Digital Surveillance in the Networked Classroom

Valerie Steeves, Priscilla Regan and Leslie Regan Shade

"We do a huge amount of tracking online. A huge amount of IT tracking"
(British Assistant Headteacher quoted in Schostak 2014, p. 329)

In the late 1990s, schools in much of the developed world connected most, if not all, of their classrooms to the Internet in an attempt to provide students with universal access to networked communications technologies (Ginsberg & Foster 1998). For the most part, policy makers, technology companies and educators agreed that this connectivity would improve learning outcomes and prepare young people for their role as information workers in the emerging information economy (Ginsberg & Foster 1998; Steeves 2010). The rhetoric of the day also celebrated the child as a natural technology user who would readily adapt to technology and use it to innovate and generate wealth (Shade & Dechief 2005).

The jury is still out on whether or not the networked classroom has delivered on its initial promise. The track record of technology in improving learning outcomes has been mixed at best (see for e.g. Young, Klemz & Murphy 2003) and, although today's students may be better at uploading videos to social media than their parents, they are not particularly savvy when it comes to evaluating online content (Steeves 2012b) or using networked resources to conduct simple research (Quarton 2003). Perhaps most telling is the fact that most young people do not see themselves as networked learners or entrepreneurs, but as social actors in a networked social space (Fisk 2014; Rooney 2012). Their primary interests online are accordingly not education or employment, but hanging out with friends, listening to music and entertainment (Steeves 2010).

However, networked communications technologies *have* significantly changed the classroom in an unanticipated way – they have exponentially increased the level of surveillance to which students are subjected (Taylor 2013; Schostak 2014; Hope 2015b). Clearly, this is not a global phenomenon. It is important to note that large parts of the world still struggle to find funding for teachers let alone computers (UNICEF 2014), and some developed countries like Germany have used privacy laws to constrain school surveillance (Chadderton 2013). However, a growing body of research[1] reports that many students are now routinely monitored on an ongoing basis.

Much of this surveillance was originally put in place because of fears that students would be exposed to offensive online content and potential sexual perpetrators (Ginsberg & Foster 1998). For example, keystroke capture software, filtering software, dedicated intranets, and webcams are often used to "keep an eye on children" and protect them from pedophiles, stalkers and hate mongers. However, that same surveillance is also used to control students who, especially in the context of cyber-bullying and sexting, are seen as risky in and of themselves (Steeves & Bailey 2016). Digital surveillance in schools as such exemplifies Lyon's Janus-faced view of surveillance as both care and control (Lyon 2001).

However care and control are just part of the picture. Digital surveillance in schools is also about profit. Educational software companies siphon off vast amounts of personal information from students and use it to profile and market to them (Singer 2015). Tracking apps like ClassDojo, which is used in 85,000 schools in the United States alone, encourage teachers to award or subtract "virtual points" based on students' daily behaviour, and to share behaviour reports with parents by smartphone (Singer 2014). Students in some schools in the United States and the United Kingdom pay for lunch in the school cafeteria by swiping a fingerprint or submitting to an iris scan. Radio-frequency identification (RFID) tags in student cards, clothing or backpacks can track the physical location of each student throughout the day; some schools even broadcast a child's location to parents over the Web.

[1] Especially in Canada, the United States and the United Kingdom.

In this chapter, we provide an overview of the ways in which these kinds of networked surveillance have reshaped the social relationships at the heart of classroom learning, blurred the lines between supervision and state control, and reconstructed education to make it more amenable to the needs of the information economy. We start by looking at how digital surveillance has disrupted experiences of, and relationships between, students and teachers in the networked classroom. We then explore the impact of what Zuboff (2015) calls "surveillance capitalism" on schools, through the lens of two emerging trends: the use of commercial software to police students on social media; and the collection of students' personal information by educational software companies. We argue that the current escalation of big data programs and analytics in schools for the purposes of tracking academic progress and for monitoring their social media communication to ensure safety creates an unnecessary incursion into student's lives that threatens their rights, as well as those of parents and teachers.

Care, Control and Classroom Relationships

For many students, digital monitoring is a given; they know that everything they say or do on a networked device is potentially tracked by their school and that they may be held to account for it at some later date (Steeves 2012a). The most frequently reported problem with this surveillance is that it interferes with students' ability to learn because school filters and other protective measures block access to sites they need to visit to complete in-class assignments and homework (McCahill & Finn 2010; Steeves 2012a). Moreover, this is not an unusual occurrence. One study conducted by the Canadian Teachers' Federation, for example, reports that 83 percent of teachers experience this in their classroom, and close to one-fifth (19%) experience it frequently (Johnson, Riel & Froese-Germain 2016).

Although students are often annoyed or bemused by this kind of constraint, they are most frustrated by the level of micro-management that the networked classroom enables (Steeves, 2012a). Part of this is rooted in what Schostak (2014) calls a “paranoid curriculum” (p. 328) that encourages teachers to keep a constant watch on incremental learning outcomes:

> The intensity of keeping the learners on track, focused, and on task was clear in the continual recourse to the smart board and the use of the tracker, the electronic ‘writing down system’ so that a history of progress, of meeting targets, falling behind targets or exceeding targets could be instantly seen by any member of staff – as well as the particular pupil tracking their own development, or indeed parent – who accessed the tracker (pp. 331-332).

Schostak concludes that this type of “supersurveillance” discourages cooperation among students and rewards conformity over creative or critical thinking (p. 334). It is also particularly bad for learning (Richards 2013; Suski 2014). As Davis (2001) notes:

> To discern and to ‘own’ appropriate connections and justifications requires a certain kind of ‘privacy’ from the teacher. That is, the teacher, as authoritative source of knowledge, needs to be distanced in some measure from the processes through which this discernment and ownership is acquired. In some measure the teacher must lack detailed access to the child’s thinking processes, at least for some of the time, and the child must be aware that the teacher lacks this access (p. 252).

However, the “continual policing” (p. 330) that students experience also makes it more difficult to develop the relationships of trust that are at the heart of education. This is perhaps most easily seen in the research on cyberbullying. Given the resilience of moral panics around children in general, and children and technology in particular, concerns about children’s online safety have been “mobilized in productive ways … [allowing for a] ‘more than usual’ exercise of control" (Fisk, 2014, p. 567). Surveillance is a key part of this control. Suski (2014) notes, for example, that the majority of policy and legislative frameworks designed to protect children from cyberbullying in the United States give schools nearly unlimited powers to place students under surveillance both inside and outside of school. This allows:

> … schools to reach into students' lives while they are at home, work, the mall or other non-school places and gather electronic activity. The laws expand the proverbial schoolhouse gates to such a degree that, in many cases, schools' authority to conduct surveillance of students is nearly without bounds (p. 68).

Moreover, these policies typically take a neoliberal approach that obfuscates the systemic issues at play, such as racism and sexism, and instead focuses attention on a punitive frame that seeks to use surveillance to identify individual offenders so they can be punished (Bailey 2014). Students see this as a form of hyper-control that encourages teachers to overreact. For example, two 13-14-year-old girls in Toronto reported that they were threatened with suspension when they compared tans after March break because they were both black. The teacher assumed that this was form of racial bullying and reported them to the principal, who then implemented a zero tolerance policy to punish the girls (Steeves, 2012a).

This kind of intervention teaches students that they cannot trust school rules to help them navigate online conflict. As Giroux (2003) notes, "Trust and respect now give way to fear, disdain, and suspicion" (p. 554), both on the part of teachers and school administrators who are increasingly being required to exercise hyper-vigilance, and on the part of students who feel that surveillance opens them up to the enforcement of rules that are misguided and unhelpful (Steeves 2012a, 2014). Paradoxically, surveillance accordingly makes it more difficult for students to get help when they need it, even from a teacher they trust, because they feel that they will be judged on the basis of their digital footprint instead of their own experiences and perceptions of the event (Steeves, 2012a).

Interestingly, teachers echo many of the concerns raised by students. Although networked technologies, like virtual learning environments, student dashboards, and video classroom management systems, can enhance learning (Hope, 2015b), teachers report that students are also more easily distracted and plagiarism rates are higher in a networked classroom (Johnson, Riel & Froese-Germain 2016; Lajeunesse 2008). Accordingly, digital technologies that make it more difficult to learn can also make it more difficult to teach.

However, like students, teachers are most concerned about the negative impact that digital surveillance has on their relationships with others in the school. One of the unanticipated consequences of the networked classroom is that teachers are monitored along with students. For example, content filters govern what material teachers can include in a lesson, and keystroke capture creates a permanent record of class discussions. As educational professionals, classroom teachers have been trained to help students evaluate both the quality and the impact of offensive or explicit content, and that often includes challenging students when they make a misstep. However, once that content is accessed over a network, a teacher's discretion is replaced by an algorithm that decides what students may and may not see and do, and the digital record makes it harder to create a private space where students can honestly talk about difficult issues because ephemeral comments may have long-lasting repercussions (Schostak 2014). Ironically, this kind of surveillance hampers the teacher's ability to make the most of teachable moments as they arise (Albury 2016). It also harms teachers' relationships with school administrators because teachers see it as proof that administrators do not trust their judgment (Steeves 2012b).

Digital surveillance accordingly disrupts the social relationships in the classroom by casting students/teachers as objects of suspicion and teachers/administrators as "agents of surveillance … the final arbiters of risk and appropriateness" (Fisk 2014, p. 567). This in turn lowers the level of trust between the social actors at the heart of learning. It also amplifies neoliberal trends in education by normalizing networked surveillance practices (Saltman & Gabbard 2003; Kupchik and Monahan 2006; Giroux 2003, Hope 2015a) as technologies of suspicion that "conflate prediction with prescription, acting as technological forms of supervision, monitoring, supposed deterrence, and ultimately control" (Fisk 2014, pp. 568-569).

Networked Surveillance and the Commodification of Learning

Like surveillance in schools, the commercialization of education is a long-standing issue of concern (Moll 2001). However, networked technologies merge surveillance and commercialization in ways that profoundly extend the impact of both. First, these technologies exponentially increase the amount of data that flows between the school and the marketplace. This creates "openings in new techno-surveillance markets to be exploited by private companies" (Hope 2015b, p. 850), in effect "[commercializing] one of the last and largest unexploited markets in the world … the K-12 sector" (Moll 2001). Second, analytic algorithms enable corporations to commodify that data and create new information products. Third, corporations use these products – and the analytics that generate them – to train children's consumption as learners, and to integrate children into the production cycle of the information marketplace. Zuboff (2015) calls this "surveillance capitalism … a new form of information capitalism [that] aims to predict and modify human behaviour as a means to produce revenue and market control" (p. 75).

These dynamics are illustrated by two emerging trends in education: the rise of commercial services that monitor students on social media on behalf of schools; and the aggressive marketing of fully-networked educational software that embeds the predictive analytics of surveillance capitalism directly into the learning process.

Commercial Monitoring of Students on Social Media

Social media has drawn the attention of educators for two reasons. First, since social media is an appealing mode of communication for school-aged students in elementary, junior and high school, many teachers argue that it should be integrated into the classroom to better engage students in the learning process (Johnson, M., Riel, R. and Froese-Germain, 2016). Certainly, social media use is ubiquitous. The Pew Research Center in the United States estimates that "24% of teens go online almost constantly" (Lenhart 2015). And the same study reports that the most popular platforms attract a significant percentage of young people: 71% of American teens use Facebook, 52% use Instagram, 41% use Snapchat and 33% use Twitter.

However the popularity of social media also creates apprehension amongst some parents and adults about young people's exposure to and participation in cyberbullying and sexting. As seen above, these concerns have put pressure on schools to use surveillance to manage social media use by their students, both during school hours and after-school, as a protective measure. The rationale for this surveillance is to deter or minimize the potential actions of students who may use social media to enact threats or potential acts of violence, cyberbullying and hate against other students or their school. In response to these concerns, some school districts are purchasing commercial services that monitor, control, and track the social media communication of students.

Securitization and responsibilization are thus the pretext for commercial social media monitoring. This justification is heightened by high-profile and tragic school shootings perpetrated often by students themselves within their own schools[1]. In addition, growing concern over the role of social media in youth radicalization has sparked policy interventions that increase the pressure on schools to monitor students' social media use. For instance, UNESCO has initiated a research call that seeks to create a global map of research "into the assumed roles played by social media in radicalization processes in all regions" (UNESCO, 2016) and the United Kingdom Department for Education has requested that schools set up filtering and monitoring systems on school computers to guard against radicalization (Sparrow 2015). Commercial monitoring is therefore an attractive option, as it ostensibly helps manage the "risks" of the networked school without unduly stressing its already over-taxed resources.

Whether to capitalize on educational opportunities or to protect students from the perceived dangers of networked communications, schools' interest in student social media use further blurs the lines between the classroom and other parts of young people's lives (Steeves 2010; Hope 2015a). It also elicits ethical and policy issues, notably around freedom of speech and privacy rights. Before we delve into a discussion of these concerns, a brief description of three American social media monitoring companies follows.

1. Three Examples of Commercial Monitoring

The three companies that will be briefly described, Geo Listening, SnapTrends, and Digital Fly, are all private American companies. In their promotional narrative, these companies position schools as sites of risk for youth, and the companies situate themselves as services that can safeguard schools against acts of violence or threats, while also assisting young people in coping with their social and emotional problems.[2]

Geo Listening monitors, analyzes, and presents daily reports to school administrators on relevant public social media posts from students aged 13 and older that could be cause for concern. The company flags student communication that, in the company's opinion, evidences negative content that goes against a school's code of conduct, content that suggests violent threats to other students or the school, or indications of cyberbullying or self-harm. Daily reports are categorized under cyberbullying, despair, hate, harm, crime, vandalism, substance abuse, and truancy (Geo Listening, About Us, 2016).

Snaptrends Inc. brands itself as a "social observer system" offering "location-based social intelligence" for industries including corporate security, healthcare, law enforcement, sports and athletics, and the educational sector. They utilize advanced analytics, custom keywords, and geofencing (i.e. geolocation information) to provide information for schools, school athletic venues, and study abroad locations. Their technology creates a social media map comprised of keywords related to school violence, suicide, cyberbullying, truancy, and illegal drugs sales, culled from a user-defined lens of locations. As they describe, "You can drop multiple lenses or a single lens in conjunction with social media monitoring outside of the lens. With Snaptrends' proprietary algorithms and processes, you hear the full spectrum of the social conversation no matter where it takes place" (Snaptrends, 2016).

Digital Fly, whose corporate motto is "Your Fly on the Wall", is a service promoted to schools and school districts that can "monitor threats in real-time to help prevent the next incident before it happens" (Digital Fly, 2016). The service flags content indicating "bullying,

[2] A more detailed analysis of these companies and the privacy and ethical aspects is in Shade and Singh (2016, forthcoming).

self-harm, gang activity, theft, hate crimes, vandalism, wild parties, substance abuse, and truancy" (ibid). Geolocation facilitates the monitoring of social media within a 10-mile radius of a school. Digital Fly promotes its "Watch List", a tailored list of keywords, users, groups and locations; an anonymous text "Tip Line"; and an "Incident Rewind" that can "search for evidence of malintent leading up to an incident. Look for signs to prevent the behavior in the future" (ibid).

2. Ethics & Privacy

As Andrew Hope (2015) argues, a regime of governmentality contributes to an actuarial turn in school surveillance and the commercialization of responsibilization by parents and adults, leading to a blurring of public and private communication which takes place in both schools and homes. In this environment, critical conversations about the policy and ethical issues of data monitoring with respect to young people's rights to privacy and their freedom of speech are significant.

It is important to note that these services monitor the social media of students not only when they are at school, but also during after-school hours. This raises free speech implications if young people are punished for material they made outside of school hours and away from their school grounds (Fahlquist, 2015). Moreover, much of this happens in a legal vacuum. For example, in the United States (a country with atypically strong protections for speech), there are no precedents by the U.S. Supreme Court about off-campus internet speech, leaving the legality of the surveillance of students' internet communication by schools unclear, even if the rationale is to protect the school population (Mendola, 2015).

