Digital Privacy in the Mainstream of Education

Lorayne ROBERTSON,
Faculty of Education, Ontario Tech University,
Oshawa, Ontario, Canada L1M2A0

Bill MUIRHEAD
Faculty of Education, Ontario Tech University,
Oshawa, Ontario, Canada L1M2A0

ABSTRACT[1]

Concerns about digital privacy are so ubiquitous that they have become part of the wallpaper of life, but the implications of large data and predictive analytics on privacy merit serious scholarly attention. Recently, a colleague recounted that he had purchased potato chips at a store with cash and was surprised the next day to be targeted with advertisements for the same chips on his home computing device. This anecdote encapsulates nicely the developments with digital privacy and surveillance in a world where the consumer is not aware of the hidden workings of corporate surveillance. North America in particular has entered into an era where the private human experience is being captured through digital devices, with or without permission, and sold for profit.

The reality is that neither policy nor education has kept pace with these digital developments, to the point that vast amounts of data are collected, synthesized, and sold without the consumer's express permission or cognizance. Data are captured continuously from smart devices and Closed Circuit Television (CCTV) footage, documenting individuals' locations and preferences. Many personal elements of life are voluntarily shared online such as heart rate and sleep habits. The "creep" of data collected with and without permission is greater than most people realize.

The educational implications of this surveillance need to be explored. Parents, students, educational leaders, and the general public have a right to know how digital surveillance works and the implications for predictive analytics on their futures and their decision-making in a democratic society. Policy gaps are evident surrounding digital privacy and education. More critical, interdisciplinary approaches to policy analysis are needed in education, guided by a critical policy analysis framework that interrogates all aspects of policy related to this emerging issue.

Keywords: Education, Digital Privacy, Surveillance, Online, Critical Policy Analysis, Reidentification, Risk

1. INTRODUCTION

Schools are part of society and they can mirror society. For example, population trends are reflected in school enrolments. Conversely, schools can have an impact on society. Schools are sometimes seen as sites for universal interventions to improve society such as smoking cessation programs and anti-bullying campaigns, etc. Schools have reportedly had some positive influence on societal changes such as promoting recycling in the community [1]. This paper examines how changes in technology affordances in society have created opportunities for digital surveillance. Next, an examination of how these changes impact schools and create potential risks for student populations is reviewed. Employing a critical policy analysis framework, the authors examine the risks and benefits afforded by the increasingly ubiquitous release of passive data in society and consider potential policy responses from the education sectors. In conducting this analysis, the authors raise key questions for the consideration of education providers and policy designers and make recommendations for next steps.

The reality is that it is increasingly difficult to be a private person in 2020. However, there appears to be a general lack of awareness of what constitutes "privacy-sensitive information" [2] p. 3. While people might be very careful about sharing personal identifiers such as their full name and credit card numbers, they may not be aware that they are passively sharing other information that can reveal their identity. Recently, there has been a proliferation of publications by the news media to alert the public to the passive collection of data from their phones and their devices. According to the New York Times Privacy Project [3], at any moment there are dozens of "unregulated, little-scrutinized" companies cataloguing the movements of tens of millions of Americans and storing the data. According to this study, location data from sources hidden in mobile phone apps has made an open book of American lives: where they visit and for how long. The resulting accumulation of data reveals the most private details of American lives, all collected through apps that users place on their smartphones. Similar alarms have been raised in the Canadian news media cautioning that companies such as Google and Facebook are tracking users' search data for marketing purposes [4].

Digital privacy policies have not kept pace with these digital developments. Vast amounts of data are collected, synthesized, and sold in a largely unregulated arena, where consumers may or may not have given access and may or may not be aware of the consequences of data recombination. In the meantime, data are captured

[1] Thanks to Dr. Ellen Vogel, Ontario Tech University for peer review.

continuously from smart devices and CCTV footage, documenting individuals' lives, locations, and preferences. Many personal elements of life are also voluntarily shared online such as heart rate and sleep habits. The re-combining of data collected with and without permission has greater consequences than most people realize because it represents a significant erosion of privacy. The educational implications of this surveillance also warrant exploration. Parents, students, educational leaders, and the general public have a right to know how digital surveillance works and the implications of predictive analytics on their futures and their decision-making in a democratic society. The curriculum and policy gaps surrounding digital privacy in education are clearly evident. More critical, interdisciplinary approaches to policy analysis are needed in general and particularly in education. In this paper, the authors outline the digital privacy landscape and explore some of the risks identified with *surveillance capitalism* [5]. A critical policy analysis framework [6] guides this interrogation and recommendations.

