Digital Privacy in the Classroom: An analysis of the intent and realization of Ontario policy in context

by

Heather Leatham

A thesis submitted in conformity with the requirements for the Degree of Master of Arts
Graduate Department of Education in the
University of Ontario Institute of Technology

© Copyright by Heather Leatham 2017
Acknowledgement

I would like to acknowledge the following people for their contribution to this research study. First, thank you to the Superintendent of Technology and the Manager of Information Technology in one particular Ontario district school board for allowing me the opportunity to conduct my research and work collaboratively. I also thank each of the almost 400 teachers who participated in the survey.

Secondly, I would like to thank Dr. Laura Pinto for her encouragement of this topic from a class paper to a master’s thesis, and her enthusiasm and support of the study.

I would like to thank my thesis committee, Drs. Jia Li and Bill Muirhead for their suggestions and support of the study. A huge thanks and appreciation to Dr. Lorayne Robertson for her endless patience, suggestions, revisions and support as my supervisor throughout the process.

Lastly I would like to thank my husband. From bringing me dinner during my classes, to keeping our dogs quiet while I was on video, his tireless support of my continuous pursuit of learning cannot be measured.
Abstract

Digital tools are becoming more commonplace within the K-12 classroom, but with the renewed opportunities come associated risks for student privacy. Digital tool use creates a digital footprint of the user which may contain personally identifiable information possibly compromising the user’s digital privacy. This study analyzes Ontario’s educational policies on the topic of digital privacy as it relates to digital tool use in the classroom. A digital survey was sent to teachers in one Ontario district school board to obtain their views regarding policy awareness and implementation, with 404 respondents. The findings of the policy analysis and survey indicate that there is a policy gap surrounding digital tool use in Ontario schools. The survey findings indicate that, though there is a high use of digital tools in classrooms, without policy support, there is an incomplete understanding of what constitutes digital privacy and the implications of its protection. This study concludes that there is a gap in policy development in Ontario education leaving early adopters of technology caught in an innovation-policy gap without relevant policies on digital privacy and digital tool use.

Key terms: privacy, digital privacy, digital tools, digital footprint, digital citizenship, apps, personally identifiable information, digital technology, public policy, policy analysis
Table of Contents

1 Introduction
   1.1 Context of Education Governance and Policy in Ontario  6
   1.2 Previous research and problem areas  7
   1.3 Statement of purpose  8
   1.4 Research Goal  9
   1.5 Summary of the Introduction  10

2 Review of Related Literature
   2.1 Digital Privacy
      2.1.1 Issues in Digital Privacy  16
   2.2 Policy
      2.2.1 Digital Privacy Presence in Education Policy in Ontario  22
      2.2.2 Ontario College of Teachers Act  24
      2.2.3 Policy/Program Memoranda  25
      2.2.4 Acceptable Use Policy  25
      2.2.5 Curriculum  26
      2.2.6 Related Privacy Legislation in the United States  28
         2.2.6.1 Children’s Online Privacy Protection Act  28
         2.2.6.2 Family Educational Rights and Privacy Act  30
         2.2.6.3 Student Online Personal Information Protection Act  32
         2.2.6.4 Summary of this Section  33
   2.3 Theoretical Framework: Policy analysis  33
      2.3.1 Defining Policy Analysis  33
      2.3.2 Policy as Text  35
      2.3.3 Policy as Discourse  38
      2.3.4 Policy Actors  39
      2.3.5 Policy Trajectories  42

3 Methodology
   3.1 Overview and Design  44
   3.2 Participants  47
   3.3 Data Collection Tool: The survey  48
   3.4 Procedure, Consent and Anonymity  48
   3.5 Data Analysis  49

4 Results
   4.1 Demographics  51
   4.2 Digital tools teachers used in their classrooms.  53
   4.3 Teachers and digital privacy.  58
   4.4 Awareness of policies on digital privacy.  63
   4.5 Parental Communication  67
   4.6 Summary of the findings.  68

5 Discussion
   5.1 The Innovation-Policy Gap  70
   5.2 Digital Privacy  72
   5.3 Communication with parents and students  74
   5.4 Summary  75
6 Conclusion

6.1 Review of the Literature

6.2 Reflections on Methodology

6.3 Findings

6.4 Recommendations

6.4.1 Recommendations for the district board level

6.4.2 Recommendations at a provincial level

6.4.3 Recommendations for Faculties of Educations

6.4.4 Recommendations for the College of Teachers and Teaching Unions

Appendix A: Consent letter

Appendix B: Sample of Teacher Digital Survey

Appendix C: Digital Tools

References

Figure 1: Privacy in Ontario, Canada (Leatham, 2017)

Figure 3: Ontario Curriculum Process (MOE, 2014)

Figure 4: Federal Trade Commission COPPA survey (FTC, 2002)

Figure 5: Easton's System Theory (Easton, 1953)

Figure 6: The Triangle of Policy Actors (Knoepfel et al., 2007)

Figure 7: Theoretical Framework for Policy Analysis (Leatham, 2017)

Figure 8: Policy Trajectories (based on Ball, 1994 and Bowe et al., 1992) (Leatham, 2017)

Figure 9: Years of teaching experience

Figure 10: Respondents and teaching assignments within the board

Figure 11: Respondents by area of the board and actual breakdown

Figure 12: Which of the following types of digital tools are you using in your class or have used?

Figure 13: Number of tools being used in a classroom

Figure 14: Digital Tool use in the classroom

Figure 15: How often are digital tools used by the students in your class as part of their learning?

Figure 16: Frequency of digital tool use to communicate with students

Figure 17: Frequency of terms

Figure 18: When posting student information online/in apps, how do you protect student information?

Figure 19: Awareness of board policies

Figure 20: Awareness of policies and procedures non-board specific

Figure 21: How often are you using digital tools to communicate with parents/guardians other than through email?

Table 1: The Administrator as a Policy Actor (Leatham, 2017)

Table 2: Alignment of research questions and survey

Table 3: Frequency of communication tool use

Table 4: Frequency of communication tool usage
1 Introduction

When individuals participate in online activity, information about them and their activity creates a digital footprint of traceable information. Some of the information is provided deliberately, while some information is collected passively without the knowing participation of the online user. According to PEW research center (2007), online participants, lured by mobile apps that make virtual participation easy, have increased the amount of personal information they make available to others online at new and unprecedented levels, and many are unaware of the range of their digital footprints (Madden, Fox, Smith, & Vitak, 2007). Palfrey and Gasser (2008) state that thousands of digital files about a person exist by the time they enter the workforce.

The information being shared, deliberately or not, creates a digital footprint.

Digital footprints contain personally identifiable information (PII), which is sensitive information such as full name, emails and age. Knowledge of one’s digital footprint is important because that footprint is a permanent record of activity on the internet. One Ontario Secondary School curriculum, the Canadian and World Studies policy, 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” (Ontario Ministry of Education (MOE), 2013, p. 174).

When traces of student data, which could include PII, are shared with online sites or through digital apps, it leaves students open to, for example, identity theft, hacking, and geotracking (Palfrey & Gasser, 2008).
According to Berson, M. and Berson, I. (2006), children are captivated by the interactivity of the internet and are unaware of the data tracking and data mining that happen when they share PII. It is the use of these data that is problematic as they can be used against students, as it could be used against any person. Berson, M. and Berson I. (2006b) argue that adults are, “inadequately prepared to assist children in understanding the complexities of privacy issues in a digital age” (p.3).

The implications of a digital footprint need to be considered at multiple levels of education, from the classroom where the technology is used, the school level, the school district level, and to the government and district agencies who design policies with respect to this issue. Using the example of social media, Phillips, Godfrey, Steuart and Brown (2013) and Palfrey and Gasser (2008) both caution about posting everything that students do, as it can be used against them when searching for a job or post-secondary admission.

Technology is now commonplace as both a learning and teaching tool. A MediaSmarts (Johnson, M., Riel & Froese-Germain, 2016) survey finds that 97% of teacher respondents have a networked device in their classroom (p. 4). The Grades 1-8 Health and Physical Education Ontario curriculum policy defines digital technology as “mobile applications and devices, the Internet” (MOE, 2015, p. 75). The possibility exists that, unwittingly, students are increasing their digital footprint in order to learn and participate in education, and if this is occurring, everyone involved in education needs to feel confident that there are corresponding security measures for student PII. Digital apps or tools are web-based software, websites, and/or games that run off a smartphone, tablet, computer or device that has internet capability. In this study, a digital tool is described as any internet connected tools which encompass web
based applications, iPad/Android apps, smartphone apps and Learning Management Systems (LMS) and require a login to proceed.

The field of education is one that is ever shifting in order to capture the attention of students with the use of digital tools. As the Internet, tablets and smartphones become more prevalent as teaching tools in K-12 classrooms, specific software on school board networked images are installed and controlled by many school district IT departments. The use of digital apps by teachers is increasing as teachers are looking for the most current tool to enhance the learning experience of their students.

Little is known, however, about the policy responses of Canadian governments, school districts, and schools to this widening digital footprint left behind by students, particularly when it concerns children and adolescents in schools. In addition, little is known about teacher awareness and implementation of policy responses to protect students’ PII given the increased facility with which student information can be shared in online spaces, and in some cases, shared for commercial purposes (Madden et al., 2007). This study attempts to respond to these areas of uncertainty by examining the following research questions:

1. How do teachers in one district school board use digital tools in their classrooms?
2. How do teachers in one district school board describe their use of digital tools to ensure digital privacy?
3. What is the current level of awareness of Ontario or district school board policies surrounding the protection of personally-identifiable information in one district school board?
4. How prevalent is student and parental communication through 3rd party apps in classrooms?
1.1 Context of Education Governance and Policy in Ontario

In this study, the education policies of public school boards in Ontario, the most populous province in Canada, are examined. To begin to examine the issue of governance and policy in Ontario begins with examining the national policies. The Constitution Act (1867) of Canada (formerly known as the British North America Act, 1867), divides the responsibilities and jurisdiction of governance between the federal and provincial governments. Section 93 of the Act allows that “each Province the Legislature may exclusively make Laws in relation to Education” (Constitution Act, 1867). Each province ensures the creation and delivery of public (secular) education from kindergarten to grade twelve, and in some provinces this also extends to Catholic school boards.

The Education Act for Ontario (RSO, c.E.2, 1990) section E(2) expands on these responsibilities by detailing the Powers of the Minister including creating curriculum policies, keeping student records and creating Policy/Program Memoranda (PPM) (MOE, 1990) in sections 8, and 8.1.

The province of Ontario has 31 English Public, 29 English Catholic, 4 French Public, 8 French Catholic school boards (MOE, 2014). These district school boards represent 3,974 elementary and 919 secondary schools and 115,154.69 full-time equivalent (FTE) teachers, and 2,003,237 students (MOE, 2014). Ontario schools are regulated by the Education Act (1990), and the Ontario College of Teachers Act (c. 12, 1996) which set out the duties and obligations of teachers in the province, as well as other Acts which, for example, contain regulations for child welfare. The Education Act (1990) is the overarching policy that governs education in Ontario. Subsequent Acts are incorporated into it as they are passed, for example the
Accepting Schools Act (c.5, 2012) which regulated the creation of a bullying prevention and intervention plans at the ministry and district levels.

In certain situations, other Ontario and Canadian laws take precedence, for example the Ontario Human Rights Code (c.H.19, 1990) and the Child and Family Services Act (c. C.11, 1990). For the purposes of this research study, the Education Act (1990), the Ontario College of Teachers Act (1996) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) (1990) are examined as they pertain directly to this study. Other related laws and policies that extend from these acts will also be examined in relation to student privacy.

1.2 Previous research and problem areas

One of the issues faced by educators with respect to student privacy is the lack of regulations regarding the adoption of applications. For example, each quarterly edition of Professionally Speaking magazine, published by the Ontario College of Teachers (OCT), contains a section entitled “Apps Analysis” profiling tablet and smartphone apps that teachers may find relevant and useful in their classroom. Readers might infer that the apps profiled will enrich their curriculum and engage students in learning because OCT is a trusted entity. Nowhere in the description of the apps does it state whether or not they are compliant with provincial or district policies on the protection of PII. Unfortunately, privacy is rarely mentioned in the apps review section (Dubowski, 2016).

Many online and digital apps are highly touted for their benefits by American educational bloggers and magazines (parental communication, student achievement tracking, badges), however what personal student information must be provided in order to access the app, as well as the storage of said information, is rarely provided (Anderson, 2014).
1.3 Statement of purpose

This study attempts to fill some gaps in the current literature on privacy of student information when digital tools are used for educational purposes because this is an emergent area of investigation and my initial investigations into the literature indicate that this topic is understudied. Literature on privacy considerations in education when using digital tools in Ontario was difficult to find through traditional literature searches. The academic literature on privacy at present focuses on social media privacy concerns specifically of teenagers (Christofides, Muise, & Desmarais, 2010; Madden et al., 2013; Park, 2013; Shade & Sheppard, 2013; Taneja, Vitrano, & Gengo, 2014). Plunkett, Solow-Niederman & Gasser (2104) addresses the need for teachers to consider student privacy from a legal perspective. There appears to be a gap in the literature in regards to student privacy and the use of apps in the classroom. Much of the literature with an education focus surrounds why and how to use digital tools in the classroom without a discussion on privacy (for example: Domingo & Garganté, 2016; Jonas-Dwyer, Clark, Celenza & Siddiqui, 2012; More & Travers, 2013).

In Canada, Media Smarts, a Canadian media awareness online network, provides articles and teacher resources as a means of support for educators and parents to self-educate about digital citizenship and online safety (Johnson, L. et al., 2014). According to Matthew Johnson (2015), teenagers are most concerned with keeping their online world away from parents. Johnson, M. (2015) also discusses the cultural norms of privacy in relation to online bullying. He concludes that more needs to be done regarding attitudes towards privacy.

Alternatively, there are many Canadian blogs and news articles that address the need for parents and students to be wary of how much information they give out online (Campbell, 2014; Watters, 2015). A common theme within the literature is digital citizenship education as
a means of being more proactive in protecting student privacy. Much of the literature addresses the lack of privacy protection and the need to do more to protect data as it pertains to students (Bernd et al., 2015; Berson et al., 2006a; Cranor, Durity, Marsh, & Ur, 2014;).

