutions conduct surveillance of BYODs for students and teachers?
- How do educational institutions define inappropriate behaviour on BYODs, and what are the potential courses of action and consequences that can be taken, relating to inappropriate use of BYODs?
- How are these policies communicated to teachers and students, and are there explicit accommodations for those in marginalized and vulnerable populations?

Research of teacher and student knowledge and use of BYODs:
- How do students and teachers define inappropriate behaviour on BYODs?
- How do they understand the policies and potential surveillance actions to which they may be subject, at work?
- How do marginalized and vulnerable populations differ in their understandings, compared to those from non-marginalized populations?
- Are marginalized and vulnerable populations at risk for negative career consequences as a result of their poor understandings of surveillance and inappropriate use of BYODs during work?

Protocol #: 00038474
Protocol Title: Bring your own devices in education: Does technology integration cause aging teachers to be more vulnerable?

Research of teacher knowledge and use of technology:
- Does a teacher's sense of professional identity relate to their level of comfort with technology?
- Does a teacher's sense of professional identity affect how a teacher understands and interacts with new mandates related to the use of technology?
- In what ways do teachers feel professionally vulnerable when using technology in the classroom?

Theoretical framework

The development, inclusion of multiple stakeholders as well as the communication of educational policies play an important role in maintaining trust and engagement. Troyna (1994) noted the "minimal inclusion of anti-racist and/or gender-based critiques" (cited by Engel & Burch, 2021, p. 476). As such, Wilkinson et al. (2015) note current trends in educational policy aim "to cultivate new understandings of the relationalities of power and agency within policy formation across vertical and horizontal policy scales, local to global" (as cited by Engel & Burch, 2021, p. 477). Questions related to privilege raise concerns for who has been silent for too long and asks critical questions regarding whose voice is represented and whose has been silenced (ibid). Maguire (2019) believes it is "necessary to fully consider how existing power structures insert and reproduce themselves in equity-oriented policy reforms" (as cited by Engel & Burch, 2021, p. 476).

In their study, Furnell and Phippen (2012) highlight "a tension between the understanding of what a policy is, and what it actually conveys" (p. 12). Furthermore, Fung and Paynter (2008) note, there is a substantial barrier due to "the lack of enforceable privacy rules" (p. 187). Ermakova et al., (2014) observed users resent the "behind the closed doors" processing of their personal data (abstract) and go further to postulate a connection between a perceived understanding of the privacy policy and the accompanying level of trust of the individual. Earp et al., (2005) noted companies tend to "protect the organization from potential privacy lawsuits than address users' privacy concerns" (Ermakova et al., 2014, p.1).

Zero trust and least privilege are concepts used in technology to signal the access and privilege users have differentiated between standard users and super users (Miller, 2021). "Least privilege is the concept and practice of restricting access rights for users, accounts and computing processes to only those resources absolutely required to perform routine, legitimate activities" (ibid). In terms of BYOD, allowing users to access Wi-Fi but not secure and confidential documents contained on the secure network equates to standard use and is considered best practice (ibid). "Least privilege also applies to processes, applications, systems and devices (such as IoT), in that each should have only those permissions required to perform an authorized activity" (Miller, 2021).

From a vulnerability standpoint, teachers and administrators pose a risk to network security and still require access to confidential data, forcing school districts to allow greater access than standard users but without the knowledge normally required of a super user. "When applied to people, least privilege access, sometimes called the principle of least privilege (POLP), means enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role" (Miller, 2021).

A technology of similar sophistication is noted by academics in Sweden as needed to protect confidential and vulnerable data and is used for the detection of malicious code, phishing attempts or distributed denial-of-service (DDoS) attacks (Naarttijarvi, 2018, p. 1020). "Generally speaking though, the type of sensor system discussed here operates by monitoring the attributes of connections to information systems" (ibid, p. 1020). However, monitoring of traffic data is also noted as controversial and "proved to be a contentious issue among regulatory authorities. Less than half believed the technology should be used to monitor data traffic and that it "should be conducted under strict legal conditions" with restrictions (European Union Agency for Network and Information Security (ENISA) as cited by Naarttijarvi, 2018, p. 1020). This coincides with objections from parents, in many cases with law backgrounds, that their child be allowed access to internet and school resources without any identifiable markers or responsibility attached to their given names, many school districts included in this study, insist that students should be tracked for their use.

Methodology

Four school districts agreed to participate and were interviewed in this study. Interviews took place on-site at school board offices, and online through videoconferencing, over the phone and through emails. Triangulation of data was achieved through teacher written response (list of questions), followed by teacher interview, and finally through external review. A case study approach was used to summarize the findings.

