Do You Know Where Your Students Are? Digital Supervision and Digital Privacy in Schools

Lorayne ROBERTSON,
University of Ontario Institute of Technology,
Oshawa, Ontario, Canada

and

Laurie CORRIGAN,
Peterborough Victoria Northumberland Clarington Catholic District School Board,
Peterborough, Ontario, Canada

ABSTRACT

More students are now online at school because of several factors such as the increasing affordability of mobile devices; the rapid proliferation of low-cost or free educational applications; and because internet access is more widely available. When students are learning online, however, their personal information needs to be protected. Student supervision in the past focused on physical presence, but it must evolve now to include students in digital settings. Updated legislative policy alone cannot eliminate risks to digital privacy. Students, teachers, and parents need to become more aware of the privacy risks and all should build digital citizenship skills. The research presented in this paper is policy analysis that examines the availability and direction of digital supervision policies in Canada and the U.S. and then compares the findings to international policies and directions. The authors find key differences in policy approaches designed to supervise students online and protect their digital privacy. Based on this policy analysis, the authors recommend that more collaborative efforts are needed to protect students' digital privacy and manage their online risks.

Keywords: digital footprint, digital privacy, digital supervision, digital permanence, information security

1. INTRODUCTION

Digital privacy is important to people across organizations and countries because they want to control who has access to their personal information [1], [2], [3]. Teachers and parents supervise young people in order to keep them safe in all situations, whether or not students are online. Issues associated with *digital supervision* are emerging now that students have increased online access [2], [3], [4]. While there have been international calls to protect digital privacy, not all of these policies address online education and digital supervision specifically. The authors employ policy analysis to identify policies and legislation that respond to issues of digital privacy and digital supervision for students. In this policy analysis, they compare policies across jurisdictions. In doing so, they raise awareness of policy gaps and make recommendations for continued policy development to address digital privacy and digital supervision. Canadians are engaged on the internet, and claims have been made that Canadians are, in fact, among those globally who are the most engaged online [5] with an internet penetration rate that varies at around 88% [6]. While email is the most common online activity for

Canadians, using the internet for banking and social media are also very popular [5]. Not surprisingly, 41% of Canadian internet users between the ages of 18 and 34 report that they access the internet most often using their mobile phones [5]. Preferred online activities change when the device used to access the internet is a smartphone and not a laptop computer. The mobile phone is the digital tool of choice for instant messaging (86%), gaming (80%) and social media (69%); these, too, are the favoured online activities of younger Canadians [5] and there are implications for their digital privacy.

The American Academy of Pediatrics [2] raises concerns about online activity and how it affects children, adolescents, and their families. Teenagers are active in social media; one in five U.S. teenagers report that they log into social media more than 10 times per day. Online activities carry some benefits such as socialization and opportunities for learning, but they also carry risks such as cyberbullying and risks to child and adolescent privacy. Teens and pre-teens are at a vulnerable stage; they are learning self-regulation and decision-making but they are susceptible to peer pressure and advertising [2].

These statistics are not unique to Canadian and American students. Research in Europe [7] indicates that most (93%) of adolescents, aged 9-16, are online for an average of 88 minutes per day. The average age of first internet use is seven in Sweden and Denmark and eight in other countries in Northern Europe. This means that young children as well as teens and pre-teens are online. Most European children and adolescents use the internet at home (87%) but 63% report that they use the internet at school [7].

The research described in this paper compares and analyzes the policy supports surrounding students and teachers when they travel *virtually* on the internet. The authors first analyze supervisory policies in Canada and

then compare them to digital privacy policies in the U.S. and internationally.