1.4 Research Goal

This study examines the policies, the literature, and the perspectives from the field on the topic of the protection of student digital information through examining teachers’ perspectives. First, this study provides a review of the literature from different countries related to the sharing of personal information online and identifies this as an area where more Canadian research is needed. Next, the study examines the legislative and district school board policy responses in one Canadian province to this issue. This review indicates that the Canadian policy landscape has not kept pace with the fast-evolving commercial world. Third, the study looks at how policies in education are defined and theorized and then presents a theoretical framework. The framework shows that different policy actors in school boards take on different roles within policy development and implementation, and experience both agency and constraints as they become the policy actors working on behalf of students. The theoretical framework and the review of the literature indicate a need to understand more closely how teachers are operating within this particular policy landscape. The research questions generated by the review of the literature are:

1. In what ways do teachers factor in or consider student privacy concerns when selecting digital tools to use in the classroom?

2. How do teachers take steps towards ensuring student privacy in the digital era?

This study employs survey research which examines teachers’ awareness of the present policies and the steps that teachers take to ensure students’ digital privacy. Next, the research
design, the methodology (survey) and the key findings are provided. The findings which
cannot be generalized except to other district school boards with identical policy landscapes,
identify the degree to which teachers in one district school board in Ontario are aware of
current policies and the digital privacy concerns generated by Web 2.0\(^1\) environment, and the
steps they take to mitigate risks to students. Based on the findings from the survey, the topics
of digital privacy and policy responses are explored more fully in the discussion chapter. This
study concludes with recommendations for further policy development and professional
development on students’ digital privacy based on the policy analysis findings and the survey
findings.

1.5 Summary of the Introduction

Education in Ontario is regulated through the Ministry of Education which sets out most
policy, including curriculum policy. Privacy policy in Canada has multiple points of origin
with both federal and provincial legislation that addresses personally identifiable information.
The digital footprint of students, a specific segment of the population, is not specifically
addressed within policy. As technology use within classrooms increases, the digital footprint
created by students becomes greater. School boards have overall privacy information
management policies regarding the sharing, collection and use of student information, but how
much this extends to online data is not known. Recently an Ontario newspaper made the claim
that, “The use of digital technology in schools is still in its infancy, and school practices about
student data are antiquated. Schools have a responsibility to let parents know how they’re using

\(^1\) The second generation of the Internet with an emphasis on collaboration and sharing (Dictionary, 2017)
Digital Privacy

children’s data” (Campbell, 2014). This study examines the availability of evidence regarding this claim.

2 Review of Related Literature

2.1 Digital Privacy

This thesis explores policy on digital privacy and teachers’ awareness and enactment of policies and procedures to protect students’ digital privacy. Thus, the concepts of privacy and digital privacy are central to this thesis. There are clear connections between privacy and digital privacy as they are outlined in the literature. The definition of the term privacy is “the state of being free from unwanted or undue intrusion or disturbance in one’s private life or affairs; freedom to be let alone” (Dictionary.com, 2017). Margulis (1977) states that “privacy as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability” (p.10). Gülsoy (2015) describes digital privacy as “the right to privacy of users of digital media (p.338). Gülsoy (2015) finds that both loss of control and intrusion are components of digital privacy, stating, “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” (p.338).

Merging the definitions of privacy with digital description, 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. Dienlin (2014) sees digital privacy as not a new type of privacy, but one to be discussed in the context of the online world. Culnan and Bies (2003) approach privacy from the consumer side, and its potential as a threat to capturing personal information.
The capturing of PII benefits the company and possibly the consumer, though it has the risk of becoming surveillance of consumers through the use of cookies\(^2\) (p.324).

Privacy as surveillance is discussed by Pinto (2016) for its policy implications. She examines the use of social media to keep watch on the teaching profession by its regulatory bodies as part of adhering to the rules. Indeed, the spring volume of Our Schools/Our Selves (2016) dedicates itself to the topic of surveillance in Canadian education, with at least five articles delving into the online context in relation to education and surveillance.

Miyasaki and Fernandez (2001) suggest that convenience of the digital tool for the user outweighs privacy concerns. Dienlin and Trepte (2015) find that though people state that they are concerned about their online privacy, they tend to engage in self-disclosure practices that do not match their concerns. They call this the \textit{privacy paradox}. This paradox is examined by Norberg, Horne and Horne (2007) who find people to be “cavalier in the protection of their own data profiles” (p.101). Norberg et al., (2007) also find that there are few studies on intentions and behaviours on the protection of privacy; their findings support the need for further studies in this area. Ignorance of privacy policies, settings and data storage can lead to privacy breaches and student information being shared inappropriately (Armario, 2016).

Teacher attitudes and behaviour about technology are a key factor (Mumtaz, 2000) to help prevent this. In summary, multiple authors (e.g. Berson et al., 2006b; Gülsoy, 2015; Palfrey & Gasser, 2008;) have concerns that digital privacy is breached when a person loses control over personal data through an unknown or unwanted intrusion.

Privacy protection in Canada falls under joint jurisdictions with the federal, provincial and municipal governments. At the federal level, the Office of the Privacy Commissioner of

\(^2\) Segments of data about a user sent between an internet server and an internet browser (Dictionary, 2017)
Canada oversees the Privacy Act (c.P-21, 1985) and the Personal Information Protection and Electronic Documents Act (PIPEDA) (c.5, 2000). Both PIPEDA (2000) and the Digital Privacy Act (c.32, 2015) are aimed specifically at private sector businesses and commercial activity. PIPEDA does not apply to public school boards because they are not involved in commercial activities, which means that there is no digital privacy law for minors in Canada. The Privacy Commissioner, writing about a PIPEDA case, states in a February 2013 decision pertinent to the app, Nexopia, marketed at youth, that,

While the Act does not single out youth, some of the Act’s requirements may call for special considerations in the youth context. For example, organizations may need to take extra care to ensure that young people can reasonably understand their privacy practices, so that any consent obtained from youth is “meaningful”, as required by the Act (Office of the Privacy Commissioner, 2012).

Each province in Canada has its own privacy laws that apply to both the private and the public sector. In Ontario education, the MFIPPA (1990) is applicable, though portions of Freedom of Information and Protection of Privacy Act (FIPPA) (c.F.31, 1990) are also applicable for the collection of information. Many school boards have a Privacy Information Management officer who oversees privacy breaches and is responsible for records and information management. School boards are also required to follow the Personal Health Information Protection Act (PHIPA) (c.3, 2004) which encompasses health information. The privacy laws are depicted in Figure 1 below.
Digital literacy and digital citizenship should not be confused as the same term. Digital literacy has been defined as the knowledge of computer related functions, and “the ability to find, evaluate, utilize, share, and create content using information technologies and the Internet” (Cornell University, 2009). Park (2013) defines digital literacy as “individual knowledge regarding computer-related functions” (p. 216), and states that knowledge is a key factor when taking digital actions, yet knowledge of technology and the internet do not correspond to knowledge and protection of privacy when online.

Berson et al., (2006b) advocate for an obligatory inclusion of digital literacy into curriculum to prepare students for responsible cyber-citizenship. Shade and Sheppard (2013) echo this advocacy, specifically for digital literacy of privacy policy, as their study finds that, although university-aged students were literate in the functionality of mobile devices, they were nonetheless ambivalent about privacy protection, and felt that they could manage their privacy individual through app privacy settings (Shade et al., 2013).
Digital citizenship is defined differently by different authors. The American website www.digitalcitizenship.net identifies nine elements of digital citizenship (see Figure 2): digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness, and digital security (2017). Figure 2 (below) outlines Duckworth’s (2015) elements of digital citizenship and relates them to the student context, based on the digitalcitizenship.net elements. The Ontario Software Acquisition Program Advisory Committee (OSAPAC) (2015) includes four skills of digital citizenship: critical thinking, creation and credit, communication, and protection. In summary, both digital literacy and digital citizenship advocate for students to be aware of what who is accessing the content they are putting online, and how to protect their privacy.

Figure 2: Digital Citizenship Sketchnote (Duckworth, 2015)

The use and prevalence of digital tools in education can be quickly ascertained by a Google Scholar search. Using the search terms digital tools+education (no quotation marks),
approximately 1,610,000 entries were returned (excluding citations and patents). In comparison, the search terms *digital privacy + education* (no quotation marks) returned 1,480,000. Large results for both searches means that there is a high level of awareness of and writing about digital tools and privacy in education. Changing the search terms to digital privacy as a term (using quotation marks), resulted in 1,790 entries (May 21, 2017). In skimming the entries, many pertained to students/youth protecting their privacy, cybersecurity, health data and consumer business topics. The search results above, indicate that there is much interest in digital privacy. However, the majority of articles focus on teenagers and social media use, not on privacy in the classroom when using digital tools.

2.1.1 Issues in Digital Privacy

Digital privacy within education focuses on the protection of student data during digital technology use. Digital privacy is an important concern for parents of adolescents because, according to Cranor et al., (2014) parents are concerned with protecting teens from online dangers which can occur from lax privacy settings, which is something that the teens do not appear to understand. Berson et al., (2006b) find that websites ask for personal information in many different ways, regardless of the age of the user. They explain that the age of the user is important because the United States Supreme Court sees three reasons why the constitutional rights of children are not the same as adults: “the peculiar vulnerability of children; their inability to make critical decisions in an informed, mature manner; and the importance of the parental role in child rearing” (p.139). Berson et al., (2006a) state that identifiable information is uncontrolled even when children’s privacy has been legislated, and explore how children manage and interact with technology considering privacy laws (Berson et al., 2006b). As Palfrey and Gasser (2008) state,
Parents, teachers, and policymakers need to concern themselves with both the sifting notion of identity and the expanding digital dossiers of our children, and they need to understand that these dossiers include contributions from a wide range of sources and are easily accessible to an even wider range of people, some of whom may use them for purposes we would not desire (p. 58).

In a presentation to school attorneys in the United States on the regulatory issues in regards to digital privacy, Microsoft gives scenarios where student data can be given out through app ‘click-through’ agreements (Mutkoski, 2013). Mutkoski (2013) cites American, Australian and UK parental surveys where parents are concerned about the online privacy of their children, especially through vendor collection of data (p.10).

In the Ontario, Canada context, in a report to the Ontario Privacy Commissioner, Christofides et al., (2010) concluded that both youth and adults tended to use the privacy settings on Facebook more often when there is an awareness of consequences for disclosing too much personal information. Christofedes et al., (2010) make two recommendations:

- To increase awareness in education about the consequences for disclosing information;
- To develop education campaigns to raise awareness and encourage users to read the privacy settings in relation to policy (pp.8-9).

Other authors who write about digital privacy outside of education find that digital privacy is a perception, or a choice that adults make based on circumstances. For example, Malhotra, Kim and Agarwal (2004) theorize privacy as a social contract; the consumer allows the collection of data with the idea that they control whether they can exit the transaction. Dinev, Xu, Smith and Hart (2013) find that perception is predicated upon the expectations of the individuals, stating that, “Privacy risk attitudes are grounded in an individual’s values in terms of information sensitivity, assessment of perceived benefits of information disclosure, importance of information transparency, and regulatory expectations that enable a person to
assess the risks of information disclosure” (p. 308). Dinev et al.’s, study is based on Norberg et al.’s, (2007) research on privacy attitudes and related behaviours in the marketplace, where Norberg et al., (2007) find that people are more likely to provide personal information if the benefits are attractive, therefore focusing on the gain from the program rather than the losses.

In summary, the literature on digital privacy concludes that, with the need for more research in this area, the control of access to personally identifiable information is a topic of great importance, and it gains importance when considered in the context of child and adolescent vulnerability. The findings from this study’s research questions “How do teachers describe their use of digital tools and continue to ensure digital privacy?” and “How prevalent is student and parental communication through 3rd party apps in classrooms?” seek to add to the literature on the topic. It may be that teachers act in similar ways to those reported by Norberg et al., (2007), who weigh the benefits of the use of apps in the classroom relative to the loss of digital privacy. The aim of this study is to fill in some existing gaps regarding teacher awareness of digital privacy policy and teacher practices to protect students’ PII.

2.2 Policy

This section of the literature review examines the intent and implementation of policies which were written in Ontario to address the issue of digital privacy for students. In Ontario the curriculum documents are policies and ordinarily teachers would look to the curriculum policies for guidance. As discussed in section 2.2.5, the Ontario curriculum offer no support to teachers in respect to the protection of student digital privacy. A single, generally accepted definition of public policy is hard to pinpoint in the literature. The online Oxford Dictionary defines policy as “a course or principle of action adopted or proposed by an organization or individual” (www.oxforddictionaries.com, 2017). Fowler (2004) defines policy in this way,
“[P]ublic policy is the dynamic and value laden process through which a political system handles a public problem” (p. 9). The protection of student digital privacy in Ontario is not represented in any single, specific policy. For the purposes of this paper, multiple definitions of policy are examined, including that of Bowe, Ball and Gold (1992), who theorize the process of policy development and implementation in different contexts.

Public policy occurs in contexts which are political, economic and societal arenas (Waller, Morris & Simpson, 2009). It can guide, outline or determine the actions of a general or specific population. Common to many definitions is that policy is a response to an identified problem. Birkland (2014) states that a key characteristic of public policy is that it “is made in response to some sort of problem that requires attention” (p.8). Pal (2010) defines public policy as “a course of action or inaction chosen by public authorities to address a given problem or interrelated set of problems” (p.35). Policy can attempt to rectify inequalities, such as Lyndon Johnson's Great Society policies of 1964-65. McConnell (2010) sees public policy as anything from the minutiae of government to the overall functioning of the country, and outlines three perspectives to understand the process of public policy: the process of policy making or the policy cycle; the tools governments use to address policy or the programmatic; and the political dimensions of policy.

Fowler (2004) sees policy as a multi-layered response by a government-type body to a public problem. A policy would be representative of the public as it reflects and uses their values as a response. Therefore, policy would assume to be inclusive in taking all stakeholders into account, something that may require a lengthy process to identify and consult. The second part of Fowler’s definition is that it includes, “a government’s expressed intentions and official enactments as well as its consistent patterns of activity and inactivity” (p.9). This echoes Pal’s
courses of action, meaning that the even the lack of policy, or lack of action, is in itself a policy issue. This is the case in Ontario where there appears to be insufficient awareness of the issue and the need for policy around student digital privacy.