2. PRIVACY-SENSITIVE INFORMATION

The authors define digital privacy as: *an expectation of privacy unless the user has given consent that includes an awareness of the risks associated with online services, and individual control over the collection, distribution and retention of personal information.* Central to a discussion about digital privacy is the concept of consent.

Consent is presently becoming eroded under the guise of necessity. Digital devices are essential to participating in commerce today, requiring the use of bank cards, credit cards, and loyalty cards that track consumers' purchases and preferences and create digital dossiers of their financial transactions. More than 550 companies make up the personal information industry and their sales of lists of consumer data and spending profiles generate billions of dollars of revenue per year [7]. Numerous applications request user consent. If users log into Wi-Fi services outside their home, they are asked to consent to terms of use. Other information is gathered unbeknownst to consumers. Clickstream data (the linked collection of actions taken, sites visited and visit durations) is collected so that advertisers can control users' choices for internet purchases [7]. This creates a situation where it is difficult for users to ensure that information collected about them is used only at their own discretion.

Big data can provide powerful insights into the health of individuals and populations based on the active and passive collection of related health data; however, the protection and management of such data are fundamental to its use and application. Data hacking increased by 320% in 2016 and 81 breaches of patient records were reported [8]. This speaks to the need for new privacy protections and increased personal vigilance regarding data collection and use.

Canada has produced guidelines for obtaining meaningful consent. One key regulation that protects individuals' rights to privacy is the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2016) which regulates privacy for the private (commercial) sector in Canada [9]. PIPEDA promotes key principles for fair information practices. These principles are:

1. **Notice**: Users should be informed when their information is collected, for what purpose, how long it will be used, and how it will be shared;
2. **Choice**: Users should have a choice about whether or not they share their information;
3. **Access**: Users should be able to check and confirm their information on request;
4. **Security**: The users' information should be protected from unauthorized access;
5. **Scope**: Only the required information can be collected;
6. **Purpose**: The purpose for collecting the information should be disclosed;
7. **Limitations**: There should be a time limit on how long the information will be held;
8. **Accountability**: Organizations should ensure that their privacy policies are followed [9].

While what is private information does vary from person to person, a Canadian policy brief in 2013 [2] identified four common categories of privacy-sensitive information:

1. Personally-identifiable information: such as the name of the user, credit card numbers, and IP addresses.
2. Lifestyle information: such as race, religion, relationship status, sexual orientation, political affiliations, friends, and family members.
3. Behavioural data: such as viewing habits, websites visited and time spent, online purchases, store loyalty programs, and credit cards.
4. Unique device identifiers: such as user location, determined by global unique identifiers connected to mobile devices [2].

Although the general public may be aware that they are targeted through their social networks and their browsing history, they may not be aware of the level of surveillance tracking that then connects to their personal information. Alarms have also been raised that the general public is not aware that elements of their data can be combined (cross-referenced) and then used to identify them [2]. A small amount of simple demographic information can identify people uniquely. For example, in one study, data such as postal code, date of birth, and gender were used to uniquely identify 87% of Americans [10]. There are indications that movie preferences can also generate similar identifications [11]. This process of combining databases that were intended to be kept apart has been labelled as *reidentification* [11], and is seen as a game changer in the digital privacy protection sphere because of its implications.

There are different forms of data capture. Passive data capture occurs when data is taken without the knowledge of the consumer; conversely, some data is offered up by the consumer with permission. At the present time, lines between these two types of data capture are blurred. For example, when customers enter a store, they may use the store's Wi-Fi and "click-through" the privacy statement rather than standing in the store and reading through a long, convoluted privacy agreement. By agreeing to the privacy policy, consumers consent to the collection of data. This can be interpreted as giving permission to access other types of data such as where they pause in the store to look at merchandise. Within this same store (or associated stores) there may have been a poster at the door indicating the use of security cameras. Customers may accept that they are being watched, but do not interpret that their image is being captured and shared. Their faces (licence plates, etc.) could be compiled in databases such as facial-recognition software programs. Potentially, a consumer's face, licence plate, credit card, and purchases could be linked and identified, calling the concept of informed consent into question. The result is that a person can go into a store and purchase a product using cash but that product will still be connected to the user through data such as smartphone location tracking.

Websites sell transaction data and digital footprints of websites visited to advertisers. The data collected by Internet Service Providers (ISP's) pose a "grave threat" to privacy that needs to be regulated [12]. Companies aggregate and republish the data to tailor advertising directly to an individual. A Google blog in 2009 announced that this initiative was designed deliberately in order to make advertising "more relevant" for its users [13]. Since 2009, evidence indicates that personalized data profiles can be used to target information for political purposes. According to a Canadian news source [14], Facebook allowed the data of 50 million users to be accessed by Cambridge Analytica. Some data was provided by users who thought it would be used for academic purposes. This data was then sold and used for political purposes [14]. It employed a technique known as behavioural micro-targeting, which delivers future advertising to those who have shown the most interest, and is based on the analysis of websites used, combined with other data, to create a consumer profile.

In another example, Facebook reportedly employed a deep learning neural network of 9 layers in order to compile both photographs and personal timelines of a dataset of 4 million photos that users uploaded to Facebook, unaware that they were providing data for a neural network. Data analytics identified the persons in these photographs, raising critical questions about whether or not permission is required to combine disparate data sets for new purposes [15]. These and other cases have crossed an invisible line with policy makers, resulting in investigations.

A quintessentially Canadian example demonstrates the utility of loyalty apps to provide information about customers. James McLeod [16] accessed the detailed location data that Tim Hortons, a Canadian coffee chain, was collecting about him through its loyalty card and found that his home address, work location, and vacation plans were known to the company through its mobile ordering app. The app was silently logging his coordinates through its corporate servers both day and night. He found that the app was tracking him when he was near competing companies, and every time he visited his parents' farm, where he was certain he did not use the loyalty app. In all, it tracked his longitude and latitude 2,700 times in five months. It tracked him at a railway station in Morocco through a Starbucks and a KFC at that location. Like many, he had assumed that the app was active only when he was ordering coffee at the coffee shop. This example is worth noting given that approximately six million people have downloaded the Tim Hortons app and the coffee company is now reportedly planning to leverage this information to drive the next phase of customer loyalty, targeted to individuals [16].

Cadillac Fairview was investigated [17] for rolling out Anonymous Video Analytics (AVA) technology facial recognition software in 12 of its malls in Canada in 2018 through cameras that recorded the faces of persons who stopped at their information kiosks. In 2020, the data capture and retention of 5,061,324 numerical representations of faces was reported by a joint investigation of Canadian privacy commissioners nationally and provincially. While the company disputed that the information collected was personal information, the Privacy Commissioners disagreed, finding that the unique biometric information (facial recognition calculations), the location, and the timestamp constituted personal information. The Commission ruled that a notice on the mall doorway that video was being collected was insufficient as consent. The mall chain has since discontinued this data capture [17].

These four examples illustrate that privacy is no longer a "given" in the digital era and consent as a concept is an increasingly blurry one. Most consent is click-through because the privacy details are lengthy and hard to understand. The explanation of the privacy policy for one online hotel booking site is 21 pages long. For example, there is no reasonable expectation of informed consent for a client booking a hotel over the phone at midnight in an unknown city. While people use their devices for convenience and trade off their privacy, corporations use their data to further erode their privacy and their solitude through data sharing and recombination. The next section explores some definitions and implications of this type of corporate surveillance.

3. SURVEILLANCE CAPITALISM

A claim has been made that a new economic logic is in place, despite warnings almost 25 years ago about the capability of data to threaten individual freedom; Zuboff [5] defines this logic as *surveillance capitalism* and finds that this type of surveillance has been relatively unchallenged by policy makers to date. This new economic order claims that human experience is free material for hidden commercial practices of data extraction, prediction, and sales. These practices are allowed to proliferate because the dangerous illusion persists that *privacy is private* [5]. In surveillance capitalism, human experience is captured by different mechanisms, and the data are reconstituted as behaviour. This data capture is allowed to continue when customers give up pieces of themselves and when pieces of their information are taken from them without their knowledge.

According to Zuboff [5], surveillance capitalism is a form of economic logic that concentrates wealth, knowledge, and power in the hands of the few. They take advantage of the "lucrative behavioural data" to fund "immense growth and profits” for corporations [5], p.42. The use of private human experience as free raw material for behavioural data presents challenges to democracy and to society. Rather than working for changes that benefit society such as improving health outcomes or the environment, this form of corporate capitalism works for profit. Zuboff warns that this represents an erosion of human rights as companies trade in human futures. She claims that this revolution began when ordinary users and consumers began sharing everyday data from “connected” products such as cars, ovens and fitness trackers. Information harvesting and information warfare by corporate entities illustrate what she terms, “the asymmetries of knowledge and power” in the United States [5], p. 179.

The public is complicit in the release of information. Despite indicating that they have privacy concerns, they use simple passcodes and share these codes among devices [18]. They share their personal information on social media sites and, in general, while they do not believe that their nationality, gender, or age constitute sensitive information, they are increasingly concerned about how data might be combined for personal profiles [18]. They want to understand the purpose of the data collection and assess whether the benefits outweigh the risks. The request for too much data, for example, might outweigh the benefit [18]. Currently, legislation in Europe does not allow the collection of personal information for purposes other than the stated, intended purpose. In Canada, as discussed, the PIPEDA legislation [9] is being applied to specific cases such as the report on Cadillac-Fairview malls [17]. Internationally, there is a range of policy and legislative responses to this issue.

4. IMPLICATIONS FOR EDUCATION

The protection of personally-identifiable information (PII) for youth has a different level of importance because there are greater risks for their safety and their age may make them less able to give informed consent. Without clear understandings, schools and school districts might be unknowingly complicit in providing third party access to student information through educational apps. It makes sense to put in place an expectation that students who use technology in schools also need opportunities to gain understandings about digital privacy. For example, in the United States, the *Children’s Internet Protection Act* (2000) requires schools that receive funding for technology to also provide students with education about online behaviour.

A Global Privacy Enforcement Network (GPEN) was established in 2010 [19] composed of 60 global privacy regulators. They identified that teaching platforms which are internet-based can put students at risk for disclosing their personal information. In a 2017 review, GPEN found that most online educational apps required teachers and students to provide their emails for access, thereby providing a link to other PII. Only one-third of the educational apps reviewed allowed the teachers to create virtual classes where students’ identities could be masked. Although teachers complied, it was also difficult to delete these classes at the end of term. While most of the online educational services restricted access to student data, almost one-third of the educational apps reviewed did not provide helpful ways for students to opt out or to block third party access to their data [19], taking away their right to make a privacy decision.

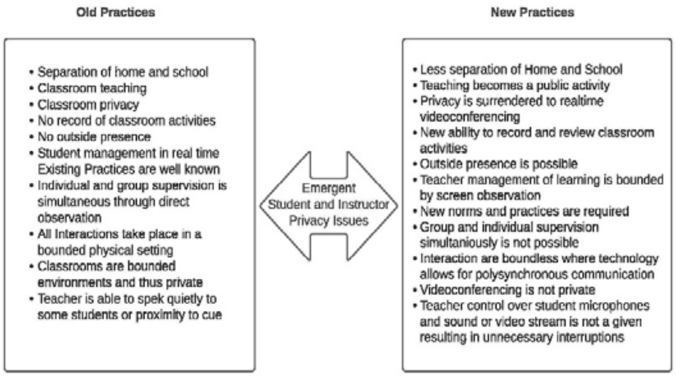
In response to the COVID-19 global pandemic, educators have adopted emergency remote teaching as an emergent pedagogy to address the closure of schools [20], [21]. Emergency remote teaching can be characterized by rapid adoption of online technologies, shifting classroom learning materials to online settings, and utilizing new technologies without substantial training in their use. While the pivot to online learning has been rapid, policies for online privacy have not kept pace with changes in modality. Educators and parents require an understanding that they should have a reasonable expectation for privacy while online.

Children and their parents need to be aware that their online presence can document their personal story long after their use has ended through data retention and data harvesting. For example, long before graduates arrive at an actual interview for a job or to attend an institution of higher learning, much of their private lives can be viewed online. As they mature, they will likely seek online information to make decisions about their health, for guidance on raising their children, and many other means of personal protection and growth. For each phase of their lives, they will need to understand the present and future implications of sharing information. They will need to acquire competencies to analyze the cost vs. the benefit of sharing information online, to protect their privacy, and have access to informed consent.

Recent re-conceptualizations of privacy have been influenced by the outbreak of the global COVID-19 pandemic and the use of new teaching tools. The pivot to utilizing online technologies has given rise to concerns about what is private, where public and private spaces meet, and what privacy means for both instructors and students. These concerns have manifested themselves in terms of expectations regarding the privacy of the home, and privacy within video-based learning contexts where private actions become public. The notion of privacy has been extended to privacy of professional practice where technologies mediate group/classroom learning contexts. A global shift has taken place. Learning used to take place in school and in individual classrooms, separated from home and without public scrutiny. Now learning happens in online environments where the classroom has been replaced by the kitchen table, the living room, and sometimes the bedrooms of students. Teachers are raising issues about what should be visible on camera and what should remain private. It is astonishing to think that the spaces once deemed the most private (the home and the bedroom) might now be considered as public spaces.

The adoption of videoconferencing has not been without controversy. While some school districts were able to shift to synchronous online learning, there were delays at the onset of pandemic closures because of tensions surrounding teaching as videoconferencing. Teacher unions have been less fulsome in their support for videoconferencing [22]. The Elementary Teachers Federation of Ontario (EFTO), in a public statement, expressed concerns regarding equity of access issues for students, as well as privacy issues for students and teachers [22]. Although the pandemic arrived in Canada during March, 2020, the Ontario Ministry of Education requirements for remote learning [23] were published in August, 2020. Within this memo, the Ministry defined synchronous and asynchronous learning and mandated teacher hours of contact with students when families opt for remote learning. In addition, on any occasion where students are at home for more than three days in a week, the school districts are required to provide synchronous learning through text, voice, or video conferencing. For students in kindergarten, 180 minutes of synchronous learning is mandated. For other grades, 225 minutes of synchronous online learning is required. Digital privacy is mentioned in the memo multiple times and teachers are asked to anonymize student presence although how this is to be achieved is not clear. The Ministry of Education, Ontario policy states that it relies on school districts to have privacy and terms of use policies [23].

The privacy inherent in homes and previously the classroom is no longer separated by expectations of home and school independence but is now open to public invasion. The pivot to involuntary participation in remote teaching has "opened the door" quite literally to homes being scrutinized for location, living conditions, family structure, and personal surroundings. This new reality includes the possibility of family members and siblings walking through camera shots and pets invading the learning space and personal spaces, with these events viewed by anyone else participating online. Other concerns have arisen about who can observe (and interrupt) online classes such as parents and care givers. There are also security concerns related to screen capturing software and the potential to record interactions online.


Old Practices

- Separation of home and school
- Classroom teaching
- Classroom privacy
- No record of classroom activities
- No outside presence
- Student management in real time Existing Practices are well known
- Individual and group supervision is simultaneous through direct observation
- All Interactions take place in a bounded physical setting
- Classrooms are bounded environments and thus private
- Teacher is able to spek quietly to some students or proximity to cue

Emergent Student and Instructor Privacy Issues

New Practices

- Less separation of Home and School
- Teaching becomes a public activity
- Privacy is surrendered to realtime videoconferencing
- New ability to record and review classroom activities
- Outside presence is possible
- Teacher management of learning is bounded by screen observation
- New norms and practices are required
- Group and individual supervision simultaniously is not possible
- Interaction are boundless where technology allows for polysynchronous communication
- Videoconferencing is not private
- Teacher control over student microphones and sound or video stream is not a given resulting in unnecessary interruptions

Figure 1. Reconceptualizing public and private learning spaces

Reconceptualizing privacy in terms of older vs. newer practices (Figure 1) presents novel ways of thinking about privacy. New privacy considerations are raised as private becomes public, as previously semi-private learning environments become public, and interactions and conversations once thought to be bounded by the context of the classroom, become not only public but can be recorded and scrutinized potentially without context (or consent). Professional judgements and actions once thought embedded in school settings are now public or semi-public and consent for recording and archiving can be hidden through screen recording on participants' machines. Many questions have arisen regarding the use of synchronous teaching tools. Zoom, Adobe Connect, Microsoft Teams, and Google Classroom are but a few of the tools that facilitate remote learning, but when used, can raise unique challenges as to what is appropriate and what is not. As privacy is reconceptualized, so too will the legacy of how online tools evolve and how synchronous tools might continue to be used after the pandemic. It is difficult to believe that a post-COVID world will completely return to the teaching and learning practices of the past. Emergency remote teaching may initiate greater use of online technologies and with this, greater potential for security breaches, online tracking, and potentially even greater capture of the online activities of students. The speed at which educators and school districts have had to pivot to using new and emerging online technologies could increase student exposure to unintended data retention and use.

Perhaps most concerning is how conceptions of security, privacy, and personal and professional boundaries have evaporated in less than a year. Home environments on display, online recording, screen capturing, file sharing, excess screen time, time shifting, the sharing of login passwords and hardware among parents, children, and siblings could have long-term implications for what is shared and what is associated with individual users.

5. CRITICAL POLICY ANALYSIS

Policy analysis is a form of educational research that examines the intent and the outcome of educational policies. This field of study was founded in an era where more traditional forms of analysis, such as neutral scientific research and cost-benefit models, dominated. The focus of policy analysis at its origins was on the process of evaluating policy enactment, including the design, plan, implementation, and evaluation of educational problem solving [24]. More recently, this type of research has expanded to include more complex forms of inquiry.

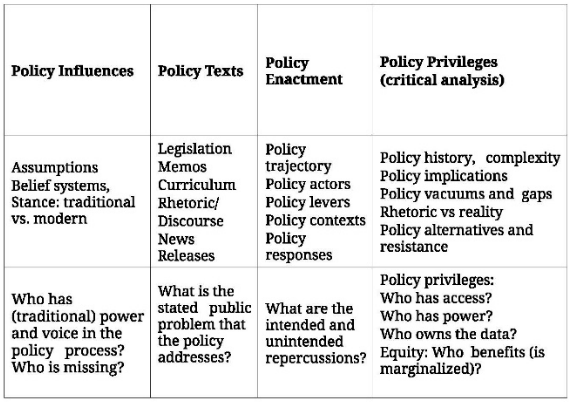
Fischer, for example, [25] sees policy analysis as a multi-disciplinary approach. Rather than a cost-benefit analysis, this type of policy analysis is more nuanced. It would include an analysis of the context of the issue, the basic values of the groups involved, the contestable nature of how the problem was defined, research findings, and arguments for various solutions. More critical approaches to educational policy analysis have emerged [24] that focus on five key innovative and more complex areas of analysis. These approaches are designed to:

1. Interrogate the policy process and compare policy rhetoric and the policy realization;
2. Examine the roots of a policy, its history and how it developed over time, and how it reinforced the dominant culture;
3. Examine how power, knowledge, and resources are distributed;
4. Examine how a policy might create or confirm existing inequalities; and

5. Examine actors who take agency against policies.

Policy analysis should include research findings and it should seek solutions. Critical policy analysis also needs to examine the roots of policies within the dominant culture and should consider how power is distributed and who has a voice or has a say in the decisions surrounding policies. It should also consider the impact of policy decisions or gaps in policy where decisions are needed.

The authors designed a framework for critical policy analysis that guides the formation of questions with the aim of seeking solutions.



Policy Influences	Policy Texts	Policy Enactment	Policy Privileges (critical analysis)
Assumptions Belief systems, Stance: traditional vs. modern	Legislation Memos Curriculum Rhetoric/ Discourse News Releases	Policy trajectory Policy actors Policy levers Policy contexts Policy responses	Policy history, complexity Policy implications Policy vacuums and gaps Rhetoric vs reality Policy alternatives and resistance
Who has (traditional) power and voice in the policy process? Who is missing?	What is the stated public problem that the policy addresses?	What are the intended and unintended repercussions?	Policy privileges: Who has access? Who has power? Who owns the data? Equity: Who benefits (is marginalized)?

Table 1: Critical policy analysis framework [6]

Critical policy analysis research considers multiple perspectives. This type of policy analysis asks fundamental questions surrounding the interplay among factors, including the impact of digital privacy policies or lack of policies on students. The authors developed the critical policy analysis framework to guide this type of rigorous analysis of educational issues. The application of this analysis is intended to make visible the opportunities and challenges of new technologies in schools as they emerge, rather than waiting to see the implications for students' life chances.

Some examples of the types of questions that could be generated by critical policy analysis of digital privacy include:

- For which types of purposes are students' privacy data being collected and combined?
- Should student data be combined for commercial purposes?
- Under what conditions should student data be combined for educational purposes?
- How long should data be retained?
- What are the intended and unintended consequences if data are co-mingled?

Other questions surround consent. For example:

- Is the consent process transparent for the student or parent user?
- Are the uses of the data for commercial purposes transparent or hidden?
- Have all of the contributors to the data been given the option to have their data included?

In the case of students being required to provide their email address in order to participate in an educational app, these questions assume significant importance. Students will want to participate in the apps that are employed in their classroom in order to be on par with the other students. This could change the balance of the privacy paradox [26] when students weigh the risks and the exposure that participation in an app or service encompasses.

More questions surround how and when students should learn about digital privacy. This could be viewed as a role for parents or for schools or as a combined responsibility. International data protection commissioners expressed their view that there is a role for schools to play in this regard, and designed a Personal Data Protection Competency Framework for School Students [27]. Their intent was to share their expertise in this field by providing a framework for data protection that could be used in training courses for all educators, regardless of their discipline. Their recommendations were in the form of student opportunities, skills, and competencies to do the following:

1. Understand the concept of personal data;
2. Understand the importance of digital privacy;
3. Learn how digital hardware and software work;
4. Learn about the digital economy, service providers, and terms of use;
5. Understand data protection;
6. Understand how to regulate the use of their personal information;
7. Know their rights to control access and delete information;
8. Learn how to use settings to protect themselves; and
9. Develop critical, ethical digital citizenship skills [27].

In other words, the privacy commissioners recommend that the education sector should undertake programs to both educate and empower students, and that students need to develop critical skills for online consumption, participation, and production. They suggest that the education sector develop curriculum policies and training to make consent understandable to students and teachers [27].

Another interim policy step is to design legislation to dictate conditions surrounding terms of use. In the interim, some mechanisms are required to help consumers, including students and teachers, understand the surveillance economy, and understand that uninformed participation online can erode both their privacy and their ability to seek information online in ways that are unfettered by earlier preferences.

6. DISCUSSION AND RECOMMENDATIONS

Every student has the right to an online profile as an adult that is uncompromised by media submitted before they were able to make reasoned decisions on their own behalf. In time, the educational arena will develop online learning guidelines, overarching policies for terms of use, curriculum policies, and assessment policies to shepherd the use of new technologies in education as they emerge. In the interim, the answer likely lies in a combination of legislative solutions to protect consumer privacy and greater education for consumers to help them understand the implications of cell-phone tracking, loyalty cards, and the digital footprints left by their online practices.

The authors recommend the following policy matrix as a guide to discussing and creating policy to support student digital privacy. While it is inadvisable to use the present to predict the future, and while it is also difficult to foretell how privacy concerns for learning will be addressed; it is clear that the conceptualization of privacy responsibilities is becoming more urgent and complex. Different players, diverse actors, and individuals with distinctive perspectives will need to share responsibility for privacy and security in the future. Figure 2 outlines both the complexity and shared responsibilities to ensure safe use of technologies for learning. Policy is but one facet of privacy. Institutions must be responsible to ensure that student behaviours online remain private and are not retained for future use unless specifically permitted. Educational institutions share responsibility with parents for ensuring that children's privacy is protected and, where learning technologies are used, transparency regarding personal identification is understood by end users.

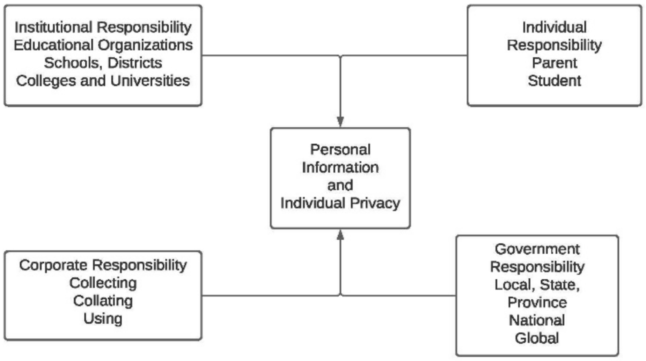


Figure 2. Privacy Matrix: A shared responsibility

Clear and comprehensible documentation needs to be made available to better educate children and parents about the protection of their personally-identifiable information. This should also apply to learners when participating as consumers in online transactions and device use.

Technology companies must also share the responsibility to ensure that the applications used in schooling protect children. From data harvesting, combining data, and engaging in the sale or use of data for profit, corporations must be proactive in developing privacy standards for those unable to give fully informed consent to application use. This becomes more important as educational institutions mandate the use of certain online tools while engaging in emergent blended learning and emergency remote teaching.

Finally, the authors encourage ongoing efforts by governments and privacy commissioners to address online privacy through legislation. Global approaches to privacy protection are needed as the internet bypasses national borders and online tools often reside both within and across national boundaries.

7. SUMMARY

Digital privacy is a concern for everyone. As information technology continues to be a constant companion in everyday life, the attendant data or behavioural surplus will also be a continuing concern. Data collection, online behavioural actions, and the growing sophistication of data collection, data transformation, and data modeling together create an increasingly complex set of circumstances that need to be managed in order to protect student privacy. For this reason, the authors propose consideration of a matrix of shared responsibilities to secure our emerging post-COVID learning environments.

Privacy concerns in a post-pandemic context will be influenced both by technological tools and their affordances but, as seen in Figure 1, school contexts are changing behavioural expectations and sensitivities regarding private personal spaces. These concerns may fade as society becomes more accustomed to working and learning from home, but important questions need to be asked and answered about protecting vulnerable populations from exposure to privacy disclosure risks.

7. ACKNOWLEDGEMENTS

Thank-you to Dr. Ellen Vogel, Ontario Tech University for reviewing this paper.

8. REFERENCES

[1] Evans, S. M., Gill, M. E., & Marchant, J. (1996). Schoolchildren as educators: the indirect influence of environmental education in schools on parents' attitudes towards the environment. *Journal of Biological Education*, *30*(4), 243-248.

[2] Bradshaw, S., Harris, K., & Zeifman, H. (2013). Big Data, Big Responsibilities: Recommendations to the Office of the Privacy Commissioner on Canadian Privacy Rights in a Digital Age. CIGI Junior Fellows Policy Brief No. 8. Retrieved @ https://www.cigionline.org/publications/big-data-big-responsibilities-recommendations-office-privacy-commissioner-canadian

[3] Thompson, S. & Warzel, C. (2019, December 19). Twelve Million Phones, One Dataset, Zero Privacy. *New York Times*. @https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

[4] Dangerfield, K. (2018, March 28). Facebook, Google and others are tracking you. Here's how to stop targeted ads. *Global News*. Retrieved @ https://globalnews.ca/news/4110311/how-to-stop-targeted-ads-facebook-google-browser

[5] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile Books.

[6] Robertson, L. & Muirhead, B. (2019). *Coming soon to a device near you: A policy analysis of mandatory online learning.* Proceedings of the 11th International Conference on Society and Information Technologies (*ICSIT 2020*). March 10-13, 2020. Orlando, Florida, USA.

[7] Solove, D. J. (2004). *The digital person: Technology and privacy in the information age* (Vol. 1). NyU Press.

[8] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1.

[9] Personal Information Protection and Electronic Documents Act (PIPEDA) (2016). Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[10] Sweeney, L. (2004), Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Retrieved @ https://dataprivacylab.org/projects/identifiability/paper1.pdf

[11] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, *57*, 1701.

[12] Ohm, P. (2009). The rise and fall of invasive ISP surveillance. *U. Ill. L. Rev.*, 1417.

[13] Google Official Blog (2009). Making Ads More Interesting. Retrieved @ http://googleblog.blogspot.com/2009/03/making-ads-moreinteresting.html

[14] Vomiero, J. (2018, March 21). How Cambridge Analytica's use of 50 million Facebook users' data turned into a scandal. Global News. Retrieved @ https://globalnews.ca/news/4096443/cambridge-analytica-facebook-data-scandal/

[15] Holmes, W., Bialik, M. & Fadel, C. (2019). *Artificial intelligence in education.* Center for Curriculum Redesign. Retrieved @ https://curriculumredesign.org/our-work/artificial-intelligence-in-education/

[16] James McLeod (2020, June 12). Double-double tracking: How Tim Hortons knows where you sleep, work and vacation. Financial Post. Retrieved @ https://financialpost.com/technology/tim-hortons-app-tracking-customers-intimate-data

[17] Office of the Privacy Commissioner of Canada (2020). Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia. Retrieved @ https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/

[18]Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480. https://doi.org/10.1016/j.giq.2016.06.004

[19] Global Privacy Enforcement Network (GPEN). (2017). *GPEN Sweep 2017: User controls over personal information*. Retrieved @ https://www.privacyenforcement.net/sites/default/files/2017%20GPEN%20Sweep%20-%20International%20Report.pdf

[20] Hodges, C., Moore, S., Lockee, B., Trust, T., & Bond, A. (2020). The difference between emergency remote teaching and online learning. *Educause Review*, *27*. Retrieved @ https://medicine.hofstra.edu/pdf/faculty/facdev/facdev-article.pdf

[21] Doucet, A., Netolicky, D., Timmers, K., & Tuscano, F. J. (2020). Thinking about pedagogy in an unfolding pandemic: an independent report on approaches to distance learning during COVID19 school closures. *Education International & UNESCO.* Retrieved @ https://issuu.com/educationinternational/docs/2020_research_covid-19_eng

[22] Elementary Teachers' Federation of Ontario (ETFO). (2020, May 13). Statement on 'Synchronous' Live Stream Instruction. Retrieved @ https://ett.ca/etfo-statement-on-synchronous-live-stream-instruction/

[23] Ministry of Education, Ontario. (2020, August 13). Policy/Program Memorandum No. 164. Requirements for Remote Learning. Retrieved @ http://www.edu.gov.on.ca/extra/eng/ppm/164.html

[24] Diem, S., Young, M. D., Welton, A. D., Mansfield, K. C., & Lee, P. L. (2014). The intellectual landscape of critical policy analysis. *International Journal of Qualitative Studies in Education*, *27*(9), 1068-1090.

[25] Fischer, F., & Miller, G. J. (Eds.). (2017). *Handbook of public policy analysis: theory, politics, and methods*. Routledge.

[26] Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology,* 45. doi: 10.1002/ejsp.2049

[27] International Working Group on Digital Education (2016). Personal Data Protection Competency Framework for School Students. Retrieved @ http://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf