

# Student Digital Privacy in Classrooms: Teachers in the Cross-currents of Technology Imperatives

Heather Leatham<sup>1</sup>, Lorayne Robertson<sup>2</sup>

<sup>1</sup>*York Region District School Board, Aurora, Ontario, Canada*

<sup>2</sup>*University of Ontario Institute of Technology, Ontario, Canada*

## Abstract

*Digital tools are beginning to be more commonplace within the K-12 classroom setting, but with these new opportunities through improved digital access, there are also risks that are associated with protecting the privacy of student information. When students are online, they leave a digital footprint that may contain personally-identifiable information. The present study examines policies in Ontario, Canada with respect to the use of digital tools in classrooms. A survey was sent to teachers in one district school board and more than 400 teachers responded. The teacher responses indicate that there is a policy gap surrounding digital tool use and privacy in Ontario schools. This has caught the early adopters of technology innovation, in particular, within the cross-currents of competing imperatives. District school boards are encouraging teachers to use technology, communicate with parents, and be innovative, but there may be insufficient privacy policies in place to protect the teachers and students. This study's findings and policy analysis lead to recommendations for district school boards to provide policies to protect student and teacher information in online settings.*

## 1. Introduction

Classrooms have employed learning tools such as textbooks for centuries but digital tools are a relatively new phenomenon in K-12 classrooms. The research reported here takes place in Ontario, Canada in a mid-sized district school board of under 15,000 students. The focus of the research is on the use of digital tools in classrooms, which are defined as internet-connected tools that require students to have an account in order to proceed [1]. This definition encompasses, for example, web-based applications, iPad/Android apps, smartphone apps and Learning Management Systems (LMS). Some commonly used classroom digital tools also include parent notification apps such as Remind, the Google Suite for Education, and social media. A key component of digital tool use is that, in order to

participate using the digital tool, students need to provide some basic information and log in online.

Some digital tool use does not have implications for the protection of student privacy or the protection of student information. For example, when Seymour Papert showed his Logo programming language to students in the 1960's, there were no pressing concerns for disclosing student information through online applications. Since then, however, schools have expanded student access to computers, software, hand-held devices and to online applications in order to enhance their learning [2].

Current Web 2.0 digital tools are interactive tools which are responsive to student input and deliver differentiated programming. The proliferation of new apps is impressive. Between July 2008 and December 2009, approximately 150,000 apps were released on iTunes, which averaged up to 275 apps per day [3]. As of May 2017, there were an astounding 2.2 million apps in the Apple iTunes store [3], under which there is a specific section just for education.

Teachers learn about these apps through multiple ways such as: Twitter, their professional associations, at conferences, and by word of mouth. When these apps are advertised to teachers, they may or may not include specific information regarding how the online app protects student data or leaves student data vulnerable to collection through third party providers.

Much of the present education literature focuses on why and how to use digital tools in the classroom without a matching focus on protecting student privacy (See for example: [4]; [5]; [6]). As soon as a digital tool is connected to the internet, however, issues with the protection of student identity can emerge, and these concerns are particularly important if the designers of the application hold third-party rights to the student log-in information.

The research presented in this paper is one part of a larger study [7] where the researchers surveyed teachers in an average mid-sized district school board in Ontario to ask if they were using digital tools, to gauge teachers' perceptions about digital privacy policy, and to ask teachers how they were protecting the privacy of students' personally-identifiable information or PII.

The findings with respect to these two aspects: digital tools and privacy, indicate that teachers are trying to operate within an overall system that encourages teachers to engage their students with online technology tools but at the same time, wants the teachers to protect student information while this is happening. What is even more pressing, however, are the present study's findings that teachers are receiving multiple, mixed messages about privacy in policies, making it more challenging for them to protect student information while using digital tools. Teachers, and in particular, early adopters appear to be caught in the cross-currents of multiple and almost contradictory technology imperatives. The sections which follow outline these multiple pressure currents and policies that are directing technology and digital privacy implementation in more detail.

In Ontario, curriculum policy is presented in subject-specific curriculum documents for the most part. There are, in addition, some broad accompanying policies guiding K-12 programming, planning and assessment for the close to 2 million students in Ontario's 76 district school boards. These policies advocate philosophically for technology integration across subjects but there is no central guideline or policy to help teachers select digital tools. This leaves teachers without guidance to determine the suitability of an app, specifically if its use might, in some way compromise digital privacy. In some district school boards, the selection of digital tools is managed centrally and this takes the burden from the teacher to determine if an app presents a risk to the release of student information to a third-party vendor. In other school boards, however, the teachers make the selection of the digital tools based on the most current policy information that is available.