In order for a policy to take place, it needs to be implemented or ignored. Fowler (2004) identifies the actors who can be considered as government players at different levels of government, both elected and appointed. It also includes agencies and official bodies that represent the government. Bowe et al., (1992) point out that these actors are “in competition for control of the representation of policy” (p.21), a key point that can direct the creation and publication of a policy. Bowe et al., (1992) see policy (and policy making) as a discourse, with the knowledge of the problem on one side and the methods to implement on the other “about how the world should and might be” (p.13). They define policy as “operational statements of values statements of ‘prescriptive intent’. […] essentially contested in and between the arenas of formation and ‘implementation’” (p.13).

Bowe et al., (1992) examine policy in three different contexts: the context of influence, the context of text production and the context of practice, -all of which inhabit different arenas (public or private). They elaborate on how “policy texts represent policy” (p.20). They also remind us that policy does not end when it becomes legislation. Legislation would be an official text outlining the policy and to whom it is addressed and how. Then there are official texts which are written to make sense of the official texts; these are the interpretive texts that help a population understand the intent and possible implementation of policy. In the view of Bowe et al., “policies then are textual interventions but they also carry with them material constraints and possibilities” (p.21).
Policy does not just happen (Fowler, 2004), as it is a response to a problem. It is also created through a process (McConnell, 2010). McConnell outlines different definitions of policy in order to establish its complexity such as: Easton’s (1953) “a web of decisions and actions that allocate... values” (p.13); Dror’s (1983) “general directives… on the main lines of actions to be followed” (p.14); and Dye’s (2005) “whatever governments choose to do or not to do” (p.1).

Easton (1953) and Lasswell (1956) describe stages of policy making which have become the policy cycle framework. The policy cycle according to McConnell (2010) is: “[to] define issues, examine options, consult (or not), take decisions, decide how they will be put into practice and decided what procedures will be used to evaluate” (p.4-5). The cycle examines the role of the various actors and their decision of “who, when and how to consult; policy alternatives…; and the policy-making route” (p.5). McConnell’s steps of the policy cycle process include the need to evaluate the failure or success of policy as part of policy analysis.

Policy analysis “is a practice that entails the application of various research methods to policy issues and policy-making processes” (Yanow, 2007, p.111). Knoepfel, Larue, Varone and Hill (2007) explore various schools of policy analysis, and find that the evaluative school of policy analysis tries to determine the impact of a policy and whether the intentions meet the results, as it is necessary to determine whether the policy actually meets the needs of its intended audience. Fowler (2004) points out that while all educational policies could be evaluated, many are not, and others are evaluated but poorly. She advocates that the final stage of the policy process should be a careful evaluation “and then either (it is) maintained as it is, changed or terminated” (p.303). Policy analysis meets many purposes, and in the present study, policy analysis will help to determine whether or not the policy exists, and where it
exists in the different educational contexts of the government, the district school board, the school and the classroom.

Policy and technology are examined by Davis (2014) who identifies an *innovation-policy gap* between the speed that technology is iterating and the policies that attempt to follow to regulate the interventions. For Davis, the policy development process is inherently time-consuming and the opposite of the speed of the development of technology, helping to widen the gap. He also identifies *knowledge gaps*, one specifically about digital privacy in that an understanding of how privacy is managed needs to happen in order for privacy policy to happen (Davis, 2014). Importantly, he states “Technology will continue to evolve in ways and with outcomes that we cannot fully anticipate. These innovations can have a deep influence that impacts our social values and our body of law” (p. 88). His four areas of ethics (digital identity, privacy, ownership and reputation) need to be thought of together and balanced to improve the innovation-policy gap (Davis, 2014).

2.2.1 Digital Privacy Presence in Education Policy in Ontario

The present research study examines digital privacy policy and awareness of this policy in the Ontario education system. A search was undertaken to determine how digital privacy is represented in education policy. Schools are regulated in Ontario by the Education Act (1990). This Act mentions privacy in sec.266.1 in relation to Personally Identifiable Information (PII) and it states that PII is defined by both FIPPA and MFIPPA. MFIPPA (c. M-56, 1990) under section 28 regulates PII.³

---

³ Personal Information as defined in MFIPPA “means recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,(c) any identifying number, symbol or other particular
In the Education Act (1990), the term *technology* appears in conjunction with applied arts in sections on post-secondary destinations (sec. 49.2(6.2); 171.1(44); 189.2). The words ‘online’ and ‘digital’ appear nowhere in the Education Act (1990), and ‘computers’ are referenced only in sec.171.1(9) for the purposes of buying computers, not their usage.

Section 301 of the Education Act (1990) establishes a provincial Code of Conduct, and it requires school boards to create their own version and include the seven purposes\(^4\) as outlined in sec. 301(2) and restated in The Provincial Code Of Conduct and School Board Codes Of Conduct/PPM 128. Broadly, the use of technology in the classroom, and the protection of student information is protected under the provincial Code of Conduct’s standards of behaviour: Respect, Civility, and Responsible Citizenship as it states that all school board members will “respect and comply with all applicable federal, provincial, and municipal laws” (PPM 128, p.4).

In summary, in the literature search for written policy texts, it was challenging to determine who has jurisdiction for digital privacy for schools in Ontario as it seems that there is lack of clarity on which area of government is responsible, and there are interjurisdictional issues between governments and school boards. For this research there was a study of multiple

---

\(^4\) 1. To ensure that all members of the school community, especially people in positions of authority, are treated with respect and dignity. 2. To promote responsible citizenship by encouraging appropriate participation in the civic life of the school community. 3. To maintain an environment where conflict and difference can be addressed in a manner characterized by respect and civility. 4. To encourage the use of non-violent means to resolve conflict. 5. To promote the safety of people in the schools. 6. To discourage the use of alcohol and illegal drugs. 7. To prevent bullying in schools. 2000, c. 12, s. 3; 2012, c. 5, s. 10 (1).
policies that address student safety (such as Policy/Program Memoranda 128 and the Education Act), but there appears to be a gap with respect to protecting students’ and teachers’ safety online. As such, it would appear that it must be difficult for educators to have a clear understanding of jurisdiction and responsibility for students’ digital privacy. In order to see where digital privacy is addressed, the review of the literature now examines specific aspects of provincial, school and district policies that provide examples of school districts’ attempts to align with the protection of student information online.

2.2.2 Ontario College of Teachers Act

The Ontario College of Teachers (OCT) Act (1996) under sec.3(7) has as an objective “to establish and enforce professional standards and ethical standards applicable to members of the College” as stated in the Professional Standards section of their website. Within the Standards of Practice, technology use is addressed in the Professional Practice section 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.” The College also publishes Professional Advisories, such as the Use of Electronic Communication and Social Media advisory (OCT, 2011) It is aimed more at the personal behaviour of teachers in their private lives, though it does mention in two different sections to “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” (OCT, 2011). Though the advisory mentions privacy in nine instances, the only legal policy it references is the Education Act (1990) not MFIPPA (1990).
2.2.3 Policy/Program Memoranda

As explained earlier, the Ontario Ministry of Education publishes Policy/Program Memoranda (PPM) which are related pieces of legislation to the Education Act (1990) which are passed and revoked as the Education Act is amended. PPMs are “directives issued to district school boards and school authorities to outline the Ministry of Education's expectations regarding the implementation of ministry policies and programs” (Ministry of Education [MOE], 2017). The Code of Conduct/PPM 128 is a revision after the passing of the Accepting Schools Act (2012) which replaces the Ontario Schools-Code of Conduct (2000) policy. PPM 128’s language is not specific to the online world as its provisions focus on the physical (e.g. school vandalism, weapons, drugs and alcohol). The district school board level Codes of Conduct implement the PPM as it is laid out, specific to the context of their own geographic, demographic and economic situations.

2.2.4 Acceptable Use Policy

The overall curriculum policy for the province of Ontario is Ontario Schools Kindergarten to Grade 12 Policy and Program Requirements (MOE, 2016). In the preamble, teachers are to include the role of information and communications technology that “align with ministry and board policy and initiatives” (p. 58). This alignment would require board level Acceptable Use Policies (AUP) for technology. As every district school board writes its own policies, a comparative analysis of these AUP’s is outside the scope of this research study.

Within this study, I analyzed some policies from the district school board where this study takes place. An analysis of the Employee AUP identifies that the policy defines Information


Technology, but does not specify the acceptable use of technology within the classroom specifically. The policy applies to all district employees, not just teachers.

Student data is addressed in section 1.11 of the Employee AUP Administrative Procedures policy. Section 1.11 states that student data must be ‘safeguarded’ according the MFIPPA (1990) and an immediate supervisor notified of breaches.

There is also a student acceptable use policy; AUP #902, section 3.1 states “Teachers shall provide students with instruction on the appropriate use of the internet” but does not expand on what constitutes ‘appropriate’. In the accompanying student AUP administrative procedure, sec. 1.4 states that, “Principals will provide access to guidelines for student safety while using the internet” (AUP # 902, 2010, p.1). This appears to assign the responsibility to the principal which also could mean that each school may have different procedures. Under the school district’s Privacy of Personal Information Policy (2010), section 3 ‘Consent’ states that staff should obtain permission when collecting any personal information.

The overall analysis of these district-level policy texts indicates that the protection of student information is addressed in multiple places in general terms, but protection of online PII does not appear to be addressed distinctively in policy at either the provincial or the district school board levels.

2.2.5 Curriculum

In Ontario, there are curriculum policies for the Early Years: junior kindergarten (JK) and senior kindergarten (SK) as well as curriculum policies for Kindergarten to Grade 12 (K-12). These policies are written for different divisions. For each subject, there is a kindergarten to grade 8 curriculum policy (Primary, Junior and Intermediate divisions) and a grade 9 to 12 policy (secondary). Curriculum in Ontario undergoes continuous revision; all individual
subjects have had their curriculum revised at least once in the last 16 years (see Figure 2 below for the process). Each curriculum policy contains an introduction which sets the context of the subject and orientates it within current pedagogical theories; the program and its learning strands (organizers); assessment and evaluation overview; and considerations for implementation before dividing into the specific grade range or course outcomes. Newer policies include teacher prompts and possible student responses for the specific expectations. For the purposes of this research study, the Health and Physical Education curriculum (MOE, 2015), grades 1-8, will be used as an example because it is the most recently revised curriculum.

Curriculum is considered policy for teachers, as it must be followed, delivered and evaluated on provincial report cards.
The policy *Ontario Schools Kindergarten to Grade 12 Policy and Program Requirements* policy (MOE, 2016) instructs teachers in what is required of them in their classroom as per policy and program policies, hyperlinking to relevant PPMs. Examples of this would be links to the PPM’s for *Daily Physical Activity* (PPM 138) and record keeping procedures in the Ontario School Record Guideline (2000). The word privacy appears once in the overarching K-12 policy *Ontario Schools Kindergarten to Grade 12 Policy and Program Requirements* and that is in relation to the transition from grade 8 to grade 9. The word digital appears six times, all in section 10 on E-learning opportunities (MOE, 2016). In other words, the overall curriculum has not kept pace with digital innovation and does not address digital privacy in policy for K-12 in Ontario.

In summary, digital privacy and protection of student PII is not present in the curriculum policies, the policy program memoranda or the Education Act or the College of Teachers Act in Ontario. With these significant policy gaps, district school boards are left to manage technology issues through Acceptable Use Policies and district level responses.

2.2.6 Related Privacy Legislation in the United States

2.2.6.1 Children’s Online Privacy Protection Act

The protection of children’s online privacy is different in the US context. The Children’s Online Privacy Protection Act (COPPA, 1998) falls under the Federal Trade Commission (FTC) because digital tools provide services to clients. COPPA’s purpose is to protect the online privacy of US children under 13 and requires parental consent for children to use online sites and digital apps. According to the FTC, COPPA “imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are
collecting personal information online from a child under 13 years of age” (FTC, Part 312, 1998).

Specifically, the COPPA legislation requires companies to do the following: 1) post a privacy policy; 2) provide notice directly to parents; 3) get parental consent; 4) allow parents to review, revoke consent and delete their child’s information; and 5) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children’s personal information. COPPA is also unique in that it repeatedly invokes provisions that mention parental knowledge, obtained consent and direct notice about their child’s use of the app. Section 312.6 of COPPA instructs how parents can ask for and review information has been collected digitally, and ask for its deletion from the vendor’s databases.

COPPA, though aimed at digital apps for children, can also apply to general audience apps that could have consumers under 13 years old and to third party plugins/services (FTC, 2013). One manner in which COPPA is specific to the online domain is section 312.1(7) in identifying what is considered PII:

First and last name; A home or other physical address including street name and name of a city or town; Online contact information; A screen or user name that functions as online contact information; A telephone number; A social security number; A persistent identifier that can be used to recognize a user over time and across different websites or online services; A photograph, video, or audio file, where such file contains a child’s image or voice; Geolocation information sufficient to identify street name and name of a city or town; or Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above (FTC FAQ, 2015).
In a 2002 survey on COPPA, the FTC found that, of 144 websites identified as being marketed to children, 72% collected some type of PII (see Figure 4). 35% of the sites obtained information that did not fall within an exemption of obtaining parental consent. Though these data are fifteen years old, the FTC has not published a follow-up, and the 2002 publication is actually a follow-up to the one done in 1998 at the creation of COPPA. One drawback of COPPA is the manner in which parental consent can be obtained. A child can easily type in their parent’s email address or obtain their credit card information or even call in to a toll-free phone number to indicate parental consent.

![Types of Personal Information Collected](image)

*Figure 4: Federal Trade Commission COPPA survey (FTC, 2002)*

2.2.6.2 Family Educational Rights and Privacy Act

In the United States, the Family Educational Rights and Privacy Act (FERPA, 1974) falls under the Department of Education and is specific to student educational records. Written before computers and the Internet were in every home, let alone schools, FERPA is similar to COPPA, in that it includes the parents as part of the Act, and means to protect their information as well as student information. FERPA is included in a discussion on digital privacy as student
records contain PII and digital apps collect data from (for example) quizzes which are attached to student records. FERPA does allow the disclosure of PII as follows. “To organizations conducting studies for, or on behalf of, the school, in order to: a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction.” (sec. 99.31(a)(6)). This means that digital apps, under contract to a district or a school, can obtain student PII. The metadata\textsuperscript{5} that these providers obtain (for example how long a student spent on a question), can be used by the provider if stripped of its PII (Privacy Technology Assistance Center, 2014).