There are limitations to the present study. First, it should be acknowledged that the participants in the study were selected based on their technological background, and position within the participating school districts. Second, the sample size is a limitation. Socio-economic status (SES) is a third consideration in this study due to the technology provided to the schools, and the experience with technology students and parents or caregivers had in the home. One final consideration is the potential for participants to formulate responses that the researcher may wish to hear, or that the school district may wish to hear when participating in a research study, such as this.

Data sources, evidence, objects or materials

Table 1. Demographic information collected from study participants

	Case Study # 1	Case Study # 2	Case Study # 3	Case Study # 4
Date	Jan 8.2020-Jan 10.2020	Oct 29.2019	Nov 1. 2019	Dec 13.2019
Location	Vancouver Island, BC	Vancouver Island, BC	Toronto, ON	Vancouver Island, BC
Size	8,000 students	11,300 students	247,000 students	14 700 students
Gender	Female: 1a, 1b, 1c, 1d	Male: 1a, 1b	Female: 1	Male: 1
Position	Teacher : 1a, 1b, 1c, Administrator : 1d	Head of Department : 1a Director (IT): 1b	Administrator : 1	Management (IT): 1

Interview transcripts were reviewed with an open-coding format, which facilitated the consideration of emergent patterns. The information collected set a framework for the literature and guided the direction of themes emerging from previous interviews, ones that aligned with the literature review as well as new ones that had yet to be mentioned. The combination of the data from the four case studies and literature review helped to refine and differentiate categories to explore that seem promising to develop. Axial coding is used to relate emergent patterns found in the case study data with literature review themes. These tables are provided at the end of this paper.

Results

Data collected during the study indicated inappropriate behaviour in schools, from the perspective of participants is anything not assignment related (CS1), without the permission of the teacher (CS3) and during instructional time (CS1; CS3; CS4), or on school Wi-Fi. Consent for taking pictures (CS1), videos (CS1), recording others, disrupting others (CS2), or interacting in a hurtful and harmful way (CS3) was also indicative of inappropriate behaviour. Finally, concerns about the use of phones in class (CS1; CS3; CS4) and the exchange of personal phone numbers (CS1) lead to the perception of cheating with phones on math problems (CS1), or during tests (CS4), and privacy concerns (CS1). As of Nov 2019, the province of Ontario has issued an acceptable use policy to guide school principals in the application of the term in Ontario schools (CS3).

During the study, qualitative data collected indicated surveillance is attributed to five themes: policy (CS2; CS4), security (CS2; CS4), punitive (CS2; CS3), assessment (CS2) and well-being (CS3). FOIPPA compliance (CS2; CS4), intent (CS4), test taking procedures (CS4) and age (CS2) were all sub-categories for the theme of policy. Security considers subcategories such as installing a footprint on a device (CS2), industry wide lists (CS2), blacklists and shares advantages for creating different networks (CS4) for different devices and limiting access based on entry site. Punitive included parent reports (CS3) about teachers, administrative monitoring (CS3), students' behaviour (CS3), investigations (CS2) and a reactive mindset without active monitoring (CS2). Few connections were made between the use of surveillance in schools and learning or assessment of learning (CS2). Similarly, few responses indicated the use of surveillance for measuring wellness in schools (CS3).

Key Findings

1. A person's understanding of the term vulnerable or marginalized dictates their assumptions of how that person might differ in their understanding

For the participants in case study 2, IT staff considered the role of assistive technologies when considering the term vulnerable or marginalized. Due to the remote and isolated community case study 2 represents, the term marginalized was modified to include the term "isolated" (CS2-1b). The school district response was to increase "hands-on" opportunities when possible. The teachers represented in case study 1 considered socio economic status and First People's to be vulnerable or marginalized, in addition to children, teenagers and senior citizens. One teacher believed that a low socioeconomic status (SES) implied a high likelihood "have less exposure to information about digital citizenship and educational use of devices" (CS1-1a). However, the other two teachers did not believe differences existed in understandings because, "in this day and age access is everywhere and usage is growing all the time" (CS1-1b), and "all people are capable of inappropriate use and actions with BYOD" (CS1-1c). The administrator in case study 1 considered English language learners, adults over the age of 50, senior citizens and administrators to be vulnerable or marginalized and believed that students learn what has been modeled to them by their environment (CS1-1d), therefore there are subtle and larger differences in understandings about social contracts. Well-being and in particular suicidal students were considered vulnerable or marginalized by the administrator/parent in case study 3.

2. Understanding is assumed to be an age-related question, a language barrier or reading comprehension limitation instead of potentially a personality trait, a lower level of caring or concern for rules, policies, lack of voice, or lack of engagement

When you ask the question does their understanding differ, you could be asking do you understand that you are checking this box because it is the only way you can go on the internet.
The identification of children, teenagers and senior citizens as vulnerable and marginalized implied that age was a consideration when checking for understanding, "Depends what has been modelled to them in past experiences" (CS1-1d). For one teacher the lack of exposure about digital citizenship and educational use attributed to lower SES was a consideration as well (CS1-1a). The lack of voice in the creation of policies may explain why the administrator/parent in case study 3 remarked that "the kids will never, they don't tell on each other" (CS3) or a lack of concern for rules, "they don't try to conceal it as much, they are often caught by their teacher" (CS3). Personality traits in one case study included the multiple suicide attempts of their students (CS3). Interestingly, two teachers from case study one indicated all people are capable of inappropriate use and actions (CS1-1c) and all people have the same amount of access (CS1-1b). A lack of engagement could be considered a problem for isolated

communities (CS2-1a) as noted by the IT staff in case study two. There is also an indication from administration that teachers' role is to keep students off of inappropriate websites (CS3)

3. The teachers in the study are assumed to conduct the majority of surveillance on a day-to-day basis of students while at school on a device.

The responses in case study 1 of the term inappropriate meaning anything not assignment related or without the permission of the teacher implies that teachers understand they control how devices are used in the classroom. IT Staff represented in case study two also indicated that the majority of monitoring "does actually fall on the teacher and sometimes the parent" (CS2-1a). Further, IT Staff indicated that a teacher can "request" a student have restricted access or blocked (CS2-1a). From an administrator/parent perspective, case study three confirmed "doing what they should be doing" (CS3) surveillance of devices and technology in the classroom is the responsibility of the supervising teacher and can only be done with the permission of the teacher.

4. Teachers conducting surveillance may be unaware of the potential consequences for a student in breech of a technology policy, as it may be outside of their scope to determine punishment or record frequencies of severity or violations.

Two of three teachers from case study 1 indicated they were "unsure" (CS1-1c) or had "no idea" (CS1-1a) if there were consequences for vulnerable and marginalized populations. While the administrator/parent in case study three indicated that a lawyer/parent challenged the school's right to touch her child's cell phone, however in general felt that "most kids will give up their phone and say 'I am sorry'" (CS3)

5. Teachers conducting surveillance may not have a voice in the policy they are asked to enforce, and it is possible teachers and administrators collaborated and engaged as a community in the development of the policy

Different perspectives were observed during the study in relation to the surveillance or collection of data at school. In case study two, IT staff reflected on a challenging situation with a parents' refusal to give consent for their child's name to be used on Google Apps for Education (GAFE) and they expressed confusion on how a teacher could assess a child in this manner effectively, "they want to use a randomized name" (CS2-1a). The administrator/parent in case study three collaborated with her staff and felt strongly connected to the policy at her school, "five years ago, we had an incident with what we as a staff deemed to be inappropriate use of cell phones and social media in schools and we developed a policy" (CS3) "every single staff member and myself it was a completely collaborative effort that lead us to the policy that we have"(CS3) and in creating a policy for her children's cell phone at a different school, "my kids walk to my school every day after school. They have a phone for safety purposes" (CS3). Safety is a key reason for students to have cell phones as a device at school, "many of our students using their phones, or computers log on to their school Wi-Fi through their student accounts" (CS3). For this participant, parents have been asked to sign the electronic device agreement for their child. This approach is mirrored by the IT staff in case study two, "we ask parents to give us consent for their child to access any internet-based resources" (CS2-1b). It also mirrored the approach by IT staff in case study four "appropriate use consent form we send home at the beginning of every school year" (CS4). For case study four participants there is only one procedure for the use of technology and it is district wide, not BYOD or site specific. (CS4). IT staff in case study two worked with their union on a general consent document for the use of "all computing devices" (CS21b) and even for both IT staff participants in case study two and four, some policies are not in their control either "We do reference FOIPPA when it comes to that and sharing that information online" (CS4) and "a FOIPPA compliance perspective, including their personal devices, if they use their personal devices in the classroom" (CS21b). While it might be assumed that it is true in all school districts, participants in case study two acknowledged policies had been approved by the board around the use of information (CS2-1). A quick scan of their policy documents by participants in case study two noted their school district policy does not identify the possibility of accommodations for marginalized or vulnerable populations. "I don't think there are any accommodations for marginalized or vulnerable. I don't think there is anything that we do related to that, I don't know if there is anything the schools do that are related to that"
(CS21b).

6. Engagement in the creation of a policy and an understanding of the events or incidents that lead to its creation may be a key factor in the acceptance, promotion or regulation of the policy

For the participant in case study three, the incident that occurred five years ago is recognized as a pivotal moment for her and her staff in the creation of a policy that they still follow five years later, "we have been under that school policy ever since" (CS3). Due to the collaborative effort of the policy making and shared experience of the incident, each staff member had a voice in the creation of the policy but for new staff members and new families the school ensures they continue to educate and promote their policy through weekly communications. "Goes out to the parents every week. Here is the electronic device policy. Here is what we follow." (CS3). Weekly communication allows parents the opportunity to raise an issue with individual pieces as well, "that is something we engage parents in and 99% of the time parents are on board with that piece as well" (CS3). Teacher acceptance of the policy and regulation can be assessed by administrators through teacher conduct and performance reviews, "if a teacher, you know is walking around the room and doing what they should be doing and checking in with kids to see if they are doing work, it is pretty easy to catch them" (CS3). Student lack of voice and resistance to the policy is also clear through their reaction to each other, "the kids will never, they don't tell on each other" compared to their reaction to their teacher "The teachers, well, from time to time we have had to have conversations with staff around phone use in the school. We have had staff members that have been caught playing video games during instructional time" (CS3). Teacher resistance to policy can include union if escalated by the administration "It has never gotten to a point where we have had to involve the union" (CS3).

7. Life experiences of stakeholders, regardless of role, may be a key factor in the voice of the stakeholder and the acceptance, promotion or regulation of the policy

Just as the life experience of the administrator/parent in case study three is a key factor in her policy creations for her school, other life experiences or stages in a career can be key factors in policy decision making, acceptance, or regulation. For some teachers, decisions related to technology polices can seem black and white, cut and dry, "If at a school, inappropriate is anything not assignment related" (CS1-1a). For other teachers it is related to time of day, "Searching personal interest websites during instructional time" (CS1-1b) and for other teachers it can be completely contextual, "Taking photos of people without consent, videoing without consent, looking up inappropriate topics on internet, gossiping about people within the school community on text/social media" (CS1-1c). Age related decisions also differ across school districts, schools, and hallways, for the administrator in case study one, "At the elementary level students do not BYOD". Or the policy may have a different focus depending on the role of the stakeholder, "For Staff, I think it would be beneficial to have stricter policies about what devices (namely phones) should be used for and when" (CS1-1d). This administrator believes that staff and students both need to be regulated on devices, and this is implied by the administrator/parent in case study three who supports a policy in her school that adults set the example they wish the students to follow, including on devices (CS3). Concerns were also apparent by one administrator that it was important to protect her teachers' privacy by concealing their phone numbers from parents (CS1-1d). The administrators in case study one described additional situations of inappropriate use of a device, "School purposes only, gaming, personal texting or social media use during learning times would not be appropriate" (CS1-1d) and "Elementary students who use devices in math to solve problems for them" (CS1-1d).

In case study three, the administrator/parent implied a teacher is accountable for the students use of technology, stating their policy stipulates "any device that is brought into this school, it is the expectation that you use that device under a teacher's direction for an educational purpose" (CS3). However, she holds students accountable as well. When students in case study three's school "pay penance" for violating school polices the are asked to work on presentations on learning skills for younger children, "You know why, it was just boys being silly but same thing, what we did was, there was nine boys involved and we grouped into groups of three and they were all grade eights, they worked with our grade six boys around presentations on learning skills, so responsibility, organization, initiative, self-regulation, that kind of work and collaboration, and they did lessons for the younger children in the building, around learning skills and they were paying penance for what they had done" (CS3).

From a technology perspective, the IT staff in case study two and four view creation of policies differently. Mainly from a security view, inappropriate behaviour is "hacking the system if it is accessing sites that are inappropriate, if its disruptive in anyway" (CS2-1a). Since IT staff are not engaged in active monitoring (CS2) they are responsible for creating firewalls to block identified sites (CS2; CS4) that are classified as inappropriate and for changing

settings on student or staff accounts to implement restrictions. "But to be clear, though, it is not an active monitoring where we go in and look for incidences, it is more reactive in that if we have an incident than we go back in and do an investigation" (CS2). In case study four the IT staff/parent participant also felt that inappropriate might include examples from his children's experiences, such as taking pictures or recordings and putting a phone away during a test (CS4). He felt sympathy for teachers' surveillance of cell phones, stating, "texting, tough to police" (CS4).

Both IT staff mentioned compliance with FOIPPA (CS2; CS4) however parent concerns are a challenge for IT staff in some situations. "Parents are concerned that data can be linked used in the future digital presence rest of their life" (CS2-1a). In response to parent concerns, the IT staff in case study two prepared documents to provide parents with more information to help achieve an informed consent, "so Google has a policy on how they treat student data many of these software companies have those kind of policies so I have kind of put together a list of all of those that we will send a parent if they ask, say they want to find out more about how their child's privacy is protected, that type of stuff" (CS2-1a). As a parent, the IT staff in case study four did not seem surprised that about restrictions for use of cell phones in school, "you know I have another kid who has been told during a test to put the phone away" (CS4).

Sometimes administrators have parents report a teacher and they contact IT staff, "Often with teachers it comes through a parent, their kid has had a concern and gone home to their parent and said, you know, my teacher is playing video games in class" (CS3). Other times, a parent challenges the administrator, "I have one parent who is a lawyer, who clearly, she really didn't have any ground to stand on but she was a parent that challenged me and this was four years ago. She said that phone is my property, I paid for that phone therefore you don't have a right to look on that phone" (CS3). The life experiences of the administrator and in the case of case study three parent, their personal philosophy may be closely aligned with school policies, "he doesn't have the opportunity. I track him on his iPod as he walks from school and that is about it" (CS3).
For students in the school, it may be difficult to have a voice in policy, "most kids will give up their phone and show you" (CS3) and it may depend on the life experiences of their home, "she was the only parent in being five years at this particular school, the only parent that has ever challenged that" (CS3).

8. Acceptable use of personal devices on schools may not be uniquely identified and may fall under general considerations of a larger district acceptable use policy

Depending on the school district, a policy that regulates the type of devices a student is allowed to bring in may exist, and an acceptable use policy for computer devices may exist, but an acceptable use policy for student personal devices may not, "So, I will say it isn't well defined right now and we actually are working on an administrative procedure on BYOD so what we do have right now is one procedure that has to do with the use of technology in the district, right" (CS4). Both case studies with IT staff participants echoed the same response, "What we have is for the use of all communication devices, we essentially have a procedure that we put in place, that let's them know that anything and everything on their computer can and will be monitored if required. It is not specific to BYOD but it is just general use of all computing devices" (CS2). Having a district wide acceptable use policy is strategic for IT staff "Especially from a FOIPPA compliance perspective, including their personal devices, if they use their personal devices in the classroom" (CS2). However, there exists some contextual considerations for access to websites "It is teacher by teacher based, what we are seeing is that middle schools tend to be clamping down a little bit more and trying to block the access. High schools, we haven't had any real issues there, elementary they want more access, so it sort of a range, right?" (CS2). When IT staff are asked about the role they play in surveillance, one school district attributed a portion of their work to reviewing apps that teachers and students could use "trying to find that fine line between where the tool is actually useful and it is contributing to the learning versus situations where it is inappropriate or distracting from the learning process" (CS2-1a).

9. Personal devices may be restricted in accessing shared folders, shared drives, and district information stored locally and may only access the internet and may only use a separate network Wi-Fi connection

Personal devices brought to the school and connected to the school wireless fidelity (Wi-Fi) are subject to monitoring of those devices…" (CS2-1b). From a security perspective, personal devices are also kept apart from district owned devices through the use of separate networks for accessing the internet. "Yes, it is for security, because we don't trust those devices, we don't control them, we don't trust them." (CS2-1b). The concern for this

school being the potential for malware or malicious files downloading or uploading to district resources through the internet connection (CS2-1b). IT staff have in both case studies "isolated to a separate network from the main devices" (CS2-1a); and "no intent on giving them access to files on district, or district files rather, just letting their device connect to the World Wide Web" (CS4). Regardless of which network, "We do have, I will say filters, on our staff or on our BYOD and those are, there are just certain websites that are blocked right. and you can't access them right and that is for everyone, the students and the staff right, we don't want them accessing certain sites right?" (CS4).

10. Industry wide blacklists, malware, malicious and blocked sites may be used by IT staff in school districts to set standards of which websites can be accessed

Both IT staff participants in case study two and case study four have a list of identified websites that are blocked, "we block so porn sites are blocked, malicious sites, malware sites are all blocked" (CS2). One school district mentioned the use of filters, "there are just certain websites that are blocked right. and you can't access them right and that is for everyone" (CS4). While the other school district identified an industry standard, "We use Palo Alto Networks firewalls and they have lists of sites that are inappropriate that we block" (CS2).

11. Cell phone use at school, in particular: during tests; taking pictures; video recordings; accessing social media and texting raised concerns for IT staff, parents, students, administrators and teachers

For some school districts, the grade level dictates policy, "At the elementary level students do not BYOD" (CS1-1d). "I mean there is somebody has a device in secondary school, almost every single student does nowadays, right" (CS4). However, administrators have commented on the policy related to the use of cell phones for students and teachers. "For Staff, I think it would be beneficial to have stricter policies about what devices (namely phones) should be used for and when" (CS1-1d). The inappropriate use of a cell phone combined with social media lead to policy change for one participant "five years ago we had an incident, with what we as a staff deemed to be inappropriate use of cell phones and social media in schools and we developed a school policy and we have been under that school policy ever since" (CS3). While also noting that the use of personal devices on school grounds has legal implications, "I have one parent who is a lawyer, who clearly, she really didn't have any ground to stand on but she was a parent that challenged me and this was four years ago. She said that phone is my property, I paid for that phone therefore you don't have a right to look on that phone" (CS3). "Kids are very trusting. You know most kids will give up their phone and say, "I am sorry I was doing this". You know there is that automatic feeling of guilt because they don't want to disappoint us, right?" (CS3).

There are so many violations of the cell phone policy that a school jail may be used in the office for offenders, "I have some students that have violated our own school policy and they have a little phone jail in the office where they walk into school every day and they don't get to have their phone. They have lost privilege for, sometimes for an indeterminant amount of time" (CS3). When dealing with staff members about inappropriate cell phone use, the conversation can go a bit differently but is still a concern, "The teachers, well, from time to time we have had to have conversations with staff around phone use in the school. We have had staff members that have been caught playing video games during instructional time. It has never gotten to a point where we have had to involve the union" (CS3). From both an IT perspective and parent, the participant in case study four concerns about cell phone use are seen as used for cheating, "you know I have another kid who has been told during a test to put the phone away" or for privacy related violations, "in terms of filming, I do know that our schools view for my students that taking a photo, taking a video of somebody without their knowledge is not allowed or frowned upon" (CS4).

12. Loss of membership is one of the first consequences requested by teachers, and administrators when a technology policy is broken

Both IT staff participants in case study two and case study four acknowledged that possible consequences "would be the removal of the service or the additional blocking of specific sites that are causing the child to be distracted or…" (CS2) or a complete loss of privileges, "an extreme is they lose their privileges not able to connect with their credentials" (CS4). The misuse of an educational tool can also result in a loss of membership, "we have blocked individual students if warranted, like if they are misusing their access or they are using, like I think and so like somebody was on GAFE (Google Apps for Education) and writing stuff and sharing inappropriate documents and

stuff so as a temporary measure we will kind of block access for a period that is deemed appropriate by the principal, or the parent, or whatever they come up with" (CS2).

13. Privacy Impact Assessments (PIA) may only be completed by IT staff for Apps hosted on US servers and not for all personally stored information stored on the district server

The use of privacy impact assessments (PIA) were identified by IT staff in case study two "We have over 200 different apps that are used by teachers in the district, we did inventory, so for a lot of them we do have privacy impact assessments in place, but for a lot, teachers may just choose an app because they saw it somewhere and they liked it, or they came across it from another teacher. That is an area we struggle with, is how do we manage, how do we ensure that we have the right privacy controls in place" (CS2-1a). The concern for school districts, and in particular IT staff is what data is being uploaded, "If a service wants to get a list of all of the students and their names and their email addresses and things then we do have to do a privacy assessment. So when we are uploading data we definitely do it." (CS2-1b). Over the past five years in the province of British Columbia, IT staff have been implementing provincial policies related to data storage and retention, "It is a provincial, it has only been in the past 3 or 4 years, that it has really been an issue as cloud computing became more prevalent. It kind of started with Google Apps for Education and went on from there, office 365" (CS2-1b). The lack of control has caused some IT staff to feel uneasy, "a few years ago organizations including school districts were in control, well had a lot more control over where their data was located because it is actually located physically within their own data centre" (CS2). The use of Google and Google Apps for education by many school districts has also lead to changes in policy, "Google has a policy on how they treat student data many of these software companies have those kind of policies so I have kind of put together a list of all of those that we will send a parent if they ask, say they want to find out more about how their child's privacy is protected, that type of stuff." (CS2-1a). Plans to include policy statements related to privacy were discussed with IT staff in case study four, "We do reference FOIPPA when it comes to that and sharing that information online is not encouraged, for sure. So that could be addressed in BYOD procedure as well" (CS4).

14. IT staff and consequentially school districts may be unsure of their application of privacy matters for the electronic storage of, or access to, personally identifiable information

Since the shift in control some school districts are struggling with their application of privacy matters, "That is an area we struggle with, is how do we manage, how do we ensure that we have the right privacy controls in place" (CS2). Everything now is on the cloud, right." (CS2). Parents have requested greater privacy controls in some cases, "we have a parent that will not give us consent to allow their child to be on GAFE using their regular name. They want to use a randomized name like island life or something like that which encloses its own sort of issues like how do the teacher or students know who that student is" (CS2). Both school districts rely on FOIPPA for guidance in privacy matters and sharing information (CS2; CS4).

15. Acceptable use may simply refer to accessing websites based on the separate network connection for BYOD, but not include websites that are already on a blacklist provided by an Industry wide acceptance and use (i.e. Palo Alto)

The focus on an industry wide block list, "we use Palo Alto Networks firewalls and they have lists of sites that are inappropriate that we block so porn sites are blocked, malicious sites, malware sites are all blocked" (CS2). Parents are also asked to give consent "for their students to access any internet-based resources" (CS2). However, IT staff are quick to point out their investigations are reactionary and triggered by accessed websites, "We don't monitor emails so we do monitor all websites accessed, and we monitor all basic traffic on the firewalls, right, so sites they are going to on firewall." (CS2-1b) or a filter, "and that is for everyone" (CS4).

Discussion

Electronic health records were digitized in Canada for the first time in 2012 and in doing so raised the question of ownership and rights to patient data (Aïmeur & Lafond, 2013). While academics may have questioned the security of electronic health records (EHRs), privacy analysts perceived the problem of access from a different perspective. "It is important to ensure that EHRs are used in a way that the integrity of personal information is

preserved and that patients have control and access to their records" (Aïmeur & Lafond, 2013, p. 822). A point that was firmly driven home 4 years later in British Columbia by privacy commissioner, Elizabeth Denham's reaction to whistleblower Tim Duncan's allegations that he was told to delete patient emails requesting access to their medical files by Ministry officials (Britten, 2016). Many school districts insist that Privacy Impact Assessment (PIA) are completed for 3rd party websites and the storage of student information, but often neglect to note which visitors or staff have accessed confidential student information and neglect to consider the ramifications of a visitor walking off site with a printed copy of student confidential information including, name, class, diagnosis, treatment, schedule, contacts, etc.

Considerations about medical conditions, mental or behavioural disorders are also a growing concern, as information related to and the documentation of behaviour is recorded in schools. The inclusion of tracking therefore creates an accountability on behalf of the school district to monitor and address the well-being of students, such as anger, depression, and other emotions displayed and tracked online. A focus on well-being instead of punitive forces the school district to be accountable for identifying emotional regulation from an early age and could present a liability if parents were not notified immediately when a pattern occurs or is recognized. The ability of the IT department to recognize patterns of behaviour from a well-being perspective needs to be addressed, as well as protocols for ensuring the child is not perceived as threatening but in need of their help.

Until such regulations are in place the danger posed to users related to loss of privacy is a consideration and potential liability for school districts. As it stands, the ability of data to remain forever on the Internet allows for legal cases to consider what was missed to a degree of accuracy beyond the resources currently available to school districts and individual IT departments. Additionally, teachers are invited to complete psych evaluations on students which asks the teacher to inform the doctor of typical observed behaviours. Often a teacher is supplied with a diagnosis but may be ill-equipped to identify behaviours or to react in a manner that supports the students well-being.

A study published in China highlighted concerns raised in Iran related to the barriers related to recognizing child injuries in an online reporting system. "Barriers were categorized in three main categories and nine subcategories. (…) poor data capture and usage (data collection, data recording, and data dissemination) and resource limitation (human and financial resources) (Azadi et al., 2019, p.229). Similar to educational settings a lack of resources can contribute to poor delivery of information to all stakeholders.

Scientific or scholarly significance of the study or work

The scholarly significance of this work is the identified need for privacy impact assessments to be considered on a grander scale in education, in addition to the accessibility rights of students and their parents to information stored. The digitization of medical records combined with advancements in natural language processing enable deep learning in the areas of public health and specifically in the field of epidemiology (Cossin & Thiébaut, 2020). Internationally, Europeans emerged in front of Canadians in the area of human rights and managing privacy and personal data through the creation of the General Data Protection Regulation (Bonatti et al., 2018, abstract).

REFERENCES

Aimeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust- An experimental study. *Computers in Human Behavior, 58*, 368-379.

American Psychiatric Association, & American Psychiatric Association. (2013). Diagnostic and statistical manual of mental disorders: DSM-5. *Arlington, VA*.

American Psychological Association. Zero Tolerance Task Force.(2008). *Are zero tolerance policies effective in the schools? An evidentiary review and recommendations*.

Azadi, T., Khorasani-Zavareh, D., & Sadoughi, F., (2019). Barriers and facilitators of implementing child injury surveillance system. Chinese Journal of Traumatology.

Bonatti, P. A., Bos, B. , Decker, S. Fernandez, J.D. , Kirrane, S., Peristeras, V., Polleres, A., Wenning, R. (2018) Data Privacy Vocabularies and Controls: Semantic Web for Transparency and Privacy. In: *Semantic Web for Social Good (SWSG2018)*, 8-12 October 2018, Monterey, USA.

Breslow, J. (2018). Moderating the 'worst of humanity': sexuality, witnessing, and the digital life of coloniality. *Porn Studies*, *5*(3), 225-240.

Cossin, S., & Thiébaut, R. (2020). Public Health and Epidemiology Informatics: Recent Research Trends Moving toward Public Health Data Science. *Yearbook of Medical Informatics*, *29*(01), 231-234.

Cripps, H., Standing, C., Prijatelj (2011). The Implementation of Electronic Health Records: A Two Country Comparison (Australian and Slovenia)

Deutsch, E., Duftschmid, G., & Dorda, W. (2010). Critical areas of national electronic health record programs—Is our focus correct?. *International journal of medical informatics*, *79*(3), 211-222.

Earp, J.B., Antón, A.I., Aiman-Smith, L., Stufflebeam, W.H. (2005). Examining Internet privacy policies within the context of user privacy values. IEEE Trans. Eng. Manag. 52 (2), 227–237.

Engel, L., & Burch, P. (2021). Policy Sociology in the Contemporary Global Era: Continued Importance and Pressing Methodological Considerations. *Educational Researcher*, 0013189X211009184.

Fuller, K. (2019). "That would be my red line": an analysis of headteachers' resistance of neoliberal education reforms, *Educational Review, 71*(1), 31-50.

Fung, M. Paynter, J. (2008) The Impact of Information Technology in Health Care Privacy, Ethical, Legal and Social Issues in Medical Informatics, pp. 186-227

Furnell, S., & Phippen, A. (2012). Online privacy: a matter of policy? *Computer Fraud & Security, 2012*(8), 12e18.

Huth, C.L., (2013).The insider threat and employee privacy: An overview of recent case law. *Computer Law & Security Review, 29*, 368-381.

Lei, J., Sockolow, P., Guan, P., Meng, Q., & Zhang, J. (2013). A Comparison of electronic health records at two major Peking University Hospitals in China to United States meaningful use objectives, BMC Medical Informatics and Decision Making 13(96).

Maguire, M. (2019). Equality and justice in education policy. *Journal of Education Policy*, *34*(3), 299-301.

Miller, 2021. What is Least Privilege and Why do you Need it? (Retrieved from https://www.beyondtrust.com/blog/entry/what-is-least-privilege

Munteanu C., Sadownik S. (2019). Field Studies of Interactive Technologies for Marginalized Users: A Canadian Ethics Policy Perspective. In: Neves B., Vetere F. (eds) Ageing and Digital Technology. Springer, Singapore

Naarttijärvi, M. (2018). Balancing data protection and privacy–The case of information security sensor systems. *Computer law & security review*, *34*(5), 1019-1038.

Perez, L. M., Jones, J., Englert, D. R., & Sachau, D. (2010). Secondary traumatic stress and burnout among law enforcement investigators exposed to disturbing media images. *Journal of Police and Criminal Psychology*, *25*(2), 113-124.

Sadownik, S., Munteanu, C., & Xu, Z. (2016, November). Ethical dilemmas during field studies of emerging and disruptive technologies – is our current state of knowledge adequate? A knowledge Synthesis Report for the Social Sciences and Humanities Research Council of Canada (SSHRC). http://www.cs.utoronto.ca/~mcosmin/share/sshrc-ethics/Munteanu_EthicsEmergingTech_CompleteReport_2016-SSHRC-KS.pdf

Troyna, B. (1994). Critical social research and education policy. *British Journal of Educational Studies*, *42*(1), 70-84.

Wilkinson, M. N., Thomas, M. A., Heyman, C., Bartlett, L., Godbole, P., Hodge, S., ... & Vavrus, F. (2015). Capturing Quality, Equity & Sustainability: An Actionable Vision with Powerful Indicators for a Broad and Bold Education Agenda Post-2015. *Open Society Foundations*.

Wortley R, Smallbone S (2006) Child pornography on the internet. Office of Community Oriented Policing Services, Washington, DC