2. DIGITAL SUPERVISION

Consider this scenario: *Students in Grade 8 History take a virtual field trip to a museum of natural history. The students have selected personal areas of inquiry. Online, they find that they are able to access the museum's catalogue and they can visit different rooms in the museum to learn more about their chosen topics. Later, an official museum guide "visits" the History classroom virtually and invites the students to ask questions. Toward the close of the question and answer period, the guide invites the students to collaborate with other students internationally by posting their email addresses and pictures on the museum's discussion board. At this point, the teacher thanks the guest speaker and advises that her students will not be sharing their contact information and photos. Later, the teacher and her principal have a wide-ranging discussion about digital affordances, digital privacy, and digital supervision. They find that, while the internet affords many new and exciting opportunities, school and district policies and procedures to protect students' digital privacy are not as clear and helpful as they need to be. Teachers are not sure of where they stand with respect to digital supervision and protecting students' digital privacy.*

When students venture outside of school in person to attend school-sanctioned field trips or excursions, they do so in the presence of educators who are responsible for their supervision. Assuming that there are well-established policies and excursion procedures (which is typical of most school districts), teachers utilize a myriad of strategies to accomplish these supervisory tasks successfully. Students are given cautions about sticking together, not speaking to strangers, staying in a group, establishing meeting points and check-ins, and other aspects of supervision. Much of these supervisory practices emanate from district school board policies and procedures that, in Canada, are designed locally by the ministries of education for the 13 provinces and territories.

Significant and compelling questions emerge, however, when the student excursions are online. One issue is jurisdiction. Students online cross boundaries into different countries. This raises questions about who has jurisdictional policy over the students' protection or release of information. The museum may be located in a country that allows pre-teen students to share their personal information without restrictions, or the county may have unknown regulations. For example, the United States has policies to constrain online vendors from approaching minors for personal information. These policies may or may not apply for children from other countries who are accessing materials online from U.S. providers.

Given these new realities, what are the *digital equivalents* to "keeping students together, supervised, and safe" when students and teachers are online? What policies and guidelines exist to guide teachers and students as they venture out into digital territory? And based on these policies and guidelines, what are some of the best practices that teachers employ for virtual excursions? A review of the literature was undertaken to determine the issues with respect to digital privacy, and the skills that students need to acquire before they take a digital leap into places unknown. This examination begins by exploring the concept of digital privacy.

Digital Privacy: A Review of the Literature

Digital privacy is a relative term that refers to the degree of control that individuals hold over the online publication of their personal information. Since the advent of Web 2.0, digital privacy cannot be taken for granted. People access the internet but they are also surveilled and tracked by internet service providers [8]. According to Stoddart, a Canadian privacy commissioner, these practices are known as online tracking, profiling, or targeting. Using data from individuals' participation online, behaviourally-targeted advertising is personalized to the consumer based on their own data and online presence [9]. Video surveillance may happen without a person's awareness. People can be tracked through their mobile devices and phone records, and newer mobile devices track people's activities through global positioning systems (GPS) in their cars or wearable technology such as fitness accessories.

One of the costs associated with being connected at all times is the loss of digital privacy. Students may not know that online users create a *digital footprint* of each site they visit, which is an online record of web activity including personal information and preferences. This digital footprint can put children and adolescents at risk because the footprint connects otherwise disparate aspects of their personally identifiable information (PII). Online participation for many free educational applications is enabled through the waiving of privacy rights, such as agreeing to terms of service (ToS) agreements. Through the tracking of digital footprints, technology enables the flow of PII into cyberspace. Asking children and adolescents to waive their rights to privacy when participating online through ToS agreements is problematic because students are not able to provide fully informed consent. This becomes a complex issue of digital supervision.

Berson and Berson [10] report that *digital privacy* aligns with *data protection* for students. Adults protect children and adolescents of vulnerable ages until they can make choices independently and this includes protecting children's privacy. The picture, however, is more complicated than that. The seeming anonymity of the internet, along with the public documentation of many aspects of children's lives by their parents and caregivers on sites such as Facebook, have desensitized people's awareness that they are losing control of their personal information. Future employers are now able to scan through decades of a child's life, based on the information that their parents have contributed while documenting many personal aspects of their children's lives online.