Contrary to MFIPPA (1990) and COPPA (1998), FERPA (1974) definition of PII are items that would be found in traditional education student dossiers, whereas COPPA (1998) includes specific digital identifiers and MFIPPA (1990) is more general. FERPA’s (1974) defines PII as including but not limited to:

(a) The student’s name; (b) The name of the student’s parent or other family members; (c) The address of the student or student’s family; (d) A personal identifier, such as the student’s social security number, student number, or biometric record; (e) Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates (sec.99.3).

\textsuperscript{5} Computer information that is held as a description of stored data (Dictionary, 2017)
FERPA has four exceptions to the disclosure of PII that are applicable to online tools (see sec. 99.31(a)(1)(i)). In order for the exception around being a provider to be valid, the onus is on the school or the district to determine if the provider is a “legitimate educational interest.” In some cases, the terms of service from the provider may encompass all the legal requirements the provider must and will be following.

2.2.6.3 Student Online Personal Information Protection Act

The current US law on the subject of student privacy, the Student Online Personal Information Protection Act (SOPIPA) (Ch.22.2, 2014) is from California. Its aim is to prevent digital tools used in the K-12 classroom from amassing student data, selling it to third parties or engaging in targeted marketing from the data gleaned from digital tool use. SOPIPA is unique in that it applies to schools and not industry as FERPA does and it does not have a parental consent exception like COPPA. Though aimed at student PII, SOPIPA also protects parents/guardians and educators who also access the digital tools.

The California Attorney General published recommendations for the Ed Tech community on ways they can protect student PII, including overviews of FERPA, COPPA and SOPIPA (2016). These recommendations include among them (pp.11-16):

- Describing the data being collected and retained,
- Describing to whom and how data is disclosed, and
- Describing the methods of data security in place.

Since the passing of SOPIPA, 26 other states had enacted similar SOPIPA-style laws as of May 2016 and 69 laws on student privacy have been passed since 2014 in sixteen states (Data Quality Campaign, 2016).
2.2.6.4 Summary of this Section

In this section of the review of the literature, the policies in Ontario schools which are related to the protection of student information and privacy were analyzed with the finding that the approach to digital privacy is on the radar but not outlined in clear policy terms for schools and school districts. The policies in effect in the US were examined for their contrasting approach, which appears to demonstrate a clear awareness of the need to protect students’ PII as well as to provide detailed policy safeguards.

2.3 Theoretical Framework: Policy analysis

2.3.1 Defining Policy Analysis

The topic of digital privacy within Ontario policy is fragmented because, as noted earlier, there are multiple policy designers such as the College of Teachers and the Ministry of Education who author policies and policy memoranda in Ontario. No policy was located which is specific to the protection of PII in a digital classroom environment. Although curriculum in Ontario is updated on a regular basis (see Figure 3 for the curriculum cycle), many policies do not reflect the reality of increased use of technology in the classroom.

Policies in education do not end their life cycle at the point that they are written because policies have implications (Lasswell, 1936) whether they are implemented or not. Some groups benefit from policy, and policies are targeted at specific groups (Knoepfel et al., 2007). Easton’s (1953) systems theory, became a policy cycle framework (see Figure 6).
Analysis of policy in the past has been concerned about assessing the impact of policy upon the intended interests. A way of visualizing this is using Knoepfel et al.’s (2007) diagram (see Figure 7) below.

Nagel’s (1984) definition of policy analysis is the “evaluation of alternative government policies or decisions in order to arrive at the best (or a good) policy or decision in light of given
goals, constraints, and conditions” (Nagel, 1984, p. xiii). Fowler (2004) also identifies that policy analysis is designed to “improve the quality of public policy” (p. 19) and she lists four types of policy analysis: monitoring, forecasting, evaluation and discursive analysis.

For this research study, the following toolbox (Figure 8) of theories will be used to analyze the related policies and the data. It is important to conduct policy analysis for the purposes of measuring if the policy is working the way it was intended (Fowler, 2004), as well as to determine how the policy is being interpreted and implemented (Ball, 1994).

![Policy Analysis Toolbox](image)

**Figure 7: Theoretical Framework for Policy Analysis (Leatham, 2017)**

2.3.2 Policy as Text

Teachers in Ontario have multiple policy texts previously cited, such as curriculum policies and safe school policies. The Education Act (1990) pulls together disparate policies as they pass assent. Policy actors (Ball, 1994; Ball, Maguire, Braun & Hoskins, 2011: Fowler, 2004) enact and interpret the policy. Policies as *texts* according to Ball (1994) are representations which are encoded (written) and decoded (read) by those who are enacting them, or the policy actors. Policy actors (Ball, 1994) are the people who create, implement and influence policy. Fowler (2004) also identifies policy actors as those who create and those who influence policy,
Digital Privacy

calling them “the cast of characters...of policy development, adoption, and implementation” (p.141).

As discussed earlier, digital privacy as a specific policy text was not located in a review of related Ontario policy. Digital privacy as a policy text can be seen in the International Society for Technology in Education (ISTE) Standards. ISTE is an international organization who for the last forty years has been promoting educational technology standards through a network of teachers and education players. In the 2017 refresh of the Standards for Educators, the Citizen section requires teachers to understand data collection in relation to student privacy and in order to protect their PII. Similar wording can be found in the Standards for Administrators (2009) and the Standards for Students (2016) on modeling and engaging in safe online spaces, and taking into account legal and ethical behaviour. In the Standards for Students, under Digital Citizenship, it also states that “students manage their personal data to maintain digital privacy and security and are aware of data-collection technology” (ISTE, 2016, 2d).

Within Ontario, policy as text related to the issue of PII could be addressed in the Code of Conduct PPM 128 (MOE, 2012). PPM 128 instructs district school boards to create their own Codes of Conduct which, though not specific to digital privacy, do encompass behaviour in the “nexus” of relevant school behaviour whether physically at a school or off school property. As each district creates its own Code specific to their board, principals also create their own school-specific Codes of Conduct. PPM 128 states how boards and principals can decode the guidelines of the code, when it directs districts to link locally-developed standards to the relevant provincial standards (e.g., school board rules for the use of electronic devices such as cell phones could be linked to the provincial standard requiring those at school to respect the need of others to work in an environment that is conducive to learning and teaching [see
“Respect, Civility, and Responsible Citizenship” on page 4] (PPM 128, 2012, p. 3). The Codes of Conduct themselves are representations of the guidelines first seen in the Education Act (1990), and then expanded upon in PPM 128 (MOE, 2012).

Ball (1994) has theorized policy as a textual intervention into practice but in the case of protection of PII, there are multiple factors. There has been an increased use of technology in the classroom, which was largely unregulated as the popularity of devices such as iPads increased according to one online source (Etherington, 2013). In 2011, Apple was marketing the iPad to schools, even promoting specific apps for use in classrooms (Butts, 2011). Digital privacy is the extension of protecting student privacy in communications, paper files and notes. With the sudden uptake of technology, schools need to solve the issue of educating teachers so that they are aware that student data in the online world can be obtained through covert methods such as hacking or being sold to third-parties. In order to address this, a school board can act on this potentially through direct education of teachers, an amendment to Codes of Conduct to specifically address privacy overall, and/or an amendment to Acceptable Use Policies.

Teachers can hide from policy by willfully ignoring it (Ball, 1994). Teachers may not act on policy because of factors such as time, lack of understanding/clarity of policy, or misguided interpretations from trusted colleagues (Ball, 1994). In other words, a teacher may decide to act on policy when it best suits them and their particular situation, for example following a district procedure of submitting an app for review in order to use the app in their class.

Constraints for a teacher to implement policy may include easy access to device’s app stores, lack of device accessibility for use in class, pressure from parents to increase the use of technology in the classroom and even the MOE’s 21st Century Competencies policy (Edugains,
2016) that advocates for the use of technology in the classroom. Morris (2017) in a blog, explains that agency “doesn’t so much exert itself upon others as it does float within the intersection of freedom and authority.” As Ball (1994) states, agency and constraint are in a relationship together; one cannot be without the other. Thus teacher ‘freedom’ is only as far as the constraint of ‘authority.’ While a teacher may have the freedom to use any digital tool within their classroom, and is so encouraged by policies such as the 21st Century Competencies (Edugains, 2016), the teachers may or may not be aware of the constraints of MFIPPA (1990).

2.3.3 Policy as Discourse

According to Ball (1994), policy may also be viewed as a discourse (see Figure 7), stating that “Discourses are about what can be said, and thought, but also about who can speak, when, where and with what authority” (1994, p. 21). Bowe et al. (1992) see policy as discourse as the “possibilities and impossibilities, tied to knowledge on one hand and practice on the other” (p. 13). Policy on privacy as discourse appears in the Acceptable Use Policies that Ontario School boards enact which aim to practice proper use of technology in school and online, although AUPs do not mention digital privacy specifically. This is then a gap in the policy. As stated in the beginning of section 2.3, most of the policies reviewed in this research study have not been revised to reflect the digital world.

One policy as discourse around the protection of PII is a video by the Ontario Association of School Board Officials (OASBO, 2016) entitled Understanding Privacy Considerations (http://www.pimedu.org/videosboardstaff.html). This video explains the process for determining approved digital tools. OASBO is acting independently of an established MOE policy with their videos, though they are part of Privacy Information Management (PIM) which enforces MFIPPA (1990). The video is from what Ball (1994) would describe as a “certain
voice...authoritative” (p. 23) 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” (OASBO, 2017).

2.3.4 Policy Actors

The table below summarizes the key roles of school administrators as policy actors (Ball et al., 2011; Fowler, 2004) with respect to policy.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Expected to fill in the frameworks by creating policy to address at the school level</td>
<td>● Can be any actor, move between roles</td>
</tr>
<tr>
<td></td>
<td>● Expected to develop an implementation plan</td>
<td>● Narrator who interprets, enforces policy – “what must be done, can be done and what cannot” (p.626)</td>
</tr>
<tr>
<td></td>
<td>● Expected to gather resources for said plan</td>
<td>● Transactors who monitor and report on policy</td>
</tr>
<tr>
<td></td>
<td>● Expected to give feedback</td>
<td>● Work with entrepreneurs to merge policies together into a coherent plan for ‘improvement’</td>
</tr>
<tr>
<td></td>
<td>● Essential to follow policy and legislative process</td>
<td>● Entrepreneur who advocates for policy</td>
</tr>
<tr>
<td></td>
<td>● Can influence future policy/revisions through various channels</td>
<td></td>
</tr>
</tbody>
</table>

| Synthesis                | The role of an administrator in policy work is the implementation at a school level of policy received from a governing authority. |

*Table 1: The Administrator as a Policy Actor (Leatham, 2017)*

Both Fowler (2004) and Ball et al., (2011) view school administrators as instrumental for developing policy, defining it and implementing it. Administrators are 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. 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, 2004). She states that administrators can also be at the forefront of influencing policy through various local and state groups or agencies (Fowler, 2004).

In Ontario, other policy actors (Ball et al., 2011) would be the Minister of Education and her office, the College of Teachers, the District School Boards (including the Directors and Superintendents), teachers, unions and advocacy groups. Policy development and the influence and input from all the actors would look similar to Figure 1 (Curriculum Review). According to Ball et al., (2011) Table 1: Policy Actors and Policy Work, multiple actors play multiple roles in policy implementation, such as narrator or entrepreneur. As policy actors, the OCT could be put in many roles. With the Standards of Practice, they can be as policy transactors (Ball et al., 2011) because they are given the authority to monitor and discipline teachers through the enforcement of their policies (Ball et al., 2011).

Teachers can take on a variety of policy roles also. For example, those teachers who are ‘early adopters’ of innovations (Rogers, 1962) could be considered policy enthusiasts (Ball et al., 2011). They are the ones who want to make sure that they are at the forefront of the newest policy or educational trend, and can be experts within a school. They thus become policy models for other teachers. In terms of board positions, enthusiasts could also be teachers who are subject-specific consultants, who also cross over into narrators (Ball et al., 2011) as they interpret policy for the subject teachers across a district. Consultants and other board level teachers, including superintendents, become policy entrepreneurs (Ball et al., 2011), encouraging those they interact with to incorporate/implement new policy as it is made available. On the other end are the receivers, or the in-class teachers. In a top-down approach to new policy implementation, they are made aware of the new policy and may be a receiver of
professional development so that they ‘understand’ what they should be doing. Receivers “rely heavily on ‘interpretations of interpretations’” (Ball et al., 2011, p. 632) and may not become policy enthusiasts because they may feel overwhelmed or be younger, new teachers (p. 632).

How a teacher enacts policy comes down to whether the teacher grasps the policy and has the resources available to enact it (Ball, 1994). They have to be willing to commit to the policy, which might have an impact (positive or negative) on their classroom practice. Ball (1994) states that enactment of a policy relies on, among other things, commitment, understanding, resources and intertextual compatibility (p. 19). Teachers may feel that they are incapable of enacting a policy well or that they need professional reading or training in order to properly understand well enough to attempt implementation (Ball et al., 2011).

Looking at policies in isolation and not as interconnected pieces may also impede enactment. Both a micro and a macro understanding of a policy’s purpose will help teacher understanding and lead to better commitment to enactment because connections can be made to work that has already been done or will be (Ball, 1994). There needs to be teacher ‘buy-in’, or making it relevant for a teacher so that they can see themselves enacting a policy. Without this, teachers may become policy critics, holding on to “a collective history” or “field of memory” (Ball et al., 2011, p. 632) of previous policies, and challenge a new policy.

When decoding or interpreting the policy, teachers relate to their experiences and histories which can influence how the policy is understood and enacted (Ball, 1994). Enactment may be problematic. Dienlin and Trepte (2015) argue that privacy concerns and privacy behaviours are a paradox; people’s concerns over online privacy do not match their actions. One recent finding is that those individuals who are most wary of online privacy actually disclose the most information (European Commission, 2011).
Ball et al., (2011), examine the context of policy enactment, particularly at the school level. They posit that schools develop their “own capacities for ‘coping’ with policy and assembling school-based policy responses” (p.586). In a December 21, 2016, Toronto Star article on the need to protect student digital privacy, the two largest school boards, in Ontario, the Toronto District School Board and the Peel District School Board acknowledged that they do not monitor, suggest or ban any digital tools in the classroom (Rushowy, 2016). Peel has a section in their Social Media Guidelines for Staff that gives some instruction on obtaining parental/guardian permission for the use of apps in the classroom, with a focus on social media use (Rushowy, 2016). Toronto has an Online Code of Conduct which advises never to give out personal information but does not specifically address doing so when having students log in to apps (Rushowy, 2016). As examples, both the boards aforementioned, are enacting policy with regards to the teacher (and to some extension, student) use of digital tools by creating board level responses to a policy lag. By conducting the research for this study in a small district school board, the data may describe the ‘school-based policy responses’ which Ball et al., (2011) describe.