Social media monitoring of student's communication also raises issues regarding appropriate notification and consent. What are the provisions for schools and school districts to notify parents and guardians of the monitoring, and can they choose to opt out of the monitoring? Are there policies for data access and retention, especially when young people leave a school district or graduate? Digital monitoring, data collection, and big data analytics in the educational sector raises, as Kathryn Montgomery remarks, “the specter of ‘digital dossiers’ that could follow young people into adulthood, affecting their access to education, employment, health care, and financial services” (Montgomery 2015, p. 268).

There are also questions about the non-transparency of the practices that are at the heart of surveillance capitalism in the education sector. Geo Listening and Snap Trends provide privacy policies but at the time of publication there was no readily available policy for Digital Fly (it may be available only for subscribers). The policies are not transparent about the types of data analytics in which these companies engage and whether the data they gather is correlated or cross-referenced with other educational information and records about the student, nor whether the data is linked with social media profiles students have on other platforms, and the profiles of their friends and other students within their wider social media network.

Perhaps most concerning is how privacy is reconstructed as a safety problem that can be solved through the use of surveillance. This construction allows the corporate collection and use of information that is at the core of surveillance capitalism to recede into the background. Privacy, the narrative goes, is no longer under threat because corporations monitor young people; instead young people’s privacy is at risk because their communications can lead to cyberbullying and other “inappropriate” behaviours. Commercial surveillance is accordingly not a problem but a solution because it can identify risky behaviour and steer and control social interaction to minimize risks. Ironically, this construction demonizes the one benefit of the networked classroom that is most closely aligned to improving educational outcomes: the ability to connect students with people outside the classroom so they can communicate with the broader community (Steeves 2010, 2012b).

Educational Software and Predictive Analytics

The alignment of surveillance and commercialization is also evident in the burgeoning market in educational software. As all countries recognize the importance of competing in the global environment and as the world becomes more of a global village as a result of economic and social activities facilitated by the Internet, countries around the globe are directing attention and resources on improving educational achievement especially at the primary and secondary levels. With the concomitant increase in the costs of providing education and concerns about financial responsibility, heightened consideration of accountability and results, elevated awareness of the range of teacher skills and student learning styles and needs, more focus is being placed on the promises offered by online software and educational technology.

Information technology companies recognize the huge market offered by K-12 education and are aggressively developing and marketing their products. Most of these companies are large international ones based in the United States, such as Google and Microsoft, but a range of new startup companies, still largely based in the United States, now populate the market. They, like the larger players in the field, are hoping to take advantage of the emerging "big data" environment, where data is collected passively through the environment and fed back into the marketplace where is can be commodified.

From the school's point of view, the benefits of big data applications include more sophisticated analyses of student learning and testing, more personalized learning, more effective delivery of educational materials, improved assessment, and more responsiveness to student needs. On the downside big data applications and products raise the possibility of discrimination as a result of profiling and tracking of students, as well as uses of student information for a wider range of purposes.

Much of the ethical discussion about big data in education has been framed in terms of privacy. This is not particularly surprising both because privacy is viewed as a multi-faceted concept with several different components and also because discussions about ethics and information technology in other sectors and over time have often been categorized under the value of privacy. We can identify six concerns traditionally associated with privacy that are challenged by big data generally and in the context of education.[3]

The *first* is that collection of information about an individual should take place with the knowledge of the individual and that the amount of information should be minimized to that which is required for the particular purpose for which it was collected. This is the classic information privacy concern that has been addressed by the Fair Information Practice Principles (FIPPs) often summarized by notice, consent, choice and transparency. These principles are the basis of much privacy and data protection legislation around the world.

Although many have questioned the effectiveness of the FIPPs approach more generally, there is almost universal agreement among privacy scholars and experts that the FIPPs approach is not appropriate in the big data environment where there is more collection of information, by more parties, about more aspects of an individual's life, and with more granularity about that life. But the issue is not merely "more" or even the qualitative changes that quantity does not convey. The issue is also how much of big data collection takes place without the individual's awareness. As the President's Council of Advisors on Science and Technology (PCAST) noted in 2014

[3] The six concerns were identified and discussed in detail in Regan (2017); their application to big data in education are more fully developed in Regan, Jesse and Khwaja (2016).

individuals “constantly *emit* into the environment information whose use or misuse may be a source of privacy concerns” (President’s Council 2014).

Moreover, enhancements in digital storage capacity combined with improvements in computational power and developments of more sophisticated algorithms for analyzing data have enabled organizations to probe and dissect datasets in ways unimagined even twenty years ago. As Rubinstein similarly points out big data make possible the extraction of new, potentially useful information from data – this “newly discovered information is not only unintuitive and unpredictable, but also results from a fairly opaque process” (Rubinstein 2013).

The enterprise of big data challenges previous ideas about how to limit data collection about individuals and how to involve the individual in the process of data collection and subsequent uses so that the individual could exercise some meaningful control. A preliminary review of ed tech company websites (Regan, Jesse and Khwaja 2016)[4] revealed that privacy is rarely highlighted in marketing and promotional materials, which predictably tend to highlight the benefits of technology and data-driven education, and that uncovering privacy statements can sometimes take many mouse clicks with a confusing array of privacy statements. A 2014 *Politico* investigation found similar patterns in ed tech companies’ policies and practices, taking particular note of their “legal jargon and fuzzy terminology,” that companies “typically reserve the right to change the policy at any time,” and that the information “may be subject to an entirely new privacy policy, if the company is sold – a common fate for a start-up.” (Simon 2014)

[4] The websites of the following ed tech vendors were examined: Schoology.com; Edmentum; Remind; Edsby; PowerSchool SIS; Clever; Public Consulting Group Canada; SAS Enterprise Analytics for Education; McGraw-Hill Connect; LoudCloud Systems; Amplify; Tenmarks-Amazon; and Google for Education.

This issue of notice, consent and transparency becomes even more complicated in K-12 education than it does in other contexts both because records of children and hence the concerns of parents come into play and also because the educational relationship is mandatory, not voluntary. Educational technology firms usually do not generally have a direct contractual relationship with the students and parents but with the schools, school boards or teachers. Thus providing information and controls about the uses of big data are at least one step removed from the data subject. In 2013, Joel Reidenberg directed a study on cloud computing in public schools, which found that school districts were not addressing privacy concerns in a uniform or informed manner when they transfer student information to cloud computing service providers (Reidenberg, Russell, Kovnot, Norton, Cloutier and Alvardado 2013). Based on their detailed investigation into a sample of schools, they concluded that "cloud services are poorly understood, non-transparent and weakly governed" (p. 6) and "an overwhelming majority of cloud services do not address parental notice, consent, or access to student information" (p.7).

A *second* concern long associated with privacy is that individuals should be able to remain anonymous or obscure if they so choose to do so. But with an ever-increasing number of social relationships and practices becoming data points, it becomes more difficult for individuals to remain unidentified or unfindable. Algorithmic searches of datasets rather quickly eradicate what had been high transaction costs on finding meaningful information (Hartzog and Selinger 2013 a and b). With big data, anonymization of information about individuals becomes more difficult, if not impossible, as big data makes reidentifying data rather easy (Sweeney 2000). In effect few characteristics are actually needed to uniquely identify an individual, making it very difficult to anonymize databases by removing some characteristics, because the bundle of characteristics remaining will likely prove sufficient to identify individuals once a database is merged with other databases and searched using sophisticated algorithms. For example, Latanya Sweeney and colleagues identified the names of volunteer participants in the de-identified public, Personal Genome Project by linking the Project's profiles to public records and data mining the results (Sweeney, Abu and Winn 2013).

Educational data are often stored in large, longitudinal data sets from which personally identifiable variables have been removed. These data sets are used for reporting purposes from the school to district to state or province and finally to the federal government. They are also used for research purposes to identify trends over time and to analyze factors that affect student performance. They have traditionally been referred to as aggregate, anonymized data – but this tradition is being challenged in the era of big data.

Computer scientists and privacy policy experts and advocates continue to press for better techniques for anonymizing data, for example by using only 3 digits of one's ZIP code or redacting year of birth or day of month. However, as databases become larger and more integrated these attempts increasingly prove to be ineffective. After reviewing the computer science and legal literatures on anonymity and reidentification, Paul Ohm concludes that: "Data can be either useful or perfectly anonymous but never both" (Ohm 2010, p.1704). This would appear to hold true in the educational context.

A *third* concern involves the surveillance or tracking that provides more and more detailed information for big data analytics – and that big data require to be even more powerful. Big data not only entails more monitoring of activities and extraction of data about those activities, but also involve analysis of those activities to determine likely future activities. This more sophisticated prediction that is built into many big data analytics transforms surveillance into a more omniscient phenomenon. The experience in New York with the educational technology firm InBloom in 2013-14 is illustrative. What ultimately led to InBloom's demise was a cacophony of voices concerned about privacy, parental consent and access to the aggregated data. InBloom's software had included some 400 "optional fields" that schools could choose to fill in and that included some fairly sensitive information such as disability status, social security numbers, family relationships, reasons for enrollment changes, and disciplinary actions. Parents and privacy advocates balked at what they saw as intrusive data gathering that seemed like surveillance. Questions were raised about who could and would access the data, especially data like disciplinary actions, with subjective terms like "'perpetrator,' 'victim,' and 'principal watch list,'" as well as the potential for such data to be used to "stratify or channel children" (Singer 2013).

In addition, online testing and teaching programs monitor how long it takes students to answer a question or read a page – and often also capture key strokes or patterns of reading or responding that might indicate the thought processes of the student. The programs also track where (home, school, computer lab) the student is working and what time of day – and often also record what other students are working on the same programs at that time. The results of all this tracking are cross-matched with more traditional information about the student as well as new information from various devices (such as how much a student moves throughout the day or how much time a student spends on social networking sites) – and all of this is fed into predictive analytics programs to determine student learning patterns, strengths and weaknesses, and advice about how best to personalize the learning environment for that student – and raises a *fourth* ethical concern regarding autonomy.

Big data, especially the analytics powered by big data, challenge individual autonomy, the individual's ability to govern his or her life as that individual thinks best. Big data algorithms jeopardize autonomy by leading people in certain directions – to buy certain items, try certain routes or restaurants – and in a certain way challenge the self as defined throughout much of Western philosophy. Some have expressed this concern about social fragmentation into “filter bubbles,” where individuals are subject to feedback loops that limit individuals’ sense of their options (Pariser 2011). Tene and Polonetsky point to the dangers of predictive analysis including the perpetuation of old prejudices and the accentuation of social stratification (2013, p.253).

Autonomy is thus related to a *fifth* privacy concern associated with big data, which involves traditional due process for individuals, the principle that individuals are treated fairly and equally and not discriminated against based on race, gender, age or other personal attributes – or based on factors of which they are not aware. Big data’s use of mathematical algorithms and artificial intelligence to make predictions about individuals based on conglomerates of their information and that of others raises questions about treating individuals as individuals fairly, accurately, and in ways they can understand (Citron and Pasquale, 2014). This concern involves issues of profiling and discrimination.

In the education environment, with its recognition of the importance of education to equal opportunity, there is a longstanding concern for not discriminating and for watching closely for subtle, as well as obvious, signs of discrimination. But with big data such subtle signs may be difficult to discern. For example, Ohm points out that “big data helps companies find a reasonable proxy for race” (Ohm, 2014). But perhaps more troubling in education is that big data facilitates the creation of more refined, intersectional categories that discriminate among students in more insidious and harder to read ways. As Jonas Lerman points out: “The big data revolution may create new forms of inequality and subordination, and thus raise broad democracy concerns" (2013, p.60). At a Data and Civil Rights Conference in 2014, these issues were explicitly addressed in one paper in which the authors pointed out: "the complexity of algorithmic analysis makes identification of bias and discrimination difficult;" the difficulty of reversing or avoiding "flawed algorithmic assessments;" the danger of self-fulfilling prophecies or prejudging students; and the risk of increasing stratification (Alarcon, Zeide, Rosenblat, Wikelius, boyd, Gangadharan, & Yu, 2014).

A *sixth* issue that has long been part of the debate about privacy, especially information privacy, is the question of the ownership of data about an individual. Does the individual "own" the information or does the third party holding the information in a database? As one moves further from either submitting personal information to one organization or clicks "I agree" on a website, any ownership in that information arguably fades. And if that information becomes part of a dataset that is then reused or reconfigured or combined with another or sold to another organization, the claim of personal ownership in that information diminishes even more. In the education arena, student records are generally "owned" by the school or school district. The involvement of ed tech companies has somewhat muddied the question of ownership – depending on how contracts with these firms are written.

Big data applications in education signal yet another fundamental change in the dynamics of sorting students. The actions of today's "digital student" are monitored and tracked in ways inconceivable in earlier times – and with the results of more fine-grained tracking, less transparency, and persistent record-keeping from pre-school through college and possibly beyond. Our review of education technology companies offerings and marketing materials indicates that these companies are amassing quite detailed information on student demographic characteristics in their databases (including not just traditional location and family information but: school lunch eligibility, emergency contact information, parent and guardian information, health profiles, disciplinary records, counselling referrals, etc.) as well as detailed information on student learning records (including not just test scores and grades but also individual learning and test-taking patterns, attention spans) – and all of this is analyzed with sophisticated algorithms resulting in new categorizations and groupings of students. Moreover, these records follow students throughout their educational careers. Whether these sortings replicate or serve as proxies for traditional discriminatory groups or create new ones may be something of an open question but one that is critical to pursue.

Policy Implications

The networked classroom raises important issues because the technologies that support it enable others – teachers, administrators, corporations – to place students under surveillance in new ways. Emerging trends, like social media monitoring and big data educational software, up the ante, and call upon us to craft policy responses that will protect privacy as an essential component of learning and healthy school relationships.

As our discussion of educational software indicates, existing privacy frameworks offer ways to push back against surveillance. The example of Germany is an encouraging one (Chadderton 2013). However, these laws could be strengthened by expressly prohibiting school administrators from consent to the collection of students' information on behalf of students and parents (see Taylor 2013). For example, Assembly Bill 1442 in the State of California addresses social media monitoring in schools, delineating that students, parents and guardians must be notified when schools and school districts are considering setting up, and when they implement monitoring programs. This would help redress the "politics of control" which currently privilege the "values and perspectives of those undertaking the surveillance in a way that disregards the interests or perspectives of the child" (Rooney, 2012, p. 331) by putting students and parents back into the mix. The Bill also stipulates that monitoring can only consist of information relevant to student or school safety. Information collected can be seen by students and parents/guardians, with appropriate mechanisms for the redress or removal of incorrect information. All student information that is collected must be destroyed wither when the student turns 18 or changes the school or leaves the school district (State of California, Assembly Bill 1442, 2014).

However, we can also supplement FIPPS-style approaches with new policy responses that seek to protect the value of a surveillance-free school more directly. Richard (2013), for one, calls for laws, policies and practices that protect intellectual privacy, i.e. "the ability … to develop ideas and beliefs away from the unwanted gaze or interference of others" (p. 389). because this kind of privacy is an essential element of the learning process. In like vein, Steeves (2015) suggests a human rights approach will deepen our ability to protect young people's privacy.

In the United States, a notable example of a campaign that combines a FIPPS approach with broader notions of privacy is the Student Privacy Bill of Rights drafted by the Electronic Privacy Information Center (EPIC). It provides principles for access and amendment of student data, promotes security through responsible data practices, and advocates for transparency with clear and accessible privacy and security practices, but it also calls for respect for the context of student data and mechanisms to hold schools and private companies accountable for the management of their data (EPIC, 2014).

Ultimately, policy makers must explicitly question the roll out of technologies and hold them to public judgment. Accountability for how and when schools implement new technologies that enable, if not require surveillance, is critical; these should not be regarded as merely new approaches to learning or security but need to be looked at more broadly as they will instil values and practices for the next generation. We argue above that the current escalation of big data programs and analytics in schools for the purposes of tracking academic progress and for monitoring their social media communication to ensure safety creates an unnecessary incursion into student's lives that threatens their rights, as well as those of parents and teachers.

Acknowledgements

We are grateful to the Social Science Humanities Research Council of Canada (SSHRC) for their funding of the eQuality Partnership Grant. For information, see: http://www.equalityproject.ca/.

Works Cited

Alarcon, Andrea, Elana Zeide, Alex Rosenblat, Kate Wikelius, danah boyd, Seeta Pena Gangadharan, and Corrine Yu. (2014, Oct 30). "Data & Civil Rights: Education Primer," produced for Data & Civil Rights Conference. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2542268

Albury, Kath. (2016). Sexting, Schools and Surveillance: Mediated Sexuality in the Classroom. In Gavin Brown and Kath Browne (Eds.), *The Routledge Research Companion to Geographies of Sex and Sexualities*. London/New York: Routledge.

Bailey, Jane. (2014). Time to Unpack the Juggernaut?: Reflections on the Canadian Federal Parliamentary Debates on Cyberbullying. *Dalhousie Law Journal 37*(2), 661-707.

Buckingham, David. (2016, January 4). Radicalisation, social media and young people: Why we need a more thoughtful approach. https://davidbuckingham.net/2016/01/14/radicalisation-social-media-and-young-people-why-we-need-a-more-thoughtful-approach/

California, Assembly Bill 1442, Pupil Records: Social Media, Chapter 799, An Act to Add Section 49073.6 to the Education Code, Relating to Pupil Records, Approved by Governor September 29, 2014. Filed with Secretary of State, September 29, 2014. Available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1442.

CBC News. (2016, January 22). Deadly School Shootings in Canada. http://www.cbc.ca/news/canada/deadly-shootings-schools-canada-1.3416685

Chadderton, Charlotte. (2014). Book Review: Surveillance Schools. *Surveillance & Society 12*(1), 182-184.

Citron, Danielle Keats and Frank Pasquale. (2014). "The Scored Society: Due Process for Automated Predictions," *Washington Law Review* (2014) 89: 101-133.

Davis, Andrew. (2001). Do Children Have Privacy Rights in the Classroom? *Studies in Philosophy and Education 20*, 245-254.

Digital Fly. (2016). See http://www.digitalfly.net

Electronic Privacy Information Center (EPIC). (2014). Student Bill of Rights. https://epic.org/privacy/student/bill-of-rights.html

Fahlquist, Jessica. N. (2015). Responsibility and privacy: Ethical aspects of using GPS to track children. *Children & Society, 29*, 38–47.

Geo Listening: https://geolistening.com/why-choose-us/

Ginsberg, Ralph B. and Kenneth R. Foster. (1998). The Wired Classroom. *IEEE Spectrum 35*(8), 44-51.

Hartzog, Woodrow and Evan Selinger. (2013, Sept. 3) "Big Data in Small Hands," *Stanford Law Review Online* 66:81-88.

Hartzog, Woodrow and Evan Selinger. (2013, Jan. 17) "Obscurity: A Better Way to Think about Your Data than Privacy," *Atlantic*. Available at: http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/

Hope, Andrew. (2015a). Biopower and School Surveillance Technologies 2.0. *British Journal of Sociology and Education* (in press).

Hope, Andrew. (2015b). Governmentality and the ‘Selling’ of School Surveillance Devices. *The Sociological Review 63*, 840-857.

Hull, Kathleen E. (2011). Book Review: Homeroom Security and Schools Under Surveillance. *Law & Society Review 45*(4), 1063-1068.

Johnson, M., Riel, R. and Froese-Germain, B. (2016). *Connected to Learn: Teachers' Experiences with Networked Technologies in the Classroom*. Ottawa: MediaSmarts/Canadian Teachers' Federation.

Lajeunesse, Claude. (2008). *Towards Empowerment, Respect and Accountability: Report and Recommendations on the Impact of the Internet and Related Technologies on English Public Schools in Quebec*. Montreal: Quebec English School Boards Association.

Lenhart, Amanda. (2015). Teens, social media & technology overview 2015. Pew Research Centre. Available at http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/

Lerman, Jonas. (2013, Sept. 3). “Big Data and Its Exclusions,” *Stanford Law Review Online* 66: 55-63.

Lyon, David. (2001). *Surveillance Society: Monitoring Everyday Life.* Buckingham/Philadelphia: Open University Press.

McCahill, Michael and Rachel Finn. (2010). The Social Impact of Surveillance in Three UK Schools: ‘Angels’, ‘Devils’ and ‘Teen Mums’. *Surveillance & Society 7*(3/4), 273-289.

Mendola, Catherine. E. (2015). Big brother as parent: Using surveillance to patrol students’ internet speech. *Boston College Journal of Law & Social Justice*, *35*, 153-192. Available at http://lawdigitalcommons.bc.edu/jlsj/vol35/iss1/7

Moll, Marita. (2001). Pianos vs. Politics: Sustaining Public Education in the Age of Globalization. In Marita Moll and Leslie Regan Shade (Eds.), *eCommerce vs. eCommons: Communications in the Public Interest*. Ottawa: Canadian Centre for Policy Alternatives.

Montgomery, K. (2015). Children’s media culture in a big data world. *Journal of Children and Media,* 9, 266–271.

New York Times. (2016--). School Shootings and Violence. http://www.nytimes.com/topic/subject/school-shootings-and-violence

Ohm, Paul. (2010). “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,” 57 *UCLA Law Review* 1701-1777.

Ohm, Paul. (2014). “General Principles for Data Use and Analysis,” in Julia Lane Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum (eds), *Privacy, Big Data, and the*

Public Good: Frameworks for Engagement. New York: Cambridge University Press, pp. 96-111.

Pariser, Eli. (2011). *The Filter Bubble: How the new Personalized Web is Changing What We Read and How We Think.* New York: Penguin Books.

President's Council of Advisors on Science and Technology. (2014, May). *Big Data and Privacy: A Technological Perspective* (May 2014), p. 38. http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

Quarton, Barbara. (2003). Research skills and the new undergraduate. Journal of Instructional Psychology 30(2), 120-**.

Regan, Priscilla. (2017). "Big Data and Privacy," in *Analytics, Policy and Governance.* Ed by Jennifer Bachner, Kathryn Wagner Hill, and Benjamin Ginsberg. New Haven: Yale University Press.

Regan, Priscilla, Jolene Jesse and Elsa Talat Khwaja. 2016. "Big Data in the Education Arena: 21st Century Student Sorting and Tracking," at the 7th Biannual Surveillance and Society Conference in Barcelona Spain (April 20 to April 23).

Reidenberg, Joel, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier, and Daniela Alvardado. (2013, Dec. 13). "Privacy and Cloud Computing in Public

Schools," Center on Law and Information Policy, Fordham Law School. Available at: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

Richards, Neil M. (2013). The Dangers of Surveillance. *Harvard Law Review 126*, 1934-1965.

Rubinstein, Ira S. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law 3*(2), 74-87. Available at: http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.full.pdf+html

Shade, Leslie Regan and Diane Yvonne Dechief. (2005). Canada's SchoolNet: Wiring Up Schools? In Alison A. Carr-Chellman (Ed.), *Global Perspectives on e-Learning*. Thousand Oaks, CA: Sage, pp. 131-144.

Shade, Leslie Regan and Rianka Singh. (2016, forthcoming). 'Honestly, We're Not Spying on Kids': School Surveillance of Young People's Social Media. *Social Media + Society*.

Simon, Stephanie. (2014, May 15). "The big biz of spying on little kids," *Politico* available at: http://www.politico.com/story/2014/05/data-mining-your-children-106676

Singer, Natasha, (2013, October 5). "Deciding Who Sees Students' Data," The New York Times, http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html.

Singer, Natasha. (2014, November 16). Privacy Concerns for ClassDojo and Other Tracking Apps for School-Children. *New York Times.* http://www.nytimes.com/2014/11/17/technology/privacy-concerns-for-classdojo-and-other-tracking-apps-for-schoolchildren.html

Singer, Natasha. (2015, March 11). Privacy Pitfalls as Education Apps Spread Haphazardly. *New York Times*. http://www.nytimes.com/2015/03/12/technology/learning-apps-outstrip-school-oversight-and-student-privacy-is-among-the-risks.html?_r=0

Snaptrends (2016) http://snaptrends.com/social-media-software/geofencing/.

Sparrow, Andrew. (2015, December 22). Tougher guidelines for schools to tackle online radicalisation. *The Guardian.* https://www.theguardian.com/education/2015/dec/22/tougher-guidelines-schools-online-radicalisation

Steeves, Valerie. (2015). Privacy, Sociality and the Failure of Regulation: Lessons Learned from Young Canadians' Online Experiences. In Beate Roessler and Dorota Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge, UK: Cambridge University Press, 244-260.

Steeves, Valerie. (2014). Young Canadians in a Wired World, Phase III: Cyberbullying: Dealing with Online Meanness, Cruelty and Threats. Ottawa: MediaSmarts.

Steeves, Valerie. (2010). Online Surveillance in Canadian Schools. In Torin Monahan and Rodolfo D. Torres (Eds.), *Schools Under Surveillance: Cultures of Control in Public Education*. New Brunswick, NJ: Rutgers University Press.

Steeves, Valerie. (2012a). *Young Canadians in a Wired World, Phase III: Talkiing to Youth and Parents about Life Online*. Ottawa: Media Smarts.

Steeves, Valerie. (2012b). *Young Canadians in a Wired World, Phase III: Teachers' Perspectives*. Ottawa: Media Smarts.

Steeves, Valerie and Jane Bailey. (2016). Living in the Mirror: Understanding Young Women's Experiences with Online Social Networking. In Emily van der Meulen and Robert Heynen (Eds.), *Expanding the Gaze: Gender and the Politics of Surveillance*. Toronto: University of Toronto Press.

Suski, Emily F. (2014). Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority Under Cyberbullying Laws. *Case Western Reserve Law Review 65*(1), 63-119.

Sweeney, Latanya. (2000). *Uniqueness of Simple Demographics in the US Population* (Laboratory for International Data Privacy, Working Paper LIDAP-WP4). Available at: http://dataprivacylab.org/projects/identifiability/index.html

Sweeney, Latanya, Akua Abu, and Julia Winn. (2013, April 24). "Identifying Paticipants in the Personal Genome Project by Name," *Harvard University Data privacy Lab*, White Paper 1021-1. Available at: http://dataprivacylab.org/projects/pgp/1021-1.pdf

Taylor, Emmeline. (2013). *Surveillance Schools: Security, Discipline and Control in Contemporary Education*. Basingstoke: Palgrave Pivot.

Tene, Omar and Jules Polonetsky. (2013). "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property* 11(5): 239-273. Available at: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip

UNICEF. (2014). *UNICEF Strategic Plan 2014-2017*. New York: UNICEF.

UNESCO. (2016). UNESCO calls for research proposals: Social media and youth radicalization in the digital age. http://en.unesco.org/news/unesco-calls-research-proposals-social-media-and-youth-radicalization-digital-age

Wrennall, Lynne. (2010). Surveillance and Child Protection: De-mystifying the Trojan Horse. *Surveillance & Society 7*(3/4), 304-324.

Young, Mark R., Bruce R. Klemz and J. Willan Murphy. (2003). Enhancing Learning Outcomes: The Effects of Instructional Technology, Learning Styles, Instructional Methods, and Student Behavior. *Journal of Marketing Education 25*(2), 130-142.

Zuboff, Shoshana. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology 30*, 75-89.