What has happened with the proliferation of the availability of digital tools is that the development of the apps has out-paced matching policy development to protect students' PII. This is an example of a *policy-innovation gap* [8]. It is precisely this lag between the technology introduction and the development of policy that leaves educators in limbo, particularly the early adopters [9]. The present legislation with respect to the protection of the privacy of student information was written earlier during the era of print media. Digital privacy protection is new territory for schools. Based on findings from the research cited here, the authors offer some potential solutions and recommendations to assist teachers with this policy gap.

In summary then, this paper defines digital privacy, analyzes relevant Ontario educational policies on digital privacy, and based on teacher responses to a survey on digital tool use, makes recommendations for educators to help teachers

navigate the cross-currents of tech innovation despite the gaps in correspondingly responsive policy on digital privacy.

A digital footprint is composed of the traces of information left on the internet after a user goes to any website, or uses any app. While a user may deliberately give away some PII, for example, when signing up for an account, other information can be collected passively without the user's knowledge. Many people are unaware of the size of their footprint, as users use more and more mobile apps in their daily lives [10]. Whether a person (deliberately or not) shares PII with a website or mobile app, their information is out there and being added to their footprint. Important to the discussion on student digital privacy is the fact that the information being asked for when creating accounts, asks for *protected* PII. The sharing of PII can leave students open to activities such as identity theft, hacking, and geotracking [11], or as Madden, Fox, Smith and Vitak point out, commercial purposes [10]. When using digital tools in the classroom without a clear policy or guidelines on how to protect PII, teachers may be giving away students' PII and increasing students' digital footprints in order for them to participate and learn.

The paradox that exists with the increase in the use of digital tools, smartphones, and digital devices is that of privacy. Whereas users are drawn to digital tools that will shorten, lessen, or make any task easier, users also profess to be concerned over the protection of their privacy. The convenience that the digital tool provides usually outweighs any concerns the user has about privacy [12]. This *privacy paradox*, examined by Norberg, Horne and Horne, finds that people are "cavalier in the protection of their own data profiles" [13] p.10. Within the scope of education, this paradox seems to exist as teachers search for apps to help students learn, be more engaged or to lessen the teachers' daily tasks. These educational apps are touted on Twitter, reviewed in the Ontario College of Teachers *Professionally Speaking* magazine, and presented at professional or educational technology conferences. Yet the topic of protecting student PII is hardly mentioned in the reviews of the apps. Therefore, teachers become part of the paradox in that they know that they are supposed to protect student PII yet they are willing to forego it if the app can be useful in their practice.

To understand digital privacy, an understanding of privacy overall is needed. Privacy is defined as "the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone" [14]. Gülsoy describes digital privacy as "the right to privacy of users of digital media" [15]. In other words, privacy

is a right that needs to be recognized in legislation, and both *loss of control* and *intrusion* are components of breaches of digital privacy. Gülsoy states that, “Digital media raise such concerns for users as unpermitted use of personal information gathered from users’ on-line activities and unpermitted release of that information to third parties” [15].

Bélanger and Crossler use the term *information privacy*, stating that, “personal communication privacy and data privacy can be merged into the construct of information privacy” [16]. These terms are taken from the four dimensions identified by Clarke, which also include privacy of a person and personal behavior privacy [17]. Bélanger and Crossler state also that many of the definitions of information privacy include an aspect of *control* over the individual’s information [16]. Leatham states that, “Digital privacy can be understood as the state of having control over what online personal data can be protected from intrusions from unwanted third-parties” [1].

Many jurisdictions had privacy protection policies in place prior to the advent of the internet. In Ontario, Canada, for example, educators and others are bound by the Municipal Freedom of Information and Protection of Privacy Act [18] which identifies what constitutes PII. Significantly, PII cannot be given out without the individual’s consent. These elements of PII include: name, age, colour, religion, sex, and any identifying number or address [18] (Sec. 28). Teachers might easily use students’ names, images or identifying numbers such as student numbers without realizing that they are not protecting students’ PII. What MFIPPA legislation does not do, however, is extend into the online world. This creates a policy gap for teachers because the policies on the protection of personal information have not been fully developed for digital applications and these digital policies have not been made available to teachers.