2.3.5 Policy Trajectories

![Figure 8: Policy Trajectories (based on Ball, 1994 and Bowe et al., 1992) (Leatham, 2017)](image-url)
Once enacted, policies may or may not be realized exactly as they are intended, and may follow their own trajectories (Ball, 1994). The trajectory of a policy is dependent on the actors, the decoding and the contexts. Ball (1994) states that “Policies are represented differently by different actors and interests” (p. 17). As Yanow (2007) espouses, the meaning of a policy is dependent on the context of its analysis (p. 111). Bowe et al., (1992) describe the legal text as a ‘working document’ (p.10). It is these secondary texts, through the interpretation of the policy, from which the actors implement policy.

Bowe et al., (1992) identify three contexts of policy trajectories: of influence; of policy text production; and of practice. Policy discourses are initiated within the context of influence (Bowe et al., 1992).

The groups who influence the path of the policy are part of greater groups, such as the media and national bodies. The second context, that of policy text production, is the construction of the text for general understanding. These texts represent policy and take on many forms, such as policy documents (Bowe et al., 1992). It is these texts that attempt to interpret the policy for the public. It is at this point that the trajectory of a policy can change from its intention, as “[m]any...rely on these secondhand accounts as their main source of information and understanding or policy” (Bowe et al., 1992, p. 21).

In the case of the context of Ontario education, teachers can be influenced to implement online learning by the MOE’s 21st Century Competencies (2016) resource (Edugains, 2016), which appears to be incongruent with the OASBO (2016) video on the protection of student privacy. In the seventy pages of the MOE resource, the word privacy is mentioned once concerning digital citizenship (p.18) and only once does it indicate that teachers should “select appropriate digital tools according to purpose” (p.58). The OASBO video series, by contrast, is
predominantly about digital privacy. Ball (1994) reminds us that one policy cannot be 
examined in isolation but rather with other policies that may be in contradiction. Referring 
again to the MOE’s 21st Century Competencies (Edugains, 2016) teachers are encouraged to 
use technology and digital tools to engage students as well as prepare them for the future (p.24) 
yet the MFIPPA (1990) states that personally identifiable information (PII) of minors is not to 
be released. When using digital tools and apps, this policy contradiction needs to be at the 
forefront of teacher thinking.

This confusion and contradiction between key secondary texts come to the forefront in the 
third policy context, that of practice. The decoding of policy as text as described by Ball 
(1994) is where the readers bring their own histories to the policy they are reading (p.17). Bowe 
et al. (1992) also state that readers “have vested interests in the meaning of policy” (p. 22). 
Both articles quote Rizvi and Kemmis (1987), finding that policies are ‘interpretations of 
interpretations’ (Ball, p. 17; Bowe et al., p.23) from which “responses will be the outcome of 
contested interpretations” (Bowe et al., p.23). Therefore, the trajectory of a policy will differ 
from the initial writing, as it is decoded, interpreted and localized to different contexts and 
circumstances, and may contradict other policies in doing so.

3 Methodology

3.1 Overview and Design

This research study employs a survey (see Appendix B) to seek answers to the research 
questions. A survey was selected in order to reach as many teachers as possible within one 
district school board. A survey is a form of descriptive research, which according to Best 
(1970) is concerned with the following:
…practices that prevail; beliefs, points of views, or attitudes that are held; processes that are going on; effects that are being felt; or trends that are developing. At times, descriptive research is concerned with how *what is* or *what exists* is related to some preceding event that has influenced or affected a present condition or event (Best, 1970, p. 12).

According to Morrison (1993), a survey is useful also because it does the following:

- gathers data on a one-shot basis and hence is economical and efficient,
- generates numerical data,
- provides descriptive, inferential and explanatory information,
- gathers standardized information (i.e. using the same instruments and questions for all participants),
- makes generalizations about, and observes patterns of response in, the targets of focus; and gathers data from a wide population.

The online survey was designed to collect both quantitative (including demographics) and qualitative data from the participants – a mixed methods approach of convergent design was used in order to obtain complementary data (Morse, 1991). A convergent design, according to Creswell and Plano Clark (2011) collects qualitative and quantitative data at the same time. This convergent design allows for the illustration of the quantitative findings with the qualitative findings to present a fuller picture of what is happening. A benefit of this convergent design approach is that neither type of data is dependent on the result of the other. The analysis of the data will demonstrate where the data “converges, diverges...relates...and combines to create a better understanding” (Creswell et al., 2011, p.78). The use of convergent design in this research study connects with the research questions because the participants’ levels of awareness of policies, for example, can be shown quantitatively through choice options. Qualitative data are obtained when asking procedural questions (e.g., Describe a process for using new apps.). Open-ended responses in the survey ask teachers to elaborate on
their decisions surrounding the protection of student privacy, and collect qualitative data in the form of more in-depth responses. The use of both types of data allows for a fuller picture to emerge of teachers’ reasoning in order to understand teachers’ perceptions of the protection of students’ PII.

Table 2 below shows the alignment between the survey questions and the research questions in the present study. Questions from the survey which are not shown in the table included demographic questions, questions on the availability of devices both in the classroom and the school, and a reflective scenario to provide additional data not pertinent to this particular study.

<table>
<thead>
<tr>
<th>Research Questions</th>
<th>Survey Questions</th>
</tr>
</thead>
</table>
| 1. How do teachers in one district school board use digital tools in their classrooms? | 14. Which of the following types of digital tools are you using in your class or have used?  
15. What purposes do digital tools play in your classroom?  
16. How often are digital tools (as per the definition at the top of this page) used by the students in your class as part of their learning? |
| 2. How do teachers in one district school board describe their use of digital tools and continue to ensure digital privacy? | 22. What is your definition of digital privacy?  
23. In what ways do you protect student digital privacy in your classroom?  
24. When posting student information online/in apps, how do you protect student information (e.g., numbering the student, using first names only)?  
32. When using apps where you can post/upload student pictures, do you: (choice of answers) |
| 3. What is the current level of awareness of Ontario or district school board policies surrounding the protection of personally- | 29. Are you aware of any policy or procedure or understanding within your board regarding the use of digital tools/apps in the classroom? (for example, approval to use, buying/installing, privacy concerns)  
30. As a teacher, are you aware of any policy or procedure or understanding regarding the use of digital tools/apps in the classroom? (for example, legal obligations) |
Digital Privacy

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
</table>
| 4. How prevalent is student and parental communication through 3rd party apps in classrooms? | 17. How often are you using digital tools to communicate with parents/guardians other than through email?  
18. How often are you using digital tools to communicate with students other than email? |

Table 2: Alignment of research questions and survey

3.2 Participants

This survey was open to all teachers within one district school board which is a small board in terms of staff (>1000 full time teaching staff), though spread out across a large geographic area of 10,000 square kilometers both urban and rural. To avoid volunteer bias, Cohen, Manion and Morrison (2011) suggests aiming for extremely large samples. The participants were invited to complete the survey through an email sent by their principals on behalf of the research team.

According to Cohen et al., (2007) online data collection is becoming commonplace. One benefit of using an online survey is that the consent form can be embedded. Another benefit is that web-based surveys are cost effective, reducing the time to “distribute, gather and process data” (p.229) and respondents can answer from home, and/or at their leisure (Cohen et al., 2007, p. 230).

The survey used for this study created a sample through voluntary participation (volunteer sampling). As stated in the consent section (see Appendix B), the teacher-respondents were under no obligation to fill in or complete the survey. They could close the window to the survey at any time and their entered data would not be recorded.
3.3 Data Collection Tool: The survey

The survey was an online Google Form (see Appendix B). The design of the survey was to be able to ask broad questions supported at certain points with follow-up questions that asked for explanations. The survey was tested by less than five teachers from outside of the board being surveyed, and revised on their feedback. The goal was to have a survey which would be completed in under thirty minutes and was not heavy with open-ended questions.

Teachers were familiar with the Google Forms and the data automatically appeared on a Google Sheets spreadsheet. The data were housed directly in the Form and could be examined by individual answer. The anticipated time to complete the survey was thirty minutes, and a progress bar within the survey indicated status or time to completion. The survey was divided into six sections: consent form, participant information, classroom technology access, digital tool use, digital privacy and understanding digital privacy. The survey used an image as well as a video in the last two sections.

Demographic data collected asked if teachers were new or experienced, the panel and area of the district where they taught, and whether respondents held specific Additional Qualifications (AQs) in Special Education, Guidance or Principal’s Qualifications (PQP). These three qualification courses offer instruction in the protection of student data but not specifically digital data.

3.4 Procedure, Consent and Anonymity

The procedure to survey the teachers followed a six-week timeline. It began with sending the survey out via email to the entire school board. At week three, a reminder email was sent
based on the rate of response. At the sixth week the survey was closed, and analysis occurred through to the eighth week.

The consent form was at the beginning of the survey. If teachers consented, they chose the response ‘Yes, I agree’. If they choose ‘No, I do not agree’, their participation in the survey ended.

Also, if at any point during the survey teacher could exit the survey and end their participation. The survey did not record any names or email addresses, only timestamps when the responses were submitted. The survey was structured so that identifiers were general (e.g., in what area of the board do you teach?) so that neither the teachers nor their schools could be identified. The survey did not collect an email address, individual names or IP addresses. This was done to ensure anonymity.

3.5 Data Analysis

Data analysis occurred in stages using thematic analysis and descriptive statistics through content analysis. The thematic analysis enabled the data to emerge into patterns, which allowed for a generation of theory of the results. The descriptive analysis produced graphical representations of the data based on statistics and counts of answers. Specifically, the quantitative questions (multiple choice/closed ended questions) in the survey were graphed. This follows grounded theory (Glasser & Strauss, 1967) in the initial coding and categorization of data, followed by an intermediate coding through a constant comparison of the data to determine any unexpected results.

When the survey closed, the qualitative questions were separated into individual sheets within the overall spreadsheet, preserving the overall responses on their own sheet. Content
analysis, which is the examination of qualitative answers to determine themes, as well as conducting a count of words (Creswell et al., 2011) was applied. A first sweep of the open-ended questions sorted them alphabetically. This was done to identify common responses, such as nil answers (n/a, ‘I don’t know’, and empty cells). Specific words were coded by conditionally formatted words by colour (colour the font and/or the cell) based on their frequency of use. By filtering the individual words by their colour, a count of repetitive words could occur. The third step was a thematic analysis where the responses were clustered into categories by theme such as correct response, partially correct response and incorrect response. Once this was done, each response was read again to determine its accuracy or inaccuracy, and, if inaccurate, how the misconception was phrased. This process was repeated for all the open-ended questions in order to understand the teachers’ perspectives. Within the content analysis, when the coded words were counted, it transformed them into quantitative data by using percentages of responses and/or respondents to describe the findings (Creswell et al., 2011).

The data collection and analysis in this study more closely resembled grounded theory (Glasser & Strauss, 1967) for the following reasons. As the qualitative data were collected, they were organized into categories and coded. Also, findings emerged from the study which were unexpected. For example, multiple teachers indicated that they would not communicate with students online and this was later explained as possibly a result of a teachers' union directive. Other surprising findings were that they were using digital tools for classroom management more so than creative purposes. Also surprising was that a significant number of teachers responded that they had never tried an entire menu of digital apps and tools. Other surprising findings came from the review of the literature where gaps and contradictions were found in policy supports. For all of these reasons, the data analysis resembled grounded theory.
methods. At the same time, there was a theoretical framework which informed the study and this was used both for the policy analysis and the data analysis.

4 Results

In this section, the results of the survey of the teachers in one district school board are discussed. This chapter is organized into five sections. The first section reviews the demographic data from the survey responses. The next four sections of the findings have been organized to respond to each of the four research questions.

4.1 Demographics

Of the 957 possible respondents, participants returned 404 responses (n = 404 or 42% of the district) and 398 teacher participants completed the survey. The results indicate that the participants in this survey are from a wide range of years of experience (Figure 10). Teachers in their sixth to fifteenth year were the largest group, whereas there was almost an equal response from teachers who have taught 1-5 years with those who have taught 16-25 years. Looking at fifteen years as a midpoint in a teacher's career, there were 64.1% respondents in their first half of teaching compared with 36% in their second half. Using 24 years old as an entry age to teaching, this would mean that respondents were mostly in the range of 24-39 years of age, part of generation Y or the Millennial generation, a demographic that has always had the internet and technology (Forbes, 2014).

---

6 2 respondents did not consent and 4 people opened the survey but never submitted answers
The participants were split 64.1% elementary to 34.4% secondary for responding panels, which was close to the actual board breakdown (Figure 12). Respondents were also proportionate to the four areas of the board meaning that the respondents are an accurate representation of the boards’ teachers both in panel and geographic area representation (Figure 11).
One survey question asked if teachers held any of three specific Additional Qualifications. 221 people responded to this question, of which 91% held Special Education qualifications, 13.6% Guidance and 11.8% Principal qualifications. This question was asked because teachers who work in Guidance and Special Education have previous experience in understanding the need to protect student identity in documentation. Teachers who have taken the Principal’s Qualification Part 1 course learn about relevant Ontario legislation regarding education, including MFIPPA. From the OCT descriptions of the Special Education and the Guidance Additional Qualification (AQ) courses, candidates will learn “cultivating safe, ethical and respectful practices in the use of technology in purposeful and legal ways; critically exploring information and communication technologies that support student learning” (OCT, Section F, 2011). In all Aqs, the OCT Ethical Standards of the Teaching Profession form the basis for the course development, including the Standard of Respect which includes teachers modelling confidentiality (OCT, 2017).

4.2 Digital tools teachers used in their classrooms.

To answer research question 1, “How do teachers in one district school board use digital tools in their classrooms?”, one section of the survey asks the teachers four questions about
digital tools use in the classroom. These questions include the frequency of use of digital tools in their classroom, the purpose of the tool, the types of tools, and whether the tool was used for communicating with students.