Adults need to consider that, while there are gains from open sharing, there are also risks [10]. When personal

information is so readily available, it can be used for ulterior motives [11]. Students and teachers may not be aware of the strategies used to gain information from them online, or of the extraordinary capability through the internet to mine data and to track users. According to Berson and Berson [10], youth do not realize that their online contributions collectively create a *digital dossier* about themselves that consists of their preferences and their information, and that they also serve as information brokers to provide data about their friends. Even adults do not realize that these digital dossiers can be sold to third parties. Private information used to be less vulnerable because it was filed in physically different locations that were not digitally connected. Data are now more interconnected, searchable, and accessible. Children and adolescents have begun to contribute to the collection of their PII online, sometimes unwittingly, such as when they provide login information that includes their email address or their parent's email address [10].

With respect to online supervision, research is not clear on who has the responsibility to teach and reinforce internet safety guidelines to protect students' privacy. MediaSmarts, a Canadian non-profit organization dedicated to media literacy education, surveyed more than 5,000 Canadian students in grades 4 through 11 [4]. They report that, while their statistics should be interpreted with caution, most of the students (41%) state that they learn about privacy settings from their parents, while 15% report that they learn about privacy settings from school. Students say that their teachers are more likely to help them find ways to search for information online and how to deal with cyberbullying than to teach them about digital privacy. The MediaSmarts report highlights several important issues. First, parents cannot assume that teachers are taking responsibility for protecting students' digital privacy, and teachers cannot assume that parents are taking responsibility. The need to educate students about digital privacy is shared among all of the caregivers in students' lives. Secondly, students need to have their information and privacy protected until they are able to make these decisions independently [4].

Other concerns with social network participation are worth noting. Youth may not realize that these data are searchable and can be connected back to them. Data posted online can be very difficult (impossible) to delete as the internet is continuously archived. Students may not understand the concept of *digital permanence* until they encounter negative consequences from posting online and then not being able to remove it. Young people may post inappropriate or thoughtless messages that, later in life, can have an impact on their opportunities or jeopardize future employment. Also, the images that children post online can be taken by others and used for nefarious purposes. A report of American physicians [2] finds that there is a need for parents, pediatricians, and advertisers to protect student privacy online but there also needs to be privacy protection through laws. The students, themselves, need to be aware of digital privacy. Some studies show that young people do care about privacy and want to protect their information [4], [12]. Some but not all school districts can negotiate district purchases of software that include privacy assurances. In other schools, however, teacher innovators use free online apps and may not be aware that the app providers are making a profit from selling the information that they collect from students [10].

The issue of the protection of students' digital privacy is one of concern internationally because internet servers can set third party cookies to allow them to track students' activities and correlate them with their other activities on other sites [1]. The Global Privacy Enforcement Network (GPEN) [1] is a co-operative of privacy regulators with membership from 39 jurisdictions worldwide. In 2017, they conducted a sweep of global privacy risks, focusing on free educational apps that require installation on a mobile device using a social login. They found that "most but not all online services" [1], p. 3 require students to provide their name and email address. Younger students can be asked for their parent or guardian's email address. The regulators at GPEN have published their concerns that this information collection is not transparent to users and could limit their ability to control their personal information. In addition, the social login can link information between the educational service and information students have provided on their social media sites. The public, in general, may not realize that the collection of their information and its sale to third parties is also a large (criminal) industry. Goodman, for example, claims that almost one in five U.S. and European Union citizens have already been victims of identity theft. Medical identity theft costs the U.S. 5.6 billion dollars annually, and the submission of false tax forms to collect equally false tax refunds will cost the U.S an estimated 21 billion dollars over the next five years. Massive amounts of data online, stored in insecure systems, support these crimes [11], and impact digital security and digital privacy.

The internet crosses borders and countries. Increasingly, global think tanks are considering the privacy implications. Frau-Meigs and Hibbard, in a 2016 paper for the Global Commission on Internet Governance (GCIC), argue that internet governance in education is needed because children and youth are using the internet for everyday life and they need protection to build healthy, positive relationships with respect to internet use [13]. They emphasize that children have the right to privacy, security, and dignity when online. Children also have the *right to be forgotten*, meaning that there should be mechanisms to remove online traces of children. Frau-Meigs and Hibbard encourage more corporate social responsibility from service providers leading them to include provisions to ensure children's safety when they access the internet and when it is used for educational purposes.

Web 2.0 is generally thought of as the interactive web, where content is not just accessed but also generated. In comparison, Web 3.0 is often called the semantic or intelligent web that has improved personalization features. Frau-Meigs and Hibbard [13] propose a reconsideration of Web 2.0 and 3.0. They see Internet 2.0 as *a tool* and Internet 3.0 as *an environment*. They also see that education 3.0 can build children's competencies in participation, co-operation, creativity, and social intervention. While they concur that age-sensitive

regulation of digital privacy is important, they also argue that children should be empowered to be the actors and not just the subjects of policies. They need to become educated online consumers. They make three recommendations in the area of media and internet literacy for schools since "the decision-making bodies for education" do not understand these media and internet literacy skills [13], p.5. First, they recommend a national Education 3.0 curriculum that crosses continents as a core discipline. Second, they recommend recognition of a level of autonomy and empowerment for students who use the internet, because they have higher agency online than offline. Finally, they recommend the creation of national, regional, and global internet governance spaces that include and secure the interests of some of the stakeholders long thought to be vulnerable and in need of protection: the students [13].

In summary, research indicates that the student use of online applications in schools is a significant issue, both because of student supervision online but also for the protection of students' digital privacy. These important issues require education for teachers, students, and parents to mitigate the risks. There are calls from numerous sources [8], [10], [13] for appropriate policy responses to protect the students.

3. METHODOLOGY: POLICY ANALYSIS

Policy studies in education, according to Delaney [14], examine what is happening with a specific topic, including positives, negatives, concerns, and issues. He argues that *policy analysis* in education should put the people at the center of educational policy considerations [14]. In this section, the authors analyze policy responses to the issue of digital privacy from the perspective of the students, adult caregivers, and federal agencies in digital privacy protection.

Policy analysis in the case of digital privacy involves detailed research to locate definitions of key terms related to digital privacy; an examination of how policies are designed to solve digital privacy problems and guide actions; and comparisons of how different nations are addressing digital privacy through policy responses. Lavis [15] creates three scenarios for policy development. In the first scenario (Scenario A, below), the processes of research and public policy- making are "often distinct, and typically asynchronous" (p.39). It can happen that research evidence will appear just as a policy is being designed (Scenario B, below) but this is rare. Scenario C (below) indicates that, when the research process and the policy design process are purposefully linked, then researchers can "push" an agenda to bring it to the attention of policy makers. The researchers or intermediary groups identify and synthesize relevant research evidence. Possibly, the policy makers can ask to see the evidence. Ideally, the knowledge translation process in Scenario C is interactive, and characterized by "high-quality, locally applicable research evidence" [15], p.41.

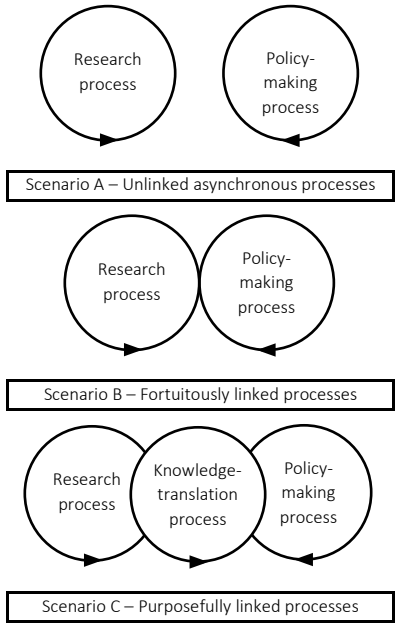

Figure 1: Research, policy and knowledge translation [15], p.40.

The authors sought to locate policies and legislation that would resemble Lavis' Scenario C, seeking jurisdictional policies that took into account the research into digital privacy and then advanced policies toward *digital privacy risk abatement.* Representative policies were sought, first in Canada, then in the U.S., and then internationally. The list of policies reviewed for their responsiveness to the issues identified in the research is intended to be illustrative of the present approaches across nations rather than comprehensive.

In Canada, The *Office of the Privacy Commissioner* made recommendations to protect the online privacy of Canadian children in 2008 [16]. Aware of the increasing frequency with which Canadian students were using technology in and out of school, the Commissioner urged providers of child-specific content to ensure that students visiting these sites could read and understand the terms of use. Currently, the Privacy Commissioner website focuses on two aspects of online activity in youth: personal information protection and online identity and reputation. No legislation, however, has been presented in Canada, leaving children's privacy largely unprotected as it relates to educational content and policy.

Canada has devolved responsibility for education to the provinces and territories. In Ontario, municipalities and cities oversee the protection of personal information. The *Municipal Freedom of Information and Right to Privacy Act* (MFIPPA) [17] defines *personal information* as recorded information that can be used to find someone's identity. This *recorded information* about an individual includes the following areas and more: race, origin, religion, age, gender, sexual orientation, or marital status; b) educational, medical, psychiatric, criminal, or employment history; c) any identifying number or symbol;

d) address, telephone, fingerprints, blood type, and name. There is little to indicate that MFIPPA has been updated to the digital realm, although it does acknowledge that a record could be electronic (p.3). MFIPPA states that institutions shall not use personal information in their custody (S. 31) unless they have consent. The Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) [18] establishes privacy laws for the private sector and has established ten principles of fair information practices. These include, for example, *Notice* that information is being collected*; Choice* for users to opt in; and disclosure of the *Purpose* for collecting the information [18].

In comparison, the American *Children's Online Privacy Protection Rule* (COPPA) designates the age of 13 as the minimum age to have an online profile [19]. This legislation was designed to protect young internet users, but recent research shows that there are many under-age users on the internet, raising questions about whether or not legislation is the answer [20]. According to a Common Sense Media report in the U.S., computer use is "pervasive" among children, as half of 2-4-year olds have used a computer, as well as 90% of 5- to 8-year olds [21], p.9. Another policy in the U.S., the *Family Educational Rights and Privacy Act* (FERPA), requires schools to have written permission from the parent or caregiver to release any information about a student's educational record [22]. A third U.S. policy example emerges from California where the *Shine the Light* law requires list brokerages to tell people on request where they have sold their personal information [23]. To the best of our knowledge, there is no parallel national Canadian legislation to protect children and adolescents with respect to online privacy in schools. The school districts or school authorities in Canada report to the provincial ministries of education. Recently, the Privacy Commissioner of Ontario suggested that if national legislation is not forthcoming, the responsibility for privacy protection may be legislated locally.

One province in Canada, Ontario, has written a policy that holds students accountable for their online activities if they impact other students negatively. *Bill 13: The Accepting Schools Act* [24] requires schools to address harassment, bullying, and discrimination using a number of interventions that include suspension and expulsion. Specifically, it identifies cyberbullying behaviours such as the online impersonation of others, and makes digital bullies subject to the consequences enacted in the legislation, including suspensions, expulsions, and police intervention. While the scope and sanctions of the *Accepting Schools Act* have given schools the authority to respond to cyber bullying and online aggression, it does not focus on or include language that develops the digital citizenship of students. It does not address the professional development of teachers who, five years after its assent, now teach students who are even more immersed in the technologies that can lead to school-based consequences.

A review of the curriculum policy approaches to digital citizenship across Canada reveals a very broken curriculum policy front [3]. Each ministry of education uses different terminology. The British Columbia curriculum has a framework for digital literacy that is used also by the Yukon. Alberta has a framework for student learning which includes the ethically responsible use of technology. Saskatchewan uses the term digital fluency. Manitoba has a model for Information and Communications Technology (ICT) across the curriculum that includes ethical and responsible use. Ontario has a scattered approach across curriculum policies where one curriculum discusses cyberbullying and another digital privacy but overall does not mention digital citizenship. Quebec students are to use ICT with critical judgement. The Maritime provinces discuss technological literacy, and the Northwest Territories and Nunavut promote the ethical use of ICT with a technology in education framework that also does not mention digital citizenship [3]. What is missing from these are common terminology and a coherent set of national standards to manage student digital privacy.

The authors examined current Ontario curriculum policy for mentions of digital privacy. The definition of *digital footprint* occurs in the 2018 *Canadian and World Studies Grades* curriculum, in the glossary. It defines *digital footprint* as, "A trail of information a person leaves when using digital devices. It enables third parties to access data such as an individual's Internet Protocol (IP) address, the Internet sites that person has visited, and comments he or she has made" [25], p.182. Digital privacy is not in the curriculum outcomes. This represents a missed opportunity for student education about digital citizenship and digital privacy. Similarly, the *Social Studies* (1-6) curriculum (2013) promotes an educational framework of citizenship without mentioning digital citizenship [26]. Internet privacy is mentioned once in the secondary school Grades 9-10 *English* curriculum, encouraging all students to be aware of internet privacy issues, safety, and responsible use, particularly when technology promotes hatred [27]. This policy analysis indicates that information about digital privacy is scarce and appears in the secondary school curriculum almost a decade after the research indicates that children are online [21]. In general, we find it concerning that the Ontario Curriculum, which is the curriculum policy in Canada's most populous province, does not address digital citizenship and digital privacy in a responsive, responsible, or coherent way.

Chen, examining the digital divide in Ontario schools, notes that, "to date there is no national policy on digital learning in place" in Canada [28], (p.4). Without a systematic approach to digital learning, the school districts are left to define ICT curricula on their own. He finds also that public schools in Ontario provide almost universal (99%) access to computers at school. He adapts a framework for theorizing the digital divide that shows the levels at which the divide occurs. The first level includes the have and have not schools, where the digital divide is associated with hardware and internet access. At the second level, there are digital divides because some teachers and students are using technology while others are not. The third level of the digital divide represents whether or not students use devices at home for their learning [28].

In summary, then, the authors' analysis of representative legislation and curriculum policies indicates that, while both the U.S. and Canada have national agencies to protect digital privacy for the general public, the legislation in the U.S. more specifically targets the protection of digital privacy for young people of vulnerable ages. The efficacy of the U.S. legislation has come into question in light of the data indicating the age of first technology use [21], but there is, at a minimum, some U.S. national policy response. Advocates for children argue that they should be educated on digital citizenship regardless of the legislation and that, in fact, firewalls are not the answer if you want to build an informed citizenry [12]. Some advocate that youth should be involved in the design of internet privacy policies [13].

Our review of the Canadian curriculum policies, with a focus on Ontario, indicates that students and teachers need a more robust, coherent, and well-articulated curriculum policy regarding digital privacy for students of all ages. Given findings such as those reported by Chen [28] and Leatham [29], students are frequently using digital technology in schools. This lack of curriculum policy is a clear gap that needs to be addressed. The curriculum should be combined with digital privacy protection policies to support schools. There is also a lack of clarity surrounding who has jurisdiction to create policies to protect students' digital privacy. Finally, our review finds that clear strategies for digital risk abatement based on fundamental privacy principles are non-existent.

4. SUMMARY OF FINDINGS

This critical policy analysis of representative American and Canadian education policy finds gaps between research that identifies a clear need to address students' digital privacy and the development of responsive policies. This overall finding aligns with Lavis' Scenario A [15], where policy and research are asynchronous processes. The authors find that policies are not being created to align with findings about the need to protect student privacy during their online activities.

A second gap is the *innovation-policy gap* [30] between the technology innovators and education policy designers. These gaps in policy leave schools to fend for themselves in creating guidelines for digital supervision. This has implications for teachers who are assuming, increasingly, the responsibility of supervision of students in digital landscapes. The traditional physical classroom is yielding to digital equivalents such as Google classroom and Wikispaces. These spaces, which are the de facto classrooms for an increasing number of students, are outside of the regulatory influence of earlier policies. Many educational jurisdictions require students to be working toward global competencies using technology. In order to align students' needs as defined by research, educational policy-makers need to mandate the teaching of the appropriate and responsible use of technology. Policies that identify the importance of the use of ICT without consideration of access, privacy, digital supervision, digital citizenship, and risk abatement, are not putting their students at the center of their policy considerations.

5. CONCLUSION AND RECOMMENDATIONS

The authors conclude with the following recommendations with respect to research, policy, legislation and education:

Research: We need to understand the best practices of teachers who supervise students online. High-quality research and publications will mobilize knowledge surrounding risk abatement and support more relevant curriculum policy development in a digital era. There is also a dearth of research on the teaching of digital citizenship and its effectiveness. These are significant gaps.

Policy: All nations should create policy to protect the digital privacy and digital footprints of its youngest internet participants (as the U.S. has attempted to do). Without the existence of policies that protect students' PII and develop students as digital citizens mindful of their digital footprints, parents, teachers, and district school boards will continue to assume the responsibility for student protection in a scattered and piecemeal way.

Legislation: Canadian students need more support to protect their privacy. The fair information practices in PIPEDA [18] could apply to education and students' PII protection. Students should not be required to sign ToS agreements that are too complicated to understand. The data of young people should not be vulnerable to list brokerage. These types of protections are offered in the U.S.'s *Family Educational Rights and Privacy Act* (FERPA) [22]. There should be strict (federal/international) limits on third-party sharing and resale of data with respect to education. District school boards should have protection from the resale of data when they agree to allow teachers and schools to use online applications.

Education: At a minimum, students who are accessing the internet on their own need to understand that parents and caregivers must review ToS agreements. Students need to consider the impact of online decisions they make and post today while also bearing in mind the future citizens and employees they will become. They should be made aware of the presence of their digital footprints and the potential sale of their personal information to third parties. Students should understand the risks associated with digital permanence and the possible ramifications of over-sharing or assuming anonymity while online. Rather than encouraging school boards to provide all of the filters, students, parents, and teachers need to be empowered to manage their online information and provide models of digital citizenship for children. Digital literacy and digital citizenship should be required courses to help students take responsibility for their digital presence. Resources are needed to assist teachers, students, and parents in accomplishing this task.

Our policy analysis reveals gaps between innovative technologies and responsive educational policies. We need to make the time to protect the digital privacy of students, families, teachers, and schools. In a cyber-world characterized by anonymity, we are called to know where our children are and whether or not they are working online in safe environments.

6. REFERENCES

[1] The Global Privacy Enforcement Network (GPEN) (2017). Online educational services. Retrieved @ https://www.ipc.on.ca/resource/2017-gpen-sweep-report-online-educational-services/

[2] O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4),800-804.Retrieved@ http://pediatrics.aappublications.org/content/127/4/800

[3] Hoechsmann, M., & DeWaard, H. (2015). Mapping Digital Literacy Policy and Practice in the Canadian Education Landscape: MediaSmarts. Retrieved @ http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/mapping-digital-literacy.pdf

[4] Steeves, V. (2014). Young Canadians in a wired world. Phase III: Life online. Ottawa, Canada: MediaSmarts. Retrieved @ http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf

[5] Canadian Internet Registration Authority (CIRA) (2017). Retrieved 9/23/2017@ https://cira.ca/factbook/domain-industry-data-and-canadian-Internet-trends/internet-use-canada

[6]Internetlivestats.com http://www.internetlivestats.com/internet-users/canada/

[7] Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. Retrieved @ www.lse.ac.uk/EUKidsOnlineFinalReport

[8] Sisk, E. P. (2016). Technical Difficulties: Protecting Privacy Rights in the Digital Age. *New Eng. J. on Crim. & Civ. Confinement*, *42*, 101.

[9] Stoddart, J. (2011). Address by Jennifer Stoddart to the Supreme Court of British Columbia Education Seminar. Retrieved @https://www.priv.gc.ca/en/opc-news/speeches/2011/spd_20111109/

[10] Berson, I. R., & Berson, M. J. (2006). Children and their digital dossiers: Lessons in privacy rights in the digital age. *International Journal of Social Education*, *21*(1), 135-147.

[11] Goodman, M. (2015). *Future crimes. Inside the digital underground and the battle for our connected world*. USA: Anchor Canada.

[12] Palfrey, J. G., Gasser, U. and boyd (2010). Response to FCC notice of inquiry 09-94: Empowering parents and protecting children in an evolving media landscape. https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Palfrey_Gasser_boyd_response_to_FCC_NOI_09-94_Feb2010.pdf

[13] Frau-Meigs, D. and Hibbard, L. (2016). Education 3.0 and Internet Governance: A New Global Alliance for Children and Young People's Sustainable Digital Development. Retrieved @https://www.cigionline.org/sites/default/files/gcig_no27web_0.pdf

[14] Delaney, J.G. (2017). *Education policy: bridging the divide between theory and practice*. Canada: Brush Education.

[15] Lavis, J. N. (2006). Research, public policymaking, and knowledge-translation processes: Canadian efforts to build bridges. *Journal of Continuing Education in the Health Professions*, *26*(1), 37-45.

[16] Office of the Privacy Commissioner of Canada. *Reflections on Reform of the Federal Privacy Act* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_r/pa_ref_df/

[17] The Municipal Freedom of Information and the Protection of Privacy Act, (MFIPPA) R.S.O. 1990, c. M.56. Retrieved @ https://www.ontario.ca/laws/statute/90m56

[18] The Personal Information Protection and Electronic Documents Act (PIPEDA). Retrieved @ http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[19] Federal Trade Commission (1998). Children's Online Privacy Protection Rule (COPPA). Retrieved @ https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[20] Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. *First Monday*, *16*(11).

[21] Holloway, D., Green, L., & Livingstone, S. (2013). Zero to eight: Young children and their internet use. Retrieved @ http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

[22] U.S. Department of Education (1974). the Family Educational Rights and Privacy Act (FERPA). Retrieved @ https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[23] Electronic Privacy Information Centre: California S. G. 27, "Shine the Light" law. Retrieved 9/24/2017@ https://epic.org/privacy/profiling/sb27.html

[24] The Accepting Schools Act, Legislative Assembly of Ontario, 2012. Retrieved 9/24/2017@ http://ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=2549

[25] Ontario Ministry of Education. (2018). *The Ontario curriculum grades 9-10: Canadian and World Studies 1-8: Health and physical education*. Retrieved @ http://www.edu.gov.on.ca/eng/curriculum/secondary/canworld910curr2018.pdf

[26] Ontario Ministry of Education. (2013). The Ontario curriculum Social Studies Grades 1-6, History and Geography d @ http://www.edu.gov.on.ca/eng/curriculum/elementary/sshg18curr2013

[27] Ontario Ministry of Education (2007). The Ontario curriculum English.http://www.edu.gov.on.ca/eng/curriculum/secondary/english910currb.pdf

[28] Chen, B. (2015). Exploring the Digital Divide: The Use of Digital Technologies in Ontario Public Schools. Retrieved @https://www.cjlt.ca/index.php/cjlt/article/view/26970

[29] Leatham, H. (2017). *Digital privacy in the classroom: an analysis of the intent and realization of Ontario policy in context* (Doctoral dissertation). Retrieved @ https://ir.library.dc-uoit.ca/xmlui/bitstream/handle/10155/816/Leatham_Heather.pdf?sequence=1

[30] Davis, K. (2014). Bridging the innovation-policy gap. *SAIS Review of International Affairs*, *34* (1), 87-92. doi: https://doi.org/10.1353/sais.2014.0015