## 2. Policy Analysis: Ontario Education

The research methodology described here for this study has two components. The first is policy analysis. The second is a survey of teachers in one district school board. The policy analysis is described first.

Policies are designed to solve public problems, and analysis of policies is essential to improve the quality of our public policies [19]. There are many ways that policy analysis can take place. Among these are: the monitoring of the policy, evaluating the policy, analyzing the policy discourse, and forecasting [19]. In the case of the research that is described here, the authors chose certain policies

which were reflected of broad curriculum policies in Ontario as well as recent curriculum policies. In the analysis of the policies, the researchers sought key words in the policies and then examined carefully the context in which these words were used.

Education in Canada is not controlled federally. Instead, each of the 13 provinces and territories are responsible for their education laws. The province of Ontario where the study reported here takes place is governed by an Education Act [20], which includes various acts including the Ontario College of Teachers Act (1996) [21] and other addenda to the Education Act such as Codes of Conduct. Procedures for these additions to the Education Act can be communicated to district school boards through a mechanism known as a Policy Program Memorandum. Each of these different sources and types of policy are examined here as they pertain to digital privacy and technology use in Ontario schools.

### 2.1. Education Act

The Education Act in Ontario [20] is a public policy, enacted by the provincial government. As a policy, it meets Fowler’s definition that policy is “a government’s expressed intentions and official enactments as well as its consistent patterns of activity and inactivity” [19]. In Ontario, the Education Act is considered permissive legislation. It tells district school boards what they can do more than what they cannot do. The Education Act instructs district school boards regarding their management, including sections which outline the key responsibilities for school leaders and teachers.

A detailed analysis of the Education Act (1990) reveals indications that there is an *implementation-policy gap* with respect to technology. Within the Act, the word *technology* appears infrequently and when the word is used, it is only with respect to post-secondary career destinations (e.g., Sec.49.2 (6.2); 171.1(44); 189.2). Other computer-related words such as ‘online’ and ‘digital’ do not appear in the legislation. The word ‘computers’ appears only in relation to the rights of school districts to make purchases or acquisitions and not with respect to the use of the computers. This is another indication of an *innovation-policy gap* as the over-arching educational policy for the province does not reflect the current state of online education in Ontario schools.

Evidence indicates that the policy is inconsistent with practice. According to a MediaSmarts survey, the use of computers for both instruction and learning is commonplace in Ontario schools [22]. For example, the Ministry of Education promotes the use of technology within the classroom with their partnership with the Council of Directors of

Education on the Technology Learning Fund grant which is directed towards “increasing technology-enabled pedagogical practices” [23].

Importantly, within the Education Act [20] *privacy* is mentioned in sec. 266.2 in relation to PII, stating that privacy is defined by both MFIPPA and the Freedom of Information and Protection of Privacy Act (FIPPA). The Education Act does not differentiate, however, whether PII needs to be addressed differently in the online world from the physical world, nor does it specify the contexts where privacy needs to be protected.

## 2.1 Ontario College of Teachers

The Ontario College of Teachers (OCT) [21] is the regulatory body for all teachers within the province. This includes licensing, publishing advisories, and taking punitive measures against teachers who contravene the Professional Standards of the OCT. The term, “technology” is addressed within the OCT Standards of Practice as it pertains to teachers’ use of technology, stating that teachers will “use appropriate pedagogy, assessment and evaluation, resources and technology in planning for and responding to the needs of individual students and learning communities.” This represents pressure from the Standards of Practice for teachers to use technology, yet the OCT does not advise teachers how to evaluate educational technology for its appropriateness or for the ways that it may or may not protect student privacy.

On the subject of *privacy*, the OCT addresses student information within their Professional Advisory on the *Use of Electronic Communication and Social Media* [24]. This advisory mentions in two different sections that teachers should “respect the privacy and confidentiality of student information” and that criminal and/or civil law implications exist if teachers are “disclosing confidential information about the school, students and colleagues, thus breaching workplace privacy policies and provisions of the *Education Act*.” The professional advisory references only the Education Act [20] and not MFIPPA [18] in relation to privacy.

Once again, the policy landscape here lacks helpful specifics for teachers. It does not define personally-identifiable information, nor does it define what information needs to be protected. Also, what is lacking is an advisory specifically as it pertains to the use of digital tools in the classroom and the protection of student privacy.

To further add to the complications of an already muddled landscape, the College of Teachers communicates with their members through the publication of a quarterly magazine, *Professionally*

*Speaking*. Each issue of this magazine contains a section entitled “Apps Analysis” where digital tools, mainly apps, are featured and profiled for teacher use in the classroom. The review of the app includes the age- appropriateness of the app and its cost *but not the protection of student privacy considerations associated with the app* [25]. Because the College of Teachers publishes the magazine, teachers who are reading it may assume that the apps listed are generally compliant with district policies on app use, and with provincial policies on the protection of PII. Based on the source of the information, teachers may not have any qualms or hesitation about installing the apps. If the teachers did install these apps, however, they would be once again on a slippery slope if they introduced and employed apps which do not provide protection from third-party access to student information.

For these reasons, we find in our policy analysis that teachers are caught in cross-currents which encourage them to use technology yet provide little support with respect to policy to protect students’ digital privacy. When the teachers implement technology, they need policy guidance or they are figuratively and quite literally set adrift without legislation that should be protecting both students and teachers.

## 2.3. Codes of conduct

The digital world has not been completely forgotten in the development of Ontario legislation, however. Ontario district school boards are mandated to establish Codes of Conduct that include the seven purposes which form the provincial Code of Conduct through section 301 of the Education Act [20]. A procedural form of this legislation is provided in Program/Policy Memoranda 128 (PPM) which outlines guidelines for Safe School procedures <http://www.edu.gov.on.ca/extra/eng/ppm/128.pdf>. While this PPM does not specifically mention *privacy*, it does include one digital aspect, cyber-bullying, as a type of inappropriate behavior. The majority of the context of this Safe School program memorandum is, however, the physical world and not the online world.

## 2.4. Privacy management officials

One body in Ontario has taken it upon themselves to address the lack of policy on the use of digital tools in the classroom. The Ontario Association of School Board Officials (OASBO) [26] has published a video entitled *Understanding Privacy Considerations* (<http://www.pimedu.org/videos>

boardstaff.html). This video explains the process for determining approved digital tools. OASBO is acting independently of an established Ontario Ministry of Education policy with their videos, though they are part of Privacy Information Management which enforces MFIPPA [18]. The video is from what Ball would describe as a policy source that has a “certain voice...authoritative” [27], as school boards are members of OASBO, which has as an objective to “advise and assist the various Ministries of the provincial Government and other organizations in promoting the interest and management of the education systems in Ontario” [26].

## 2.5. The role of school administrators

School administrators are instrumental in developing policy, defining it and implementing it [19];[28]. Administrators are the agents of the governing authority, tasked with creating the rules and regulations within their schools that correspond to policy, such as, for example Codes of Conduct. According to Fowler, a knowledge of the political landscape, of issues that do and can affect education, is a key item for administrators so they are not caught off-guard by new policies. Fowler also states that administrators can also be at the forefront of influencing policy through various local and state groups or agencies [19]. The role of the school administrator in supporting digital privacy policy is not a role that has been delineated in a significant way in the literature. This represents another missed opportunity with respect to digital privacy.

The table below summarizes the key roles of school administrators as policy actors. According to Fowler,

- ✓ The role of an administrator in policy work is the implementation at a school level of policy received from a governing authority.
- ✓ As a policy maker: the school leader knows the policy process in order to create rules and regulations to respond to needs;
- ✓ As a policy implementer: school leaders are expected to carry out policy and motivate teachers to cooperate with the policy;
- ✓ As followers of policy issues: school leaders identify major social and economic issues; and stay informed;
- ✓ As influencers of policy: school leaders exert influence on the level above to create, modify or protest policy [18].

According to Ball et al., the role of a school administrator is:

- ✓ As a policy actor: to move between roles;
- ✓ As a policy narrator: to interpret and enforce policy;

- ✓ As a policy transactor: to monitor and report on policies;
- ✓ As a policy implementer: to work with others to merge policies together into a coherent plan for ‘improvement’ [28].

In addition to these key policy roles for school administrators, we suggest that there is also a role for school leaders to identify when there are policy gaps and contradictions, and they need to advocate for students, teachers, and schools. Teachers look to their school leaders to help them understand legislation and to identify the ways forward when there are policy contradictions or gaps.

## 2.6. Curriculum Policy

The overall, curriculum policy for the province is the *Ontario Schools Kindergarten to Grade 12: Policy and Program Requirements* [29]. This policy states that teachers are to include technology within their pedagogy and that this technology needs to “align with ministry and board policy and initiatives”. In Ontario, curriculum policy is generally distributed to two panels: elementary (grades kindergarten to 8) and secondary (grades 9 through 12). Each subject has its own set of curriculum policies which include a philosophical front matter, and overall and specific learning objectives by strands. Though curriculum policies proceed through a revision cycle, there is clear evidence of an *innovation-policy gap* in terms of the promotion of the use of technology in the classroom, and the policies necessary for teachers to protect student digital privacy. Fowler, cited earlier, explains that *evidence of inactivity* is also a key aspect of policy analysis which can also include discursive analysis to determine the emphasis placed on key terms or discourses, or the lack of written policy to address a public problem [19].

The philosophical front matter of the new Ontario curriculum policies contains a reference to suggest that teachers should integrate technology. This section of the policy also details the types of *information and communications technology* which teachers could use for teaching, and students could use to support and communicate their learning. Teachers are advised that “there are potential risks attached to” the use of the Internet and that “all students must be made aware of issues related to Internet privacy, safety, and responsible use” [30]. This section of the policy does not advise teachers on how to protect student privacy. It also does not offer suggestions in terms of websites, digital tool evaluation or instructions for teachers on the protection of student PII. Even though this curriculum is from 2014, it still references digital

tools such as CD-ROMs which do not exist on many newer computers and does reflect the reality of the popularity of tablets and Chromebooks being used presently in Ontario schools [31].

A more current curriculum policy, *The Ontario curriculum grades 1-8: Health and Physical education* [32] contains references to digital privacy, including prompts for teachers to initiate discussions about digital privacy. However, the prompts refer to student use of cell phones, and the hazards of sexting and cyberbullying. Here again, there is a missed opportunity to address the protection of student PII when using digital tools, and there is a lack of a clear procedure for choosing appropriate digital tools that will not leave student information vulnerable.

In summary then, this brief but focused policy analysis reveals that there are several significant policy gaps in the Ontario landscape with respect to the absence of the legislation on the topics of technology implementation and the protection of students' digital privacy.

### 3. Teacher Survey

The teacher survey described here was part of a larger study. The survey was sent to all teachers in one Ontario district school board, which compromised both urban and rural communities spread over a geographic area of 10,000 km<sup>2</sup>. Of the approximately 1000 potential respondents, there was a return of 404 responses (n=404, or 42% of the district).

The survey was conducted online through Google Forms. It was divided into six sections that included demographic questions, digital tool use, digital privacy and understanding digital privacy. The survey was comprised of both quantitative and qualitative questions in a mixed-methods approach of convergent design.

The purpose of the survey was to ascertain teacher's knowledge of privacy-related policy at both a local district level, as well as at a provincial level. To do so, the survey aimed to understand how digital tool use decisions are made within the classroom, and how the digital privacy of students is being protected when using digital tools. The respondents were evenly distributed with the regions of the district school board, as well as evenly distributed between the two panels (elementary and secondary schools). This demonstrated that the responses garnered were a fairly accurate representation of the district school boards' teachers. Additionally, 64% of respondents were in their first half of an average career of 30 years of teaching, with these teachers ranging in age from 24-39 years of age.

## 4. Findings

### 4.1. Survey findings about digital tool use

In order to understand digital privacy protection, the survey asked about how digital tools were being used in their classrooms, as well as frequency of use. The Google Suite for Education (also known as Google Apps for Education) and the software Smart Notebook (for use with Smart interactive whiteboards) were the most popular digital tools in use. Interestingly, parental communication apps, such as *Remind* and *Seesaw* were popular with 55.5% of respondents indicating they had used them. From the responses, between two to five digital tools were being used by teachers in the classrooms for purposes such as: presentations purposes (75.9%), classroom management (attendance) (71.9%), and creative purposes (67.1%). Overall, the survey indicated a wide variety of digital tools being used in this school district and for a variety of purposes.

### 4.2. Teachers views about digital privacy

This section outlines the findings which were gleaned from the responses of the more than 400 teachers who responded to the survey. Analysis of the survey responses reveals that teachers' understanding of what constitutes digital privacy is not cohesive and it is generally not accurate. Approximately 35% of teachers provided responses to define digital privacy which were deemed accurate/partially accurate. The following words were given when respondents were asked for a definition of digital privacy: *information, access, protect, private* and *share* [1]. Dishearteningly, the remaining 65% of responses fell into the inaccurate category. There were definitions from teachers that indicated a misunderstanding or willful ignorance of digital privacy, such as: *Do not post or print anything you would not say to your [relative] or [religious leader] or to the whole world; an illusory term intended to bolster an [individual's] sense of security, and autonomy.*

When asked how they protect student PII, 62.5% of responses were more specific and considered proactive/protective: *apps only with NO personal info; Apps used have been approved by the board or have been vetted for safety for use with children...we do not use last names...photos and info sharing limited to parents of individual students.*

The responses which indicated a lack of protection included the following examples: *I assume they have their own privacy settings; don't look at*

*what they are doing; clear the history and hope it works.*

Lastly, in relation to awareness of both district school board and/or provincial policies regarding the protection of student digital privacy, 60% of teachers were aware of a district policy, with almost 32% having read it. At the provincial level, 47% of respondents were aware there are policies. Many teachers indicated a specific policy that had been addressed at staff meetings and the need to protect student privacy. Those who had misconceptions about policy gave responses such as: *I think there is a policy but I just use common sense (or best judgement); I assume that iPad use has been approved by the Board as well as the apps.*

## 5. Recommendations

The current Ontario educational policy, as it relates to technology and student digital privacy, demonstrates a clear innovation-policy gap in that policy has not kept pace with the online reality of the schools and classrooms. From an examination of the relevant policies, the following recommendations can be made at various levels of education:

First, an update to MFIPPA should be undertaken to include the context of the online world, and what PII would look like online, and what the protection of PII would look like online. This should then be reflected in the Education Act and trickle down into a revision of other various policies, such as those mentioned in this paper.

Second, a specific policy that addresses digital tools in the classroom, including how to choose them and the privacy concerns that need to be addressed, would give teachers recourse to protect both students and themselves with their choices of digital tools in the classroom. This could appear as a revision to PPM 128, which would then update district Codes of Conduct, or as a new policy program memorandum.

Third, teachers, especially new teachers, rely on the curriculum policies for instructions on student learning outcomes, and, to a certain extent, how to approach the learning program. Part of the curriculum revision cycle could include a more specific section on information and communication technology use in the classroom that takes into account the protection of student privacy, as well as strategies to do so.

This leads into the last recommendation, which is that Faculties of Education need to address the topic and legal obligations with respect to the protection of student PII for pre-service teachers. As pre-service teachers are learning pedagogy as well as digital tools that they could use when they are completing their practicum, they also need to know how to make

informed decisions about the protection of student PII.

If the teachers of today and the preservice teachers of today are working with the students who will be the citizens of tomorrow, the protection of everyone's information and privacy are important concerns that need to be addressed.

## 6. Conclusion

Based on the findings of this one study, some Ontario teachers may feel unprepared to select and implement digital tools in their classroom, but they would feel that there is an expectation to use technology. Despite the reality that technology is in the schools, there are insufficient policies and guidelines to which teachers can refer. Teachers who feel prepared to adopt technology may not consider the implications of their digital tool choice in relation to student digital privacy. An update of various educational policies to be more specific and include the protection of student digital privacy is a recommended first step.

## 7. References

- [1] Leatham, H., (2017). Master's thesis Digital privacy in the classroom: An analysis of the intent and realizations on Ontario policy in context, [in press].
- [2] Boss, S. (February, 2011). *Technology integration: A short history*. Edutopia. <https://www.edutopia.org/technology-integration-history> (Access Date: 25 January, 2017).
- [3] Costello, S., (May 5, 2017). *How many apps are in the App Store?* Lifewire. <https://www.lifewire.com/how-many-apps-in-app-store-2000252>, (Access Date: 25 January, 2017).
- [4] Domingo, M. G., and Garganté, A. B., (2016). Exploring the use of educational technology in primary education: Teachers' perception of mobile technology learning impacts and applications' use in the classroom. *Computers in Human Behavior*, 56, 21-28.
- [5] Jonas-Dwyer, D., Clark, C., Celenza, A. and Siddiqui, Z., (2012). Evaluating apps for learning and teaching. *International Journal of Emerging Technologies in Learning (iJET)*, 7(1), 54-57.
- [6] More, C.M, and Travers, J.C., (2013). What's app with that? Selecting educational apps for young children with disabilities. *Young Exceptional Children*, 16(2), 15-32.
- [7] Robertson, L., Leatham, H., and Corrigan, L., (2018) [in press] An incomplete script: Teachers' understandings of digital privacy. ICSIT Proceedings March 13-16, 2018.

- [8] 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>.
- [9] Rogers, E. M., (2010). *Diffusion of innovations*. Simon and Schuster.
- [10] Madden, M., Fox, S., Smith, A., and Vitak, J., (2007). *Digital footprints: Online identity management and search in the age of transparency* (Report No. 202-415-4500). Washington, D.C: Pew Internet & American Life Project.
- [11] Palfrey, J. and Gasser, U., (2008). *Born Digital: Understanding the first generation of digital natives*. New York: Basic Books.
- [12] Miyazaki, A.D. and Fernandez, A., (2001) Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs* 35(1), 27-44.
- [13] Norberg, P.A., Horne, D.R. and Horne, D.A., (2007). The Privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, Vol. 41(1), 100-126.
- [14] Privacy, (2017). In *dictionary.com*. Retrieved from <http://www.dictionary.com/> (Access Date: 25 January, 2017).
- [15] Gülsoy, T. Y., (2015). Advertising ethics in the social media age. In *Handbook of Research on Effective Advertising Strategies in the Social Media Age* (pp. 321-338). Hershey, PA: IGI Global.
- [16] Bélanger, F., and Crossler, R. E., (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 35(4), 1017-1042.
- [17] Clarke, R. 1999. "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM* (42:2), pp. 60-67.
- [18] The Municipal Freedom of Information and the Protection of Privacy Act, (MFIPPA) R.S.O. 1990, c. M.56.
- [19] Fowler, F., (2004) *Policy Studies for Educational Leaders: An Introduction*. New Jersey: Pearson.
- [20] Education Act, R.S.O. 1990, c. E.2.
- [21] The Ontario College of Teachers Act, S.O. 1996, c.12.
- [22] 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.
- [23] Council of Ontario Directors of Education, (2016). The Technology and Learning Fund, <http://www.ontario-directors.ca/CODE-TLF>, (Access Date: 25 January, 2017).
- [24] Ontario College of Teachers, (2011), Professional Advisory on the Use of Electronic Communication and Social Media <https://www.oct.ca/resources/advisories/use-of-electronic-communication-and-social-media> (Access Date: 25 January, 2017).
- [25] Dubowski, S., (2017, March). Apps Analysis. *Professionally Speaking*, 19. Retrieved from <http://oct-oeo.uberflip.com/i/783423-ps-march-2017>, (Access Date: 25 January, 2017).
- [26] Ontario Association of School Business Officials. [Ontario OASBO]. (2016, February 5). *Webcast 3: Understanding Privacy Considerations (Videos for School Board Staff)* [Video file], <https://www.youtube.com/watch?v=xq5K1wSfmeE> (Access Date: 25 January, 2017).
- [27] Ball, S. (1994). What is Policy? Text, trajectories and toolboxes. In Ball, S. (Ed.) *Education Reform* (pp.14-27). Buckingham: Open University Press.
- [28] Ball, S. J., Maguire, M., Braun, A., & Hoskins, K. (2011). Policy actors: Doing policy work in schools. *Discourse: Studies in the cultural politics of education*, 32(4), 625-639.
- [29] Ministry of Education, Ontario. (2016). Ontario Schools, Kindergarten to Grade 12: Policy and Program Requirements. [http://edu.gov.on.ca/eng/document/policy/os/onschools\\_2016e.pdf](http://edu.gov.on.ca/eng/document/policy/os/onschools_2016e.pdf), (Access Date: 25 January, 2017)
- [30] Ministry of Education, Ontario, (2014). *The Ontario curriculum grades 9-12: French as a Second Language* [Program of Studies].<http://www.edu.gov.on.ca/eng/curriculum/secondary/fsl912curr2014.pdf>, (Access Date: 25 January, 2017).
- [31] Jesdanun, A., (February 10, 2017). *How Google Chromebooks conquered schools*. The Associated Press. <http://www.ctvnews.ca/sci-tech/how-google-chromebooks-conquered-schools-1.3279513>, (Access Date: 25 January, 2017)
- [32] Ministry of Education, Ontario, (2015). *The Ontario curriculum grades 1-8: Health and physical education* [Program of Studies], <http://www.edu.gov.on.ca/eng/curriculum/elementary/health1to8.pdf> (Access Date: 25 January, 2017).