When asked about which type of tool is being used in their classroom, the responses show that the Google Suite of Tools (See Appendix C: Digital Tools) and Smart Notebook are being used the most (74.6%), with Apps already installed on the network (e.g. MS Office) (58.8%), iPad/Android apps for creation purposes (52.3%), and parental communication apps such as Remind and Seesaw (55.5%) following (See Figure 12). Figure 13 breaks down the responses by how many tool options were chosen, of which 22.8% of respondents use 4 tools in their classroom (Figure 13). There were 24 ‘other’ tools being used, including (in the order they appeared) Clicker 6, web based apps, google website(4x), no technology use (5x), Class Dojo (which could be included as a LMS), YouTube, Idoceo, Kidblog and Powtoon.

![Chart showing usage of digital tools](chart.png)

**Figure 12: Which of the following types of digital tools are you using in your class or have used?**
Teachers were then asked the purpose for using the tool, and specifically communication purposes (with parents and/or students) was not an option. Teachers could respond as many options as they used in their class. Communication was specific to another set of questions and is noted further along. Teachers reported using digital tools primarily for presentation purposes (75.9%), followed by classroom management (71.9%) and then creative purposes (67.1%) (see Figure 14). Those who chose the ‘Other’ option, gave examples of other tool use for specific purposes which include (in the order they appeared in the responses): music programs, playing games, using apps that reinforce IEP and curriculum goals, research, reading, free choice for apps, activity based learning with apps and websites to consolidate learning, math specific apps for graphing, and access to people and resources (such as a Skype interview with a professional).
With respect to how often teachers are using the digital tools, 71.8% of teachers are using digital tools on a daily and/or weekly basis in their classroom (See Figure 15). Less than a quarter of teachers are using tools monthly or every few months. This would appear that digital tool usage is commonplace within the classrooms in this school district.

Teachers were also asked about the frequency of specific tools being used to communicate with students (other than email) (See Figure 16). The never option was the highest across the tools. A LMS (learning management system) was the most frequently used, followed by the Remind App, with the Seesaw app and a class website rounding out the responses. A breakdown of the most frequently used tools by both parental and student communications are in the table 3 below. Remind, then Seesaw, then a LMS are most frequently used to communicate (other than email) with parents, while the LMS is first for communication with students. Remind and Seesaw
were asked about because of the popularity of the tools as individualized methods of sending quick messages. *Remind* was also featured as a “time saving tech” in the September 2016 Ontario College of Teachers magazine *Professionally Speaking* with no mention of privacy considerations.

![Graph](image)

**Figure 16: Frequency of digital tool use to communicate with students**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Communicate with parents</th>
<th>Communicate with students</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Daily</td>
<td>Weekly</td>
</tr>
<tr>
<td>Remind</td>
<td>36</td>
<td>42</td>
</tr>
<tr>
<td>Seesaw</td>
<td>46</td>
<td>29</td>
</tr>
<tr>
<td>Twitter</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>Class website</td>
<td>21</td>
<td>20</td>
</tr>
<tr>
<td>LMS</td>
<td>34</td>
<td>41</td>
</tr>
</tbody>
</table>

*Table 3: Frequency of communication tool use*

In summary, the responses to the four survey questions indicate that the teachers report that they use digital tools frequently in the classroom, across nine different types of tools, and for a variety of purposes such as assessment. The responses in this section of the survey indicate that there is frequent usage of digital tools within the classroom, across platforms and for a variety of purposes. There are two main tools being used to communicate with students (an LMS such as Google Classroom or Moodle, and Remind). Google Classroom is contained within a school board’s network system and set up by the school board. *Remind* is a mobile...
phone app which texts students or parents and would not be considered an appropriate app per Ontario Elementary Catholic Teachers Association (OECTA) communication guidelines (see section 5.3).

4.3 Teachers and digital privacy.

The second research question, ‘How do teachers in one district school board describe their use of digital tools and continue to ensure digital privacy?’ was addressed in a section of the survey on teachers’ perceptions about digital privacy. There are eleven questions that asked about teacher’s understanding of the term ‘digital privacy’ followed by their understanding of educational policies which apply to the protection of student information. Three of these questions will be explored in this section.

For the question “What is your definition of digital privacy?” an analysis of the returned definitions and concepts associated by the teacher were coded. 398 responses were returned with 18 none/?/*/not sure/na. This was done by using spreadsheet software to sort keywords by frequency, which allowed the responses to be clustered into groups of similar wording (see Figure 16). Based on this, 128 of the teachers identified that "information" was critical to privacy and 68 teachers associated privacy in some way with access. 52 teachers responded that information should be protected.

To analyze the responses, the researcher first went through all of the responses and coded the responses which were accurate definitions. These were the responses that included an understanding that digital privacy is concerned with who has access to the digital information, and whether or not that information is kept private. Of the 398 responses, there were 48 accurate responses (12%) and 92 partially accurate (23.1%). Both accurate and partially-accurate responses totaled 35.1 % of the responses. This means that 258 or 64.8% of responses
were inaccurate. Of the accurate responses, a common element for what constituted digital privacy was that respondents are concerned with their information being accessed by persons other than with whom it was shared. Their answers used the words *confidentiality/not shared with whom it is not intended/not shared without permission/consent* (34).

Next, an analysis was undertaken of the numerous inaccurate or misconceptions provided in this response by the teachers. Some sample responses in answer to the question, “What is your definition of digital privacy?” are listed below:

- Do not post or print anything you would not say to your grandmother or priest/say to the whole world;
- pictures of yourself you would not like made public;
- my work and home life are separate;
- an illusory term intended to bolster an individuals [sic] sense of security, and autonomy.

Included in the inaccurate responses were *don’t know* (12)/*doesn’t exist/is possible* (14).

There were 5 responses that indicated that the use of the apps *Remind* and *Seesaw* was a means of keeping student information safe. From the analysis, two themes emerged: 1) who can access my information, and 2) protecting my information. Figure 16 (below) identifies the responses to this question in the order of most frequent to least frequent.

![Figure 16: What is your definition of digital privacy?](image-url)
The survey asked two questions specifically on how teachers protect student digital privacy. The first, “In what ways do you protect student digital privacy in your classroom?” asked about the ways this was happening in the classroom. For this question, the researcher coded the answers for frequency of terms (Figure 17) and then coded for proactive/protective ways and not useful ways/non-answers. The word don’t (don’t use digital/social media/apps, don’t do it, don’t post/don’t post pics) appeared 32 times.

![Figure 17: Frequency of terms](image)

There were 73 proactive/protective ways and 176 partly, which is 62.5% of respondents. 40 of the answers were not answered/non-answers (including no, not sure), and there were 109 ways given. Examples of proactive/protective ways included:

- 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;
- Each child has their own email, password and codes. I do not allow the students to share passwords. We also review Digital Literacy Etiquette to inform students of the proper and ethical use of technology, protecting one’s personal information, plagiarism, and on-line [sic] relationships.

Examples of not useful ways included:

- I assume they have their own privacy settings;
- Don’t look at what they are doing;
- clear the history and hope it works;
- board policy precludes students from expecting digital privacy.
The second question which is pertinent to this research question is “When posting student information online/in apps, how do you protect student information (e.g., numbering the student, using first names only)?”. The answers are seen in below Figure 18:

![Figure 18: When posting student information online/in apps, how do you protect student information?](image)

The remaining responses were varied. They are presented here from most frequent to least frequent responses. Though the teachers who wrote the responses below may believe that they are protecting student privacy, they are not fully. For example, Seesaw allows the sharing of content by the teacher to a public class page or to social media, and allows family members to share to third party services.

- I use Seesaw which is secure/ which is password protected – 34 teachers or 8 %
- I use Google classroom to protect privacy – 11 teachers.
- I follow the board-approved conventions and software – 3 responses.
- I block/cover/don’t show/ the faces – 4 responses
- I obtain parental consent to use photos – 3 responses

Individual teachers believe that the programs they are using establish the privacy settings. Here are some of their comments:

- I use the privacy setting.
● The program does the privacy for me.
● The website is secure if only parents use it.
● Only students and parents can access the information sent to them.
● My class Instagram is private. To use Twitter I seek parental consent for posting. I only post to Facebook. I only post to Edmodo. I only post to Remind. My class Instagram is private. I only share student names with the class Dojo.

Some other comments that are helpful for understanding the teachers’ perspectives are as follows:

● I only send student work to other teachers for professional development purposes.
● I try to post only the positive work as examples.
● I use discretion when I share student information.
● I am too worried about privacy to use online apps.

These three survey questions indicate that most of the teachers’ responses do not reflect an accurate understanding of what needs to be done to ensure student digital privacy. The teachers appear to understand that digital privacy involves protection of personally identifiable student information, and that access to such information should only be granted through sharing with specific people.

Many answers indicated that how sharing of information (photos, work, student information) was being done with individual parents. What may not be understood is that a photo of a student is considered PII (as a physical description can identify a person) in MFIPPA and that it needs to be protected as much as posting full names and other PII. The findings indicate that teachers are not cognizant of what constitutes PII as defined by MFIPPA (refer to section 2.2.1) and instead see privacy protection as providing permission to share, monitoring, and having passwords. Of the 61 teachers who used the word ‘share/sharing’ to describe how they protect privacy, it was in relation to passwords (13), work (5), accounts/logins (3) and photos (2). Two
teachers responded about not sharing personal information (though what information was not specified), and three were non-specific about what is shared.

4.4 Awareness of policies on digital privacy.

In order to determine research question 3, “What is the current level of awareness of Ontario or district school board policies surrounding the protection of personally-identifiable information in one district school board?”, the survey asked two specific questions regarding knowledge of policies or procedures in order to understand the current level of awareness of Ontario or district school board policies surrounding the protection of personally-identifiable information. The first question asked whether the teachers were aware of any policies at the district school board level, and the second question asked about teacher awareness of outside policies (e.g. legal obligations). Both questions asked teachers to elaborate on the multiple choice question on awareness.

When asked “Are you aware of any policy or procedure or understanding within your board regarding the use of digital tools/apps in the classroom? (for example, approval to use, buying/installing, privacy concerns)”, teachers had four options from which to answer (see Figure 19 legend). Over sixty percent of teachers were aware that a policy existed. The remaining 32 percent were divided into not being aware or not sure if there is a policy.
When asked a similar question but directed to policies at a level outside of the district school board, teachers had three options to choose from ("As a teacher, are you aware of any policy or procedure or understanding regarding the use of digital tools/apps in the classroom? (for example, legal obligations)). Less than half the teachers were aware there are policies, and over 50% were unsure or not aware of any policy (Figure 20). In summary, it is interesting is that more respondents were more aware of district level policies than other policies (67% vs. 47%).

Teachers were asked to elaborate on their answer to the above question ("As a teacher, are you aware of any policy or procedure or understanding regarding the use of digital tools/apps in the classroom? (for example, legal obligations))". Below are the highest answers by frequency.
Digital Privacy

divided into categories. These responses are organized in the following way: A are Yes responses, B are limited responses, C are not aware responses, D are misconceptions and E are not answered. An x indicates the frequency of the response.

A: Yes responses included, Yes, I know the policy and yes I would seek permission and yes I would protect student privacy = 108 responses in total (outlined below) or 30%

A1. Yes 56 responses (outlined below)
- I have read our policies: xxx I have read this policy xxxxx
- This issue has been discussed at a staff meeting/reviewed with us xxxxx
- I understand my obligations and responsibilities xxx
- We need to ensure that every app is safe for our students and their privacy and information is protected and confidential xxxxxx
- The Acceptable/Appropriate Use Policy covers this (e.g., Students and parents fill in a sheet at the beginning of the year) = 22 responses Not sure if the Acceptable Use Policy covers this x
- OECTA policies are in place. I would not be comfortable with student access to me as an individual x

A2. Yes, I would seek permission to use apps 24 responses (See below):
- Computer services provides training for this: xxxx
- Principal looks after this = xxxxx
- Librarian looks after this = xxx
- The computer expert in my building looks after this = xx

A3. Yes: As a teacher this is how I would protect student PII: (28 responses – see below for the highest answers)
- We need to protect the privacy of our students and our teachers xxx
- I use only Board-approved programs xxx
- I would check with my principal xx
- I would check the policy/read the policy if I wanted to use a new app xx
- The IT department looks after apps to be sure they are safe xxx
- I generally use only the apps on the IPads xxx

B Limited responses: Some knowledge / limited knowledge (56 responses – see below) or 16%
- Not sure where to find policy, I have seen it once, I have looked at it, Policy has not been made clear to us = 18 responses
- I am sure /aware that there is a policy to protect students but I have not read it = 36 responses
Digital Privacy

Teachers identify what they need (21 responses – see below) 5%

- I need to learn about our technology policies
- I need to know more about our legal obligations
- Concerned about legal obligations

C responses - Not aware /Not sure there are policies: 137 responses or 39 %

- I am not aware of any policies for the use of digital apps: 81 responses
- I am NOT SURE of any policies or procedures: 31 responses
- Have never been told what apps are allowed: xxx Have never been told there is a policy x
- Don’t know = 5 responses/Don’t know what the board policy says about digital tools xxx
- I do not know what I can and cannot use in the classroom or add to the iPad xxxxx

D. Misconceptions (35 responses – see below): 10 %

- I think there is a policy but I just use common sense (or best judgement) xxxxx
- I assume that iPad use has been approved by the Board as well as the apps xx
- I assume that if the app is on the computer then the Board has the licence xx
- That policy on apps applies only to some computers x
- The school board has a security block that keeps out unwanted apps x
- I know that certain apps have privacy issues so I use them with caution x
- It is a basic courtesy to respect others’ privacy but if there was a crime we would need to report it x

E: N/A No comment, NA, Don’t use apps = I never download an app xx 19 responses or 5%

Based on the written responses of the teachers, there is an indication that there is a high level of trust that the school board has checked every app, even though many teachers indicated a low level of knowledge of a relevant policy or procedure regarding digital tool use. This indicates a potential for student PII breach due to the lack of understanding of privacy and privacy policy. Of the teachers who indicate that they are aware of policies which would protect student digital privacy, the understanding of the policy as a protection tool was evident. With 39% of teachers indicating that they are not even aware that policies on privacy exist within and/or outside of the board, the implication for protecting student PII goes further than the use of digital tools in the classroom. Teacher misconceptions of policy and procedure
compound the lack of policy awareness, and indicates a potential willful ignorance when using digital tools.

4.5 Parental Communication

The last research question, ‘How prevalent is student and parental communication through 3rd party apps in classrooms?’ was addressed with two specific questions in the survey. As indicated in section 4.1, the question of using digital tools to communicate with parents and students were separate questions from digital tool use in the classroom. Just as the respondents were asked to indicate with which digital tools they communicate with students, (see section 4.1) the same question was asked of how they communicate with parents (other than email).

The responses were similar to the responses for communicating with students. A majority of teachers indicated ‘never’ for each type of method (see Figure 21). This indicates that, though 55% of respondents in a previous question on digital tool use in the classroom indicated that they use tools for parental communication, when the option is not email, the tools used most frequently (33% of teachers indicating they are using each) are either tools such as Remind (27%) or Seesaw (21%), and LMS (25.8%) tools are the most used.

![Figure 21: How often are you using digital tools to communicate with parents/guardians other than through email?](image)
Looking at the data set to respond to this question as a whole, teachers used the word *Remind* approximately 40 times as an example of an app being used to communicate with both parents and students. The application *Seesaw* appeared approximately 80 times as answers in different questions. This indicates that there is a dedicated use of the apps by a small number of teachers, which the graph above demonstrates (see Figure 21). Different from the student communication findings is that more digital tools are being used overall to communicate with parents, and more often (See Table 4 above).

### Table 4: Frequency of communication tool usage

<table>
<thead>
<tr>
<th>Tool</th>
<th>Communicate with parents</th>
<th>Communicate with students</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Daily</td>
<td>Weekly</td>
</tr>
<tr>
<td>Remind</td>
<td>36</td>
<td>42</td>
</tr>
<tr>
<td>Seesaw</td>
<td>46</td>
<td>29</td>
</tr>
<tr>
<td>Twitter</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>Class website</td>
<td>21</td>
<td>20</td>
</tr>
<tr>
<td>LMS</td>
<td>34</td>
<td>41</td>
</tr>
<tr>
<td>All other tools</td>
<td>28</td>
<td>44</td>
</tr>
</tbody>
</table>

### 4.6 Summary of the findings.

The data in this study indicate that within this school board, teachers are using digital tools frequently in their classrooms, and an array of tools for multiple purposes. There is a dedicated number of teachers who are using *Remind* and/or *Seesaw* frequently as a communication tool with both parents and students. The data also indicate that there is in an incomplete understanding of what digital privacy is, including that photos of students are considered PII
under the MFIPPA. Teachers responded that the protection of privacy is mainly through sharing permissions, monitoring students and having secure passwords.

In terms of policy awareness at both the district and the provincial level, teachers were more aware of district level policies than other policies (67% vs. 47%). Overall, 39% of teachers were unaware of any policy. This is significant with respect to protection of student PII and digital privacy when the level of use of digital tools is considered. Though the district school board has an AUP for both students and staff, as well as the MFIPPA, teachers are not enacting the AUP policy in its intended state, although the policy could be updated.

5 Discussion

The findings for this study, which showed that teachers had some challenges with defining and protecting students’ online personal identities, can be examined by framing the issue as a need for teacher development, or by framing the issue as a gap between the speed of innovation and the development of policy to regulate the innovation. Based on the findings from one, small to mid-sized district school board, the findings point to an innovation-policy gap (Davis, 2014) that is being realized in a district school board’s early technology adopters. In this discussion section, I examine how the implications of such a policy gap might be explained using Ball’s (1994) theory of policy as text and policy as discourse and teacher implementation of policy. The theories underpinning this study (Ball, 1994; Bowe et al., 1992; Fowler, 2004) help to explain the gap happening as a result of the speed of technology innovation when examined in the context of the policy enactment.

While we might want policies to keep pace with technology in a perfect world, the reality is that the pace of innovation (which moves quickly) is faster than the pace of policy in Canada.
The discussion for this chapter focuses on the gap between the design of the innovation and the design of policy and the implication of that gap.

5.1 The Innovation-Policy Gap

As stated previously in the review of the literature, Davis (2014) finds that policy has not kept pace with the rate of technology innovation and iteration. When examining digital privacy, there is a large difference between just North America and the European Union in the approach to the protection of privacy. See for example Bennett & Rabb (1997) who contrast the EU data protection directives with the US and Canadian laws and find North America lacking. Davis (2014) states that borders and the challenge of creating useful policy across them are a key issue to policy innovation. What is relevant for this study, however, is a knowledge gap. Davis explains a knowledge gap as a lack of understanding of how the deeper concepts of identity and privacy are managed across systems. He states that, “Policymakers must understand the complexities of how identity and privacy are technologically instantiated in any given system. Furthermore, they must understand how identity and privacy are managed generally across many different systems” (p. 88). The policy gap in Ontario educational policy points to the possibility that the policy makers have not understood the complexities of technology and its use in the classroom fully because they have not kept pace in updating/creating necessary privacy policy and procedures to address it.

As stated previously, there is no clear educational policy in Ontario that takes into account digital tools. This is a large policy gap. Though teachers are instructed to use technology (as per the philosophical front matter of current Ontario curriculum documents), the references to technology are vague and there are no recommendations about digital tool selection or considerations for privacy. Although the Health and Physical Education (MOE, 2015)
curriculum policy includes teacher prompts on digital privacy, its focus is on the use of communications technology, such as cell phones, to instruct students about the perils of sexting and cyberbullying. This indicates a gap in curriculum policy which is needed to address the safety of students’ PII when using digital tools in the classroom, and a gap in teacher procedure in choosing safe digital tools to use.

Unlike the United States, which has legislation such as FERPA, COPPA and SOPIPA which are specific to the protection of student information online, Ontario district school boards rely on Codes of Conduct for the overall regulation of student behaviour. Unfortunately, the provincial PPM 128 on Codes of Conduct (MOE, 2012) does not account for the online world that many students now inhabit, which also is indicative of a policy lag. This was supported by the findings of the present study where only 31.7% of respondents knew about, and had read, the district school board policy, and 32.2% of respondents were unsure/unaware of an existing policy. In fact, the district school board policy does address digital privacy but not with the kind of specificity needed for teachers to discern among communications applications to see which ones are the safest with respect to the protection of students’ PII.

If teachers are unaware of a policy which protects students, it is not a giant leap to predict that the protection of student data is not happening in a prescribed manner. For example, when posting online or emailing, teachers reported using first names or initials as a method to protect student identity, though this is not an indicated method in the policy documents studied. Ideally, a replication of this study would include a focus group to interview for more detailed elaboration of answers which would garner further insight into technology use in the classroom.

In summary, while Europe and the United States have clearly addressed the issue of PII in policy, Ontario has not. Teachers in this study had difficulty distinguishing between MFIPPA
in the physical world and the online world. Teachers were confused as to what PII could be taken and subsequently shared, for example with parents, while using digital tools.

5.2 Digital Privacy

The ramifications of this policy gap can be seen in this study’s findings which indicate that there is a partial understanding by teachers of what constitutes digital privacy. Many responses indicate that teachers have a good understanding of privacy, and are transferring a general privacy definition to digital one. For example, using the definition from Margulis (1977), “Privacy as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability” (p.10), many respondents saw a need to control who has access to their a) work and b) information. This can be seen in their answers as there were 34 instances that used the words confidentiality/not shared with whom it is not intended/not shared without permission/consent. Though there was a high frequency of responses which used the word information, it was not clear that digital privacy included the protection of personal information, rather it was centred around access to information (whether that was identity or documents).

In coding the survey answers to “What is your definition of digital privacy?”, the fulsome answer that was being looked for would have included points about protecting/securing personal information/identity (including examples) and unwanted intrusion/confidentiality. Only 35.1% of answers were considered accurate or partially accurate, which indicates that this area should be addressed. Many partial answers included the notion of access/control which correlates with Gülsoy’s (2015) definition of digital privacy. Digital or not, teachers are in a position of controlling information access of a vulnerable population and for which they are duty bound to protect the best interests of the student. While the responses of the teachers
indicated that they wanted to protect the students, there were clear indications that they did not know how to do this using the innovative apps suggested to them.

Teachers demonstrated also that they do not have a clear understanding of PII as it is outlined by MFIPPA. This was found in the answers in how they protect student digital privacy as the protection of passwords was highest, followed by names (Figure 8). Though having another person’s password allows for possible intrusion into their digital life, knowledge of PII will garner a deeper level of intrusion, as the more PII is known by a hacker, the greater their access. PII can be used to verify the intrusion (recovery emails asking for mother’s maiden name for example). Though 32.1% of teachers responded that they do not post student information online/in apps, this seems contradictory to other answers where teachers responded that they post pictures of students on multiple online platforms, as long as they have parental permission, or that they only post pictures and not names. Though obtaining parental permission is applaudable, perhaps a reflection of why pictures need to be shared and a proper medium for sharing should be discussed more. Teachers may not be aware that pictures are PII even if the student’s name is not attached to the picture. The practice of blurring or using a digital sticker on student faces, or only taking pictures from behind does more to protect student identity if there is a need to post a digital image.

There was an indication that teachers also have high regard for the digital tools being used in that they felt that the tool’s privacy settings/agreements are protecting users for them: for example, *I use the privacy setting; The program does the privacy for me; The website is secure if only parents use it.* This indicates a need for better understanding by the teachers of the privacy policies of the tools they are using to know what data is being asked for, what is potentially being shared to third party apps, and what data is being stored. Either this is done
by the school board who controls which digital tools are used within a district, or by the teacher at the classroom level, but more care needs to be taken with a critical lens to the purpose of the digital tool and the PII it requires.

In summary, teachers at a ratio of 2:1 indicated that they do not have an understanding of what digital privacy is, which highlights the need for policy and significant education for teachers on this topic.

5.3 Communication with parents and students

In the absence of a clear policy, it appears from the findings that teachers are attempting to match their knowledge of current policies to the digital world. In 2015, the Ontario Elementary Catholic Teachers Association (OECTA) published advice on electronic communication (2015) which advises teachers to not email students, and to never send confidential information by email. Yet, in a document from OECTA on parent engagement, it states “Effective communication is necessary to building good relationships and the key to managing or resolving misunderstandings and conflict” (OECTA, n.p, n.d), while reiterating the advice for the use of technology to do so.

In light of these contradictory directions to teachers from union communications, the findings about how teachers responded to communicating with parents and students becomes clearer. Two of the survey questions asked about the use of digital tools to communicate with both parents and students (other than the use of email). The overwhelming responses indicated that of the options presented, teachers were not using these digital tools or apps to communicate with either parents or students. Looking back at Table 4, teachers were communicating with parents slightly more on a daily basis than with students, of which this represented approximately 36% of the responses. Between 263 and 371 teachers responded with never for
the tools listed, which may indicate that email, phone calls and written communication with parents are still the favoured means of communication. Compare this with the use of digital tools to communicate with students, and it appears that teachers use an LMS the most, and the amounts for *never* were similar. One response for another question may give an indication for why digital tools are not used as frequently; “I see my students in person every day.”

In terms of digital privacy, the perceived lack of use of digital tools for communication purposes is a positive thing, as the less student PII is transmitted digitally, the higher the protection is. However, educators are expected to communicate regularly with parents on the progress of their child or adolescent. With the increased use of smartphones, it would make sense to use email and approved communication apps to give real-time/’just-in-time’ information to both parents and students for the purpose of awareness of student achievement, but this will need to be wrapped in a type of policy framework.

5.4 Summary

Ball (1994) states that in order for policy to be enacted, teachers need to commit, understand, be capable, have resources and have intertextual compatibility (p. 19). In this study, the findings indicate there is no policy for teachers to refer to that explains current digital privacy implications and obligations when using digital tools. Further, teachers may not be fully cognizant of what constitutes PII in the digital sense and may be inadvertently sharing information with digital tools not approved by their district, in order to share information including assessment data with parents. This may be because Ontario educational policy lags behind in terms of being current with the digital world that teachers are jumping into. There is a lack of policy and resources for teachers to understand and process intertextual compatibility of multiple policies which Ball (1994) states is part of enactment of policy; this impacts their
ability to adequately protect student PII while using digital tools. What policy is available to teachers has followed a trajectory though the decoding of policy within the context of practice (Bowe et al., 1992) where the policy is interpreted. In this study, teachers have enacted their own interpretation of OECTA advice to communicate with parents and students in absence of a clear policy on the use of digital tools.

6 Conclusion

This study examined the intent and realization of digital privacy in Ontario educational policy in the context of one small to mid-sized Ontario district school board. Teachers were surveyed on the topic of digital tool use and student digital privacy in order to come to an understanding of policy enactment. The study employed a survey to collect the data voluntarily from teachers, of which approximately 42% submitted a response. The study sought to understand in what ways teachers were protecting student digital PII when using digital tools in the classroom, as well as their understanding and/or awareness of policies designed to protect student’s PII.

6.1 Review of the Literature

An extensive review of the literature for this study explored how digital privacy was defined as well as laws and policy relating to digital privacy. A policy analysis toolbox was developed for a theoretical framework that referenced Ball’s (1994) theory of policy as text and policy as discourse; Fowler’s (2004) theory of policy actors and Bowe et al.’s, (1992) concept of how policies take on trajectories through implementation.

This study merged definitions of different authors (Margulis, 1977; Gülsoy, 2015) and define digital privacy was defined in two ways as:
1) the state of having control over what online personal data can be protected from intrusions from unwanted third-parties and

2) the right to protection of privacy when using digital media (Gülsoy, 2015).

These same themes from the literature also emerged in the findings. Teachers understand that digital privacy involves measures to determine who has access to digital information.

The literature review highlighted the need to include digital literacy and digital citizenship in curriculum policies (Berson et al., 2006b; Christofides et al., 2010; Shade et al., 2013). The analysis of policies for this study indicated that the Ontario curriculum policies have not yet addressed digital citizenship, but the survey indicates that teachers are seeking official sources to guide them. But while it has been theorized that desire to use an app takes precedence and outweighs the potential privacy intrusion (Dinev et al., 2013; Miyasaki et al., 2001; Norberg et al., 2007) this study shows that there are multiple, conflicting contingencies. Overall, however, there is a significant gap in the literature of academic research on the topic of student digital privacy when using digital tools in the classroom.

This study also examined Canadian and Ontario privacy laws to better understand who has legislated the protection of PII. The policy analysis found no distinct policy that addresses specifically digital policy, though acts do refer to the MFIPPA as the guiding act to define PII. In addition to this gap, a policy paradox was found – the use of digital tools is promoted without instructions or guidelines to protect student privacy when using the tool. The lack of Ontario policy contrasts with American policy: two federal and one specific state law have been enacted specifically for the protection of student privacy, and two address the online world.
6.2 Reflections on Methodology

While the digital survey provided a district-wide snapshot of the perceptions of the teachers with respect to digital privacy, the findings could not be generalized to every school board. The findings, could however be helpful in understanding how teacher’s problem-solve the pressure to communicate with parents and to use digital tools in the absence of curriculum policy and privacy policy.

6.3 Findings

The data revealed that close to 72% of teachers are using digital tools in their classroom on a daily/weekly basis, which indicates a robust use of digital tools with a high response to specific tools, such as the Google Suite of Education tools and Smart Notebook. There was a low incidence of digital tools used for communicating with parents. Digital tool use in this case may have been impacted by an advisory from the teachers’ union but without specific focus group data, this can only be speculated.

On the topic of digital privacy, teacher’s responses indicated an incomplete comprehension of the term and the implications of its protection. Further, teachers’ examples of how they protect student PII when using digital tools included safety measures that are indicative of pre-digital protection of privacy, with many misconceptions, and a low percentage of responses that were correct. This was not an unexpected finding, given the policy gaps found in district board and provincial level policies on the topic of the protection of student PII.

6.4 Recommendations

This section outlines recommendations for district school boards and the province of Ontario and faculties of education. One limitation of this study was that was conducted solely through
the use of a digital survey. Though this allowed for a large data set (398 responses), for certain
question an interview would have helped to provide greater insight. Also if this survey was
used in a different school board, a few of the questions would be modified to examine
awareness of union policy on communication with students and parents. Additionally, the
inclusion of a question for a process for having digital process would be beneficial. Also, the
survey used in this study was more an informal survey, than a standardized test instrument.

6.4.1 Recommendations for the district board level

Based on the responses, teachers in this district do not assume responsibility for the selection
of digital apps for use in their classroom and look to others ("the librarian/principal/computer
expert looks after this") for policy direction. The teachers reported that they would like to
know more about how to protect student PII, as well as the relevant policies. At the district
school board level, suggestions to improve teacher awareness, understanding and enactment of
privacy policies include: a) having a checklist of yearly opening procedures which details what
PII is and how teachers need to protect it with scenarios and a FAQ; b) continuous updates to
the district Acceptable Use Policy and included it as part of compliance/mandatory yearly
training for all employees who interact with students in any digital capacity; c) the creation of
district-specific procedures for the selection of digital tools for use in the classroom, in
conjunction with the district’s Privacy Information Manager; and d) including students in the
conversation as part of digital citizenship. Though teachers do not need to become experts in
digital privacy, they do need to cognizant of what to look for when reading privacy policies.
This is an ideal digital modelling opportunity, as students are expected to be critical readers of
texts, to go beyond a superficial understanding, so too do teachers when reading Professionally
Speaking, educational blogs and twitter or visiting conferences which tout the newest digital tool.

6.4.2 Recommendations at a provincial level

On a broader level, the lack of a specific policy which addresses the protection of student PII and digital tools needs to be addressed by the appropriate ministries in the province. Whether this comes through an update of PPM 128 or the drafting of a digital tool PPM which includes digital privacy, the lack of guidelines for teachers on which tools to use or even how to select them needs to be addressed. This includes: a) creating guidelines from the OCT for teachers or a Professional Advisory; b) an update of curriculum to the level of the Health and Physical education (MOE, 2015); and c) even further to be more specific in the front matter of curriculum about technology use, choice and privacy implications within the classroom. The province can also look towards legislation such as SOPIPA and be more proactive with the digital tools creators to ensure that Ontario laws are respected. The province should also consider how to update MFIPPA to encompass the protection of students' digital PII.

As stated by the Ontario Information and Privacy Commissioner, Ann Cavoukian, in 2007, Upholding compliance with Ontario privacy laws is not simply a matter of following the provisions of enacted legislation…Unless privacy policies are woven into the fabric of an organization’s day-to-day operations, they won’t work – full stop.” In hospitals, government offices and schools, privacy must become “embedded in the institutional culture” (Scott, 2008, para. 36).

Most teachers know from the OCT Professional Advisory and their union advisories that they should not use social media with their students, but they do not see the same stop sign when using digital apps in the classroom. This is the crux of the innovation-policy gap.
When teachers are bombarded by educational magazines, conferences, students and parents to use more technology in the classroom for engagement and communication purposes, the encouragement to use digital tools should also clearly outline the risks to student privacy. Given the absence of provincial policy direction on digital tool selection, where can districts, schools, and teachers turn in order to make sure that student privacy is protected? Teachers know not to photocopy or share information in an Ontario Student Record (OSR) from the moment they enter the system, but the transfer of the protection of student privacy in the digital world has not been outlined for teachers. Without clear policy, teachers are making decisions with insufficient information. They need to understand the significance and longevity of a digital footprint, and the need to protect students’ private information as they decide to use a digital tool.

6.4.3 Recommendations for Faculties of Educations

Faculties of Education are in an ideal situation to help through pre-service and in-service programs to address this topic. Though technology integration is in the philosophy section of Ontario curriculum policy, it is not whether or not Faculties of Education are addressing technology integration in content areas. At the very least, Faculties of Education need to help pre-service teacher make informed decisions about PII when entering the profession around both instructional and management uses of digital tools.

6.4.4 Recommendations for the College of Teachers and Teaching Unions

One of the findings of this study do not use email because they have been cautioned through an advisory by their union. At the same time, teachers are pressured to be in constant communication with parents. There are many parallels between the students’ understandings of digital footprints and teachers’ understandings. Unless teachers have opportunities for a
fulsome understanding of the implications of 3rd party apps, social media and email, teachers will continue to be caught between believing they are fulfilling their required mandate but operating in a policy vacuum.
Appendix A: Consent letter

You are invited to participate in an approximately 20-minute online survey which is part of a research project entitled, “The school board as a learning organization: Building capacity and leveraging technology” which is looking at teacher use of digital technologies. This study has been approved by the Leveraging Technology committee of the - and the UOIT Research Ethics Board REB #14301 on March 20, 2017.

This research is being conducted by Dr. Lorayne Robertson, Associate Professor, Faculty of Education, UOIT and Heather Leatham, who is a graduate student researcher. If you have any questions concerning the research study or experience any discomfort related to the study, please contact the researcher Lorayne Robertson at lorayne.robertson@uoit.ca. Any questions regarding participants' rights may be addressed to the research ethics board through the Ethics Coordinator: researchethics@UOIT.ca or 905 721 8668 ext.3693.

Any questions regarding your rights as a participant, complaints, or adverse events may be addressed to Research Ethics Board through the Research Ethics Coordinator – researchethics@uoi.ca or 905.721.8668 x. 3693

Your participation in the research is completely voluntary and will consist of answering questions related to the use of technology and specific digital tools in the classroom. Your responses are anonymous. Nothing in the survey will identify you. You are under no obligation to participate. You may stop participating in this survey at any point by closing the browser. If you decide after the survey to withdraw your data, that will NOT BE POSSIBLE because the survey form gathers the data continuously.

Purpose
This survey examines teacher use of digital technology and teachers' views on digital privacy and digital citizenship. This information will be collated into a report which is designed to support student learning and teacher professional development. Within the survey there are some questions which ask how you, as teachers, choose apps for classroom use. This is a topic which has not been examined in-depth in the literature and these findings may contribute to knowledge in this area.

Potential Risks: There are no risks to you for participating in this study. You may feel a sense of obligation to participate in the survey as the request to participate is being made to you through your Superintendent and principal, but your participation is absolutely voluntary.

Benefits: You may not benefit directly from participating in this study but by completing the survey, you will have an opportunity to reflect on how you make decisions about the selection of digital tools for use in your classroom and how you manage student digital privacy. This may be beneficial to your practice. The survey may also prompt new questions for you, and space is provided in this survey for teacher input.

Confidentiality and Anonymity: Participants will not be identified in this survey because the survey does not collect any identifiable information. You are not required to report to your
principal whether or not you have completed the survey. Your privacy shall be respected. No information about your identity will be shared or published without your permission, unless required by law. Confidentiality will be provided to the fullest extent possible by law, professional practice, and ethical codes of conduct. Please note that confidentiality cannot be guaranteed while data are in transit over the Internet.

Data Security: None of the data for this study contains any identifying information. The survey data will be collated and stored offline in a flash drive that is maintained securely by the principal investigator, Dr. Lorayne Robertson and the graduate student researcher. These raw data will be kept for only two years then deleted.

Debriefing and Dissemination of Results: The results of this study will be provided to the Leveraging Technology Committee in the form of a report. In addition, the graduate student researcher will use the data for her thesis which will be made available online. In addition, there will be other academic publications resulting from this survey, and access to these publications can be made by emailing the principal investigator: lorayne.robertson@uoit.ca.

Authorization
By clicking YES below, you agree that you do not waive any rights to legal recourse in the event of research-related harm. You are agreeing also to the following statements:

1. I have read the consent form and understand the study being described.
2. I have had an opportunity to ask questions and my questions have been answered. I am free to ask questions about the study in the future.
3. I freely consent to participate in the research study, understanding that I may discontinue participation at any time without penalty. A copy of this Consent Form has been made available to me.

I have read over the consent statement
☐ Yes, I agree
☐ No I do not agree
Appendix B: Sample of Teacher Digital Survey

Teacher Digital Privacy Survey
Thank you for taking the time to complete this survey. Your answers will provide data to help understand how technology is in use in the [district school board]. The information collected in this survey will not identify any individual person or school. Your IP address will not be collected. By completing this survey, you are consenting to having your information collected and used. There are 6 sections to this survey, the first being a consent statement. You may opt out of the survey at any point by simply closing the browser.

* Required

Consent Statement
You are invited to participate in an approximately 20 minute online survey which is part of a research project entitled, “The school board as a learning organization: Building capacity and leveraging technology” which is looking at teacher use of digital technologies. This study has been approved by the Leveraging Technology committee of the [district school board] and the UOIT Research Ethics Board REB #14301 on March 20, 2017.

This research is being conducted by Dr. Lorayne Robertson, Associate Professor, Faculty of Education, UOIT and Heather Leatham, who is a graduate student researcher. If you have any questions concerning the research study or experience any discomfort related to the study, please contact the researcher Lorayne Robertson at lorayne.robertson@uoit.ca. Any questions regarding participants' rights may be addressed to the research ethics board through the Ethics Coordinator: researchethics@UOIT.ca or 905 721 8668 ext.3693.

Any questions regarding your rights as a participant, complaints, or adverse events may be addressed to Research Ethics Board through the Research Ethics Coordinator – researchethics@uoit.ca or 905.721.8668 x. 3693

Your participation in the research is completely voluntary and will consist of answering questions related to the use of technology and specific digital tools in the classroom. Your responses are anonymous. Nothing in the survey will identify you. You are under no obligation to participate. You may stop participating in this survey at any point by closing the browser. If you decide after the survey to withdraw your data, that will NOT BE POSSIBLE because the survey form gathers the data continuously.

Purpose
This survey examines teacher use of digital technology and teachers' views on digital privacy and digital citizenship. This information will be collated into a
report which is designed to support student learning and teacher professional development. Within the survey there are some questions which ask how you, as teachers, choose apps for classroom use. This is a topic which has not been examined in-depth in the literature and these findings may contribute to knowledge in this area.

Potential Risks: There are no risks to you for participating in this study. You may feel a sense of obligation to participate in the survey as the request to participate is being made to you through your Superintendent and principal, but your participation is absolutely voluntary.

Benefits: You may not benefit directly from participating in this study but by completing the survey, you will have an opportunity to reflect on how you make decisions about the selection of digital tools for use in your classroom and how you manage student digital privacy. This may be beneficial to your practice. The survey may also prompt new questions for you, and space is provided in this survey for teacher input.

Confidentiality and Anonymity: Participants will not be identified in this survey because the survey does not collect any identifiable information. You are not required to report to your principal whether or not you have completed the survey. Your privacy shall be respected. No information about your identity will be shared or published without your permission, unless required by law. Confidentiality will be provided to the fullest extent possible by law, professional practice, and ethical codes of conduct. Please note that confidentiality cannot be guaranteed while data are in transit over the Internet.

Data Security: None of the data for this study contains any identifying information. The survey data will be collated and stored offline in a flash drive that is maintained securely by the principal investigator, Dr. Lorayne Robertson and the graduate student researcher. These raw data will be kept for only two years then deleted.

Debriefing and Dissemination of Results: The results of this study will be provided to the Leveraging Technology Committee in the form of a report. In addition, the graduate student researcher will use the data for her thesis which will be made available online. In addition, there will be other academic publications resulting from this survey, and access to these publications can be made by emailing the principal investigator: lorayne.robertson@uoit.ca.

Authorization
By clicking YES below, you agree that you do not waive any rights to legal recourse in the event of research-related harm. You are agreeing also to the following statements:
1. I have read the consent form and understand the study being described.
2. I have had an opportunity to ask questions and my questions have been answered. I am free to ask questions about the study in the future.
3. I freely consent to participate in the research study, understanding that I may discontinue participation at any time without penalty. A copy of this Consent Form has been made available to me.

I have read over the consent statement*
Mark only one oval.

☐ Yes, I agree
☐ No, I do not agree  Stop filling out this form.

Participant Information
This section is to collect demographic information to clearly report the results. Your individual identity will not be shared at any point in the data or the findings.

How long have you been teaching as a contract teacher? *
Whether part or full time, please indicate the length of time you have been teaching since you receiving a contract with the [district school board].
Mark only one oval.

☐ 1-5 years
☐ 6-15 years
☐ 16-25 years
☐ 26+ years

In which area of the board do you teach? *
Mark only one oval.

☐ Area 1
☐ Area 2
☐ Area 3
☐ Area 4

In which panel do you currently teach for most of the day? *
Please choose the option that best matches your current position (if split
Digital Privacy

between levels, which is the majority level you are teaching currently)

Mark only one oval.

☐ Elementary (early years and primary)
☐ Elementary (junