Toxic Environment or Conflict of Interest- Issues of Surveillance in Education

Dr. Stephanie A Sadownik [1]

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

Abstract

The current study addresses ethical considerations in education and the frameworks that regulate human computer interactions of vulnerable and marginalized groups with emerging and disruptive technologies. Data collected presents evidence from technology staff of emerging issues and considerations related to privacy policies. Theoretically the paper is positioned at the intersection between leadership monitoring of toxic work environments and technology and workplace related privacy considerations. The results of the study indicate teachers, administrators and technology staff do not claim to be experts in privacy policy. Considerations for conflict of interests, benefits from disclosure and the potential for unprecedented reactions to both surveillance and awareness of surveillance within a school potentially point to an increase in lockdown measures or mass school shootings.

Keywords: *Leadership; Ethics; Emotional Regulation; Organizational Change*

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

"The totalitarianism of dictated education policy, surveillance and punitive accountability destroys the soul"- Fuller (2019)

Introduction

The objectives of this current study are to address ethical considerations for surveillance in education and the educational policy frameworks that regulate human computer interactions of vulnerable and marginalized groups with emerging and disruptive technologies for both punitive and well-being measures. For the purposes of this paper, a toxic environment is defined and created when two or more people conspire against or discuss an individual in the same environment. Personal communication is defined in this paper as the use of school electronic resources (i.e. Internet, email, devices, storage). Current educational trends in Canada regarding decentering whiteness (Carter Andrews et al., 2021) and decolonization in addition to teaching tolerance (Graves & Orvidas, 2015) support the provision of safe spaces for students experiencing trauma to speak (Wiest-Stevenson & Lee, 2016) and for Caucasian students to ask questions that may be offensive as they struggle to understand their privilege and the importance of equity without experiencing guilt (Lensmire, 2011) for transgressions they are not responsible for nor participated in. It attempts to provide a broad picture inclusive of curriculum about Nazi Germany, Black Slavery, and missing Indigenous women or unmarked graves of residential schools, and the representations of knowledge in textbooks or other data resources available to them. It is important for all children to feel pride in who they are, their unique family structures and cultures as they move forward.

If student voices are provided safe spaces to speak about trauma in schools and agency to choose the space, students may choose to express themselves through trans life writing (Vipond, 2019) and displaying emotions during mathematics (i.e. anxiety, frustration) in journals (Sadownik, 2017) or use school electronic resources such as the Internet (i.e. social media, chat) to communicate, develop and share thinking (Sadownik, 2015a; 2015b; 2018); hate (Samaras, 2013) or to receive help regulating problematic use of the Internet (Gómez et al., 2017). However, current educational policies may be ill prepared for hate or emotion filled communication, sexual expression, or questions about gender identity and policy may challenge schools to consider this communication in a negative context (Doblanko, 2021) or as risk taking (Gómez et al., 2017) or manipulating the relationship (Mellor et al., 2013). The dichotomy of online disclosures of sexuality have been noted (Henry, 2009). "The benefits of online self-disclosures are inherently linked to the risks of that same behaviour, namely a loss of privacy" (Moll et al., 2017, p. 484). The abundance of information has afforded some students protection from Information Technology (IT) departments who do not have the resources to conduct active monitoring of all members, or whose strict guidelines of use may suggest to students it is safer to use social networking at home in place of school (ibid).

Surveillance of electronic resources in schools challenges many IT departments, administrations and teachers who may consider an insider threat model, to mean finding and exposing negativity instead of a way of controlling the leaking of documents to outsiders and controlling the communication of trade secrets or espionage (Huth, 2013) as justification for reviewing private communication and monitoring school climate. Studies from China indicate students may share privacy concerns about expressing negativity online and act in a way to mediate these concerns. Keng and Liao (2013) suggest "users with anxiety are more inclined to use different social media platforms to alleviate their negative emotion" (as cited in Teng et al., 2021, p. 2).

Although punitive monitoring of private online communication in the workplace is not encouraged by Courts in the United States (Huth, 2013) or the Criminal Code in Canada (Section 319(2) C-46) which stipulates private communication is viewed differently than public; vulnerable and marginalized populations may not feel encouraged to have voice or agency in schools about lived experiences, sexuality, gender or difficulties with mental well-being in the forms of emotion dysregulation, or specifically a Disruptive Mood Dysregulation Disorder (DMDD) as noted in the American Psychiatric Association (APA) Diagnostic and Statistical Manual of Mental Disorders (DSM-5). "Education policy changes in different environments have aimed to cultivate new understandings of the relationalities of power and agency within policy formation across vertical and horizontal policy scales, local to global" (Wilkinson et al., 2015 as cited by Engel & Burch, 2021, p. 477). "Managing privacy and understanding the handling of personal data has turned into a fundamental right- at least for Europeans- since May 25th with the coming into force of the General Data Protection Regulation (GDPR)" (Bonatti et al., 2018, abstract). Proposed

legislative changes suggested in Bill C-36 (Doblanko, 2021) may also impact the use of the Internet and hate messages on school electronic resources.

In this paper, I suggest the current surveillance model may be responsible for the increase in mass school shootings as students and staff feel monitored and misunderstood. The awareness of staff of a student who is noted as a threat can exacerbate a situation when teachers are not trained on surveillance and possibly hold unrealistic expectations of reactions or are unaware of the hypervigilance of students who are labelled as at-risk, and hypervigilance is noted as typical of vulnerable populations lived experienced with trauma (Dooley, 1996; Goeke, 2017; Menees & Segrin, 2000; Mucowski, 1991; Paccione-Dyszlewski, 1992; Sternthall, 1988; Thompson & Calkins, 1996). Systemic and systematic abuse often is cited as the cause for catching the child that is being bullied based on their inability to control their reaction to repeated and undisciplined abuse (Milne, 2016). As such this study seeks to answer the following questions:

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

This research involved interviews with school board administrators and instructional technology leaders, in addition to analysis of Bring Your Own Devices (BYOD) in Education policy documents and legal expectations for appropriate use (Hills, 2018; MacKenzie, 2016; Maxwell, 2018). Previous research conducted on the use of BYOD for teacher and student laptops and mobile phones, teacher professional development with BYOD and the potential surveillance of teachers and students while on these personal devices on school property was also reviewed (Berg, 2015; Fuller, 2019; Goodyear et al., 2019; Hope, 2016; Monahan, 2006; Page, 2017; Perry-Hazan & Brinhack, 2018; Taylor, 2013)

Beginning in 2014, studies began to emerge considering how student owned devices could be used in the classroom. This initial consideration looked at the potential use of cellphones (Bruder, 2014; Imazeki, 2014) and the associated risks (Bruder, 2014). In 2015, a focus on university students (Pagram et al., 2015; Van Wingerden et al., 2015) became of interest and parental engagement (Kiger & Herro, 2015). Once again, security issues were also considered (Olalere et al., 2015). In 2016, two years after the initial onset of BYOD research, academics were focused on secondary students (Adhikari, & Parsons, 2016) and primary students (McLean, 2016), risks to health (Merga, 2016) and academic rigour (Dawson, 2016). Flipped classrooms (Hung, 2017), motivation (Castillo-Manzano et al., 2017; Hopkins et al., 2017; Laxman, & Holt, 2017) and distractions (Kay et al., 2017) were introduced in 2017 while parent engagement was revisited (Chan et al., 2017). Adding apps to BYOD appeared in 2018 (Song, & Wen, 2018) and finally teachers' experiences with 'always on' became of interest in 2019 (Murray et al., 2019).

The collection of data and the protection of privacy has been heralded by human rights agencies and government watchdogs that support court rulings in Canada, however as of 2020 academics have noted potential human rights violations that may have gone undetected (Agrawal, 2021; Joly & Wheaton 2020; Lamarche, 2020; McBride et al., 2020; Mykhalovskiy et al., 2020; Robertson, et al., 2020; Tisdale & Symenuk, 2020; Torelli, 2020; World Health Organization, 2020). Naarttijarvi (2018) an academic in Sweden notes obligations exist for government states to oblige human rights of users from whom the data is collected, and tasks states to "both act and to refrain from acting" (ibid, p. 1020). Moral education parallels this dilemma between power imbalances that may co-exist within schools that represent multicultural populations by asking authorities to be accepting of various perspectives (Umpleby, 2012). "As such, they are legally precluded from monitoring private communications if doing so would violate their obligation to protect privacy under article 8 of the Convention or article 7 or 8 of the Charter" (ibid, p. 1020). Naarttijarvi (2018) further differentiates expectations for government implementation are different from private enterprises. "Signatory states to the European Convention on Human Rights ('ECHR', "the Convention') as well as member states of the European Union subject to the EU Charter of Fundamental Rights ('the Charter') are required to uphold the fundamental rights enshrined in those legal instruments" (p. 1020). Which raises the question of whether schools and their staff are considered private enterprises by the Court or investigative arms of the government.

Recent NDP proposed legislation in Canada would afford private companies in British Columbia the collection, use, and disclosure of information without consent where a reasonable person would agree that the information is required for an investigation or prevention of fraud or criminal activity and this has raised concerns in Canada from government watchdogs in a similar manner. "This process corresponds to a well-known phenomenon in privacy studies- function creep, which describes a measure installed for one purpose that is then applied to other purposes" (Bennett & Raab, 2006, p. 177 as cited by Perry-Hazan & Birnhack, 2018, p.49). "The GDPR requires that both consent and data processing are tied to a concrete purpose and processing data for other than this purpose is unlawful" (Bonatti, et al., 2018, p.2). Both Meghan McDermott, Civil Liberties Association policy director and B.C.'s Freedom of Information and Privacy Association (FIPA) executive director Jason Woywada believe this would blur lines, is an erosion of privacy and sets a dangerous precedent for unspecified investigations.

For the purposes of this paper countries identified by the World Health Organization eHealth survey conducted in 2006 were considered as key players in the protection of both human rights and the online storage of personal and confidential data of electronic health records as a guideline for considerations for privacy protection and human rights in school settings for vulnerable and marginalized populations. Educational records are considered to be more confidential than health or financial records. "As of 2006, there were 112 countries participating in the World Health Organization eHealth survey (…) at that time, five countries were approaching universal adoption of EHRs – Australia, Denmark, the Netherlands, Norway and New Zealand. Three countries – United States (US), United Kingdom, and Germany – had made substantial progress; Japan and Canada had begun implementation efforts" (Jha & Blumenthal, 2008 as cited by Lei et al. 2013, p. 2). With two countries noted as vigilant in their protection of human rights "The issue of privacy and security seems to be of greater issue in the United States of America (USA) and Australia (…) Denmark and England have a far higher level of adoption than those in Australia and the USA" (Cripps et al., 2011, p. 132).

Challenges that arose in the adoption of eHealth platforms and the sharing of data were noted in a comparison study between Australia and Slovenia and are also used as a guideline of where potential problems (politics, perceived costs, and staff) may occur in the education sector.

"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). Of further interest may be the legal liability for schools to monitor communication from a well-being perspective and to act with a well-being focus "Warnick warned that electronic surveillance, which can preserve the past, signals neither forgiveness nor forgetfulness" (Perry-Hazan & Birnhack, 2018, p.49). From a punitive lens, the use of surveillance has not corrected behaviour. "Despite the increased removal of misbehaving students from schools, there has been little evidence to suggest zero-tolerance policies deter students from engaging in future misbehavior" (Tobin et al., 1996 as cited by Goldstein et al., 2019, p. 62).

"The dominance of surveillance practices is typically associated with zero-tolerance policies, which include the frequent use of punitive sanctions and discipline codes, leaving educators little discretion in tailoring responses to particular incidents" (Kupchik, 2010; Taylor, 2013 as cited by Perry-Hazan & Birnhack, 2018, p.48); and for which I suggest are responsible for an increase in mass school shootings, noting the negative consequences present for an individual after only one report. "Beyond the failure of zero-tolerance policies to fulfill their intended roles as deterrence mechanisms (American Psychological Association Zero Tolerance Task Force, 2008) suspended, expelled, and arrested students often experience negative academic, social and well-being outcomes" (Raffaele-Mendez, 2003; Skiba et al., 2002 as cited by Goldstein et al., 2019, p. 62). The use of this surveillance in schools as a punitive measure to control communication on devices (Berg, 2015; Fuller, 2019; Goodyear et al., 2019; Hope, 2016; Monahan, 2006; Page, 2017; Perry-Hazan & Brinhack, 2018; Taylor, 2013) or on the Internet and in some cases to assess children and staff emails as potential insider threats for hate speech and racism under zero tolerance has created an environment that is considerably more dangerous.

Methodology

Research and data collection began in 2019, with four Canadian School Districts (located in British Columbia (BC) and Ontario (ON)) agreeing to participate in person and online. Coronavirus disease 2019 protocols for Face-to-Face contact were followed and noted in this study, with the additional complexity of Ontario teachers and administrators engaged in Work-to-rule job action which has yet to be resolved as of the date of publication. 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

During the study, qualitative data collected indicated surveillance is attributed to five themes: policy (Case Study 2 (CS2); Case Study 4 (CS4), security (CS2; CS4), punitive (CS2; Case Study 3 (CS3), assessment (CS2) and well-being (CS3). Freedom of Information and Protection of Privacy Act (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).

In Case Study 3 (CS3), 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).

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 (CS2), IT staff considered the role of assistive technologies when considering the term vulnerable or marginalized. Due to the remote and isolated community CS2 represents, the term marginalized was modified to include the term "isolated" (Case Study 2, Participant B (CS2-1b). The school district response was to increase "hands-on" opportunities when possible. The teachers represented in Case Study 1 (CS1) 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" (Case Study 1, Participant A (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 CS1 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 (on inappropriate websites) by their teacher" (CS3). There is an indication from administration "if they are doing their job" that a teachers' role is to keep students off of inappropriate websites while at school (CS3) and that schools do not wish to learn about their students through monitoring their agency and voice on websites not considered appropriate for school electronic resources.

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 in school assignments could be considered a problem for isolated communities (CS2-1a) as noted by the IT staff in case study two.

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 maybe 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 wireless fidelity (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 Google Apps for Education (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 Freedom of Information and Protection of Privacy Act (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

School staff in Canada are tasked with increasing surveillance demands and obligations, including the new provision for Ontario College of Teachers to attain qualifications from the Canadian Child Protection Services agency and the badge of honour for that qualification that is to be displayed as "achieved" or "pending" on their teaching qualifications and public registrar as of Jan 3, 2022 (retrieved from https://oct.ca/becoming-a-teacher/requirements/sexual-abuse-prevention-program).

Transformative Reciprocity

Jameson, Clayton, & Jaeger (2010) describe transformative reciprocity as "a deep, thick collaboration that holds the possibility for all stakeholders to be transformed by the partnership" (Stanlick and Sell, 2016, p. 80). The general acceptance by the world population for government surveillance is the assumption that surveillance is a benefit to the population and this is echoed by Bennett (2001) as acceptance of surveillance is due to **"**the assumption that a certain level of monitoring online and offline is in the individual's interests" (p.201). Aimeur, Lawani & Dalkir (2016) believe transformative reciprocity in the form of developing trust between users and those conducting surveillance may be achieved under certain conditions, "giving users control of their data coupled with caring about their interests" (abstract). The private and personal information of educational records which may include custody arrangements and individual education plans is compounded by the inclusion of both academic records and medical information in addition to personal identifiers, which Phelps et al. (2000) notes as sensitive (Nam, 2019, p.533).

Training

The compounding tasks of surveillance that are requested of teachers (in loco parentis) in Canada have grown to include considerations for sexual abuse, child grooming, and neglect while also monitoring for hate messages, emotional regulation, inappropriate websites and general off task behavior. Current trends that aim to decenter whiteness and teach tolerance to remove privilege and classist approaches in schools seek to honour the trauma marginalized and vulnerable populations have endured. Training for both teachers and IT staff must consider not only the methods of data collection and monitoring, legalities of inappropriate sites and language but the position and upbringing of those who are conducting surveillance.

Sexual health is of particular interest as schools endeavour to correct language for Lesbian, Gay, Bisexual, Transgender, Queer, Two-Spirit (LGBTQ2), (the acronym used by the Government of Canada to refer to the Canadian community (retrieved from https://women-gender-equality.canada.ca/en/free-to-be-me/lgbtq2-glossary.html) students, to provide guidance and appropriate language, and to identify abuse. Literature reviews on this topic considered the role of bias and presented inadequate training for medical professionals (Mellor, Greenfield, Dowswell, Sheppard, Quinn & McManus, 2013) and mental health provider bias (Herbitter, Vaughan & Pantalone, 2021) "against the less recognized groups who may be marginalized due to their sexual identities or sexual and relationship practices" (abstract).

Scientific or scholarly significance of the study or work

A gap exists in the literature to identify the extent to which school districts have trained staff and students on privacy concerns related to BYOD policies as well as clear indications of what constitutes inappropriate use. While staff and students may have signed a form acknowledging they are expected to adhere to responsible use of technology, it remains the responsibility of the school district to ensure compliance. This may be viewed ethically as a conflict of interest, if school districts believe this admonishes their accountability for the collection of personal data or the surveillance of BYOD. 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.

The results of the study indicate teachers, administrators and technology staff do not claim to be experts in privacy policy and identify struggles and challenges in implementing policy mandates. Considerations for conflict of interests, benefits from disclosure and the potential for unprecedented reactions to both surveillance and awareness of surveillance within a school potentially point to an increase in lockdown measures or mass school shootings. The scholarly significance of this study points to potential logical fallacies connected to surveillance in education while identifying the tendency to lean towards a punitive focus on surveillance in educational organizations and the potential for change towards a well-being lens.

REFERENCES

Adhikari, J., & Parsons, D. (2016). Bring your own device to secondary school: The perceptions of teachers, students and parents, *Electronic Journal of e-learning*, *14*(1), 66-80.

Adler, A. (1996). What's Left: Hate Speech, Pornography, and the Problem for Artistic Expression. *Cal L. Rev.*, *84*, 1499.

Agrawal, S. (2021). Human rights and the city: A view from Canada. *Journal of the American Planning Association*, *87*(1), 3-10.

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

Bennett, C.J. (2001). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology*, *3*, 197-210.

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

Berg, T. (2015). The pedagogy of the observed: How does surveillance technology influence dance studio education? *Research in Dance Education*, *16*(3), 230-244.

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.

Bruder, P. (2014). Gadgets go to school: The benefits and risks of BYOD (Bring Your Own Device). *NJEA Review*, 15-18.

Carter Andrews, D. J., et al., (2021). Decentering Whiteness in Teacher Education: Addressing the Questions of Who, With Whom, and How. Journal of Teacher Education, 72(2).

Castillo-Manzano, J.I., Castro-Nuno, M., Lopez-Valpuesta, L., Sanz-Diaz, M.T., & Yniguez, R.

(2017). To take or not to take the laptop or tablet to classes, that is the question. *Computers in Human Behavior*, *68*, 326-333.

Chan, T-W., Liao, C.C.Y., Cheng, H.N.H., Chang, W-C. (2017). Supporting parental engagement in a BYOD (bring your own device) *Journal of Computers in Education, 4(*2), 107-125.

Criminal Code in Canada (1985) (R.S.C Section 319(2) C-46). Willful promotion of hatred. (Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-46/section-319.html)

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

Dawson, P. (2016). Five ways to hack and cheat with bring-your-own-device electronic examinations. *British Journal of Educational Technology*, *47*(4), 592-600.

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.

Doblanko, (2021). Combating online hate, yes your tweet could be considered hate speech. Retrieved from https://www.constitutionalstudies.ca/2021/08/combating-online-hate-yes-your-tweet-could-be-considered-hate-speech/

Dooley, S. Y. (1996). *A comparison of adult children of alcoholic families with adult children from non-alcoholic families: A replication*. University of North Texas.

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.

Goeke, J. (2017). Identifying Protective Factors for Adult Children of Alcoholics.

Goldstein, N.E.S., Cole, L.M., Houck, M., Haney-Caron, E., Brooks Holliday, S., Kreimer, R., Bethel, K. (2019). Dismantling the school-to-prison pipeline- The Philadelphia police school diversion program

Gomez, P., Harris, S.K., Carreiro, C., Isorna, M., Rial, A., (2017). Profiles of Internet use and parent involvement, and rates of online risks and problematic Internet use among Spanish adolescents

Goodyear, V.A., Kerner, C., & Quennerstedt, M. (2019). Young people's uses of wearable healthy lifestyle technologies; surveillance, self-surveillance and resistance. *Sport, Education and Society*, *24*(3), 212-225.

Government of Canada (2022). Free to Be Me: LGBTQ2 Glossary(retrieved from https://women-gender-equality.canada.ca/en/free-to-be-me/lgbtq2-glossary.html)

Graves, J. L., & Orvidas, I. B. K. (2015). Race≠ DNA. *Teaching Tolerance*, *50*.Henry, M. (2009). Surveillance

Henry, M. (2009). Surveillance

Herbitter, C., Vaughan, M. D., & Pantalone, D. W. (2021). Mental health provider bias and clinical competence in addressing asexuality, consensual non-monogamy, and BDSM: a narrative review. *Sexual and Relationship Therapy*, 1-24.

Hills, A. (2018). Teachers privacy rights and cloud storage. *Education Law Journal*, *28*(1), 123-130.Hope, A. (2016). Biopower and school surveillance technologies 2.0. *British Journal of Sociology of Education*, *37*(7), 885-904.

Hopkins, N., Tate, M., Sylvester, A., & Johnstone, D. (2017). Motivations for 21st century school children to bring their own device to school. *Information Systems Frontiers*, *19*(5), 1191-1203.

Hung, H-T. (2017). Clickers in the flipped classroom: Bring your own device (BYOD) to promote student learning, *Interactive Learning Environments*, *25*(8), 983-995.

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

Imazeki, J. (2014). Bring-Your-Own-Device: Turning Cell Phones into Forces for Good, *The Journal of Economic Education*, *45*(3), 240-250.

Jameson, J. K., Clayton, P. H., & Jaeger, A. (2010). Community engaged scholarship as mutually transformative partnerships. In L. Harter, J. Hamel-Lambert,& J. Millesen (Eds.), Participatory partnerships for social action and research (pp. 259–277).Dubuque, IA: Kendall Hunt.

Jha, A., & Blumenthal, D. (2008). International adoption of electronic health records, health information technology in the United States: where we stand. *ONC and RWJF*, *7*, 104-142.

Joly, M. P., & Wheaton, B. (2020). Human rights in countries of origin and the mental health of migrants to Canada. *SSM-population health*, *11*, 100571.

Kay, R., Benzimra, D., & Li, J. (2017). Exploring factors that influence technology-based distractions in bring your own device classrooms. *Journal of Educational Computing Research. 55(*7), 974-995.

Keng, C. J., & Liao, T. H. (2013). Self-confidence, anxiety, and post-purchase dissonance: a panel study. *Journal of Applied Social Psychology*, *43*(8), 1636-1647.

Lamarche, L. (2020). Resisting Rights: Canada and the International Bill of Rights, 1947–76 by Jennifer Tunnicliffe.

Laxman, K., & Holt, C. (2017). Do Mobile Devices increase learners' access to learning opportunities and enhance learning motivation. *International Journal on e-learning, 16*(3), 245-263.

Kupchik, A. (2010). *Homeroom security*. New York University Press.

Laxman, K., & Holt, C. (2017). Do Mobile Devices increase learners' access to learning opportunities and

enhance learning motivation. *International Journal on e-learning, 16*(3), 245-263.

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).

Lensmire, T. J. (2011). Laughing white men. *Journal of Curriculum Theorizing*, *27*(3).

MacKenzie, B. (2016). #Inappropriate: Ramifications of teachers' off duty social media postings, *Education Law Journal, 26*(1), 53-72.

Maxwell, B. (2018). When teachers' off-duty creative pursuits conflict with role model expectations: A critical analysis of Shewan. *Interchange, 49*(2), 161-178.

McBride, B., Shannon, K., Bingham, B., Braschel, M., Strathdee, S., & Goldenberg, S. M. (2020). Underreporting of violence to police among women sex workers in Canada: amplified inequities for im/migrant and in-call workers prior to and following end-demand legislation. *Health and human rights*, *22*(2), 257.

McLean, K.J. (2016). The implementation of bring your own device (BYOD) in primary [elementary] schools, *Frontiers in Psychology, 7*, 1739.

Mellor, R. M., Greenfield, S. M., Dowswell, G., Sheppard, J. P., Quinn, T., & McManus, R. J. (2013). Health care professionals' views on discussing sexual wellbeing with patients who have had a stroke: a qualitative study. *PloS one, 8*(10), e78802.

Menees, M.M & Segrin, C (2000). The Specificity of Disrupted Processes in Families of Adult Children of Alcoholics, *Alcohol and Alcoholism*, 35 (4), 361-367.

Merga, MK. (2016). "Bring your own device": Considering potential risks to student health. *Health Education Journal, 75*(4). 464-473.

Milne, E. (2016). "I Have the Worst Fear of Teachers": Moments of Inclusion and Exclusion in Family/School Relationships among Indigenous Families in Southern Ontario. *Canadian Review of Sociology/Revue canadienne de sociologie, 53*(3), 270-289.

Moll, R., Pieschl, S., & Bromme, R. (2017). Whoever will read it–The overload heuristic in collective privacy expectations. *Computers in Human Behavior, 75*, 484-493.

Monahan, T. (2006). The surveillance curriculum: Risk management and social control in the neoliberal school. Routledge.

Mucowski, R. J. (1991). *Adult children of alcoholic parents: Verification of a role typology* (Doctoral dissertation, The Fielding Institute).

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

Murray, A., Luo, T., & Franklin, T. (2019). Embracing a technologically enhanced environment: Teachers' experience educating students in an always-on and connected bring your own device (BYOD) classroom. *International Journal of E-learning, 18*(1), 53-78.

Mykhalovskiy, E., Kazatchkine, C., Foreman-Mackey, A., McClelland, A., Peck, R., Hastings, C., & Elliott, R. (2020). Human rights, public health and COVID-19 in Canada. *Canadian Journal of Public Health, 111*(6), 975-979.

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

Nam, T. (2019). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal, 56*, 530-544.

Olalere, M., Abdullah, M.T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *Sage Open, 5*(2), 1-11.

Paccione-Dyszlewski, M. R. (1992). *Personality characteristics of adult children of alcoholic parents* (Doctoral dissertation, Fordham University).

Page, D. (2017). Conceptualising the surveillance of teachers. *British Journal of Sociology of Education, 38*(7). 991-1006.

Pagram, J., Cooper, M., & Newhouse, P.C. (2015). Bring your own digital device in teacher education, *Journal of digital learning in teacher education, 31*(2), 64-72.

Perry-Hazan, L. & Brinhack, M. (2018). The hidden human rights curriculum of surveillance cameras in schools: due process, privacy and trust. *Cambridge Journal of Education, 48*(1), 47-64.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing, 19*(1), 27-41.

Raffaele Mendez, L. M. (2003). Predictors of suspension and negative school outcomes: A longitudinal investigation. *New directions for youth development*, *2003*(99), 17-33.

Robertson, K., Khoo, C., & Song, Y. (2020). To surveil and predict: A human rights analysis of algorithmic policing in Canada. Citizen Lab and International Human Rights Program, University of Toronto.

Sadownik, S. (2015a). Social Media in the Classroom. In R. Caine, H. Wheaton, & L. Massey (Eds.), Proceedings from the International Conference for Bridging Gaps-Higher Education, Media and Society. (pp.69-74) Toronto, ON: WaterHill Publishing.

Sadownik, S. (2015b). Social Media in the Classroom. 3rd Annual Justice, Crime and Deviance: Regional Graduate Research and Networking Conference. Wilfrid Laurier University, Brantford, Ontario.

Sadownik, S. (2017). Creating a social ecological model for elementary mathematics homework. In E. Galindo & J. Newton, (Eds.), Proceedings of the 39th annual meeting of the North American Chapter of the International Group for the Psychology of Mathematics Education (pp. 1341-1344). Indianapolis, IN: Hoosier Association of Mathematics Teacher Educators.

Sadownik, S. A. (2018). *Under Construction: Developing Mathematical Processes and Discourse Through Dialogue in Computer Supported Collaborative Learning Environments* (Doctoral dissertation, University of Toronto (Canada)).

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

Samaras, S. A. (2013). *# ThingsIHate: You: A study of problematic social media discourse and how we as leaders can teach to mitigate the harmful practices and effects on today's children*. University of Victoria (Canada).

Skiba, R. J., Michael, R. S., Nardo, A. C., & Peterson, R. L. (2002). The color of discipline: Sources of racial and gender disproportionality in school punishment. *The urban review*, *34*(4), 317-342.

Song, Y & Wen, Y. (2018). Integrating various apps on BYOD (Bring your own device) into seamless inquiry-based learning to enhance primary students' science learning. *Journal of Science Education and Technology*, *27*(2), 165-176.

Stanlick, S., & Sell, M. (2016). Beyond Superheroes and Sidekicks: Empowerment, Efficacy, and Education in Community Partnerships. *Michigan Journal of Community Service Learning*, *23*(1), 80-84

Sternthall, C. (1988). *Adult children of alcoholics: personality development, interpersonal relationships and parenting* (Master's thesis, California State University, Northridge).

Taylor, E. (2013). *Surveillance schools: security, discipline and control in contemporary education*. Palgrave Macmillan: New York.

Teng, L., Liu, D., Luo, J. (2021). Explicating user negative behavior toward social media: An exploratory examination based on stressor-strain-outcome model. Cognition, Technology & Work

Thompson, R. A., & Calkins, S. D. (1996). The double-edged sword: Emotional regulation for children at risk. *Development and psychopathology*, *8*(1), 163-182.

Tobin, T., Sugai, G., & Colvin, G. (1996). Patterns in middle school discipline records. *Journal of emotional and behavioral disorders*, *4*(2), 82-94.

Umpleby, S. (2012). Moral Education. University of Victoria.

Van Wingerden, C., Lidz, A., Barse, A.J., DeMark, J., Hamiter, D. (2015). Bring your own device (BYOD): The power of the tablet to pocket size mobile device on learning and assessment- possibilities and impacts on university faculty, students. *Handbook of research on learning outcomes and opportunities in the digital age*. 482-509.

Vipond, E. (2019). Becoming Culturally (Un) intelligible: Exploring the Terrain of Trans Life Writing. *a/b: Auto/Biography Studies*, *34*(1), 19-43.

Weiss, M. D. (2008). Gay shame and BDSM pride: Neoliberalism, privacy, and sexual politics. *Radical History Review*, *2008*(100), 87-101.

Wiest-Stevenson, C., & Lee, C. (2016). Trauma-informed schools. *Journal of evidence-informed social work*, *13*(5), 498-503.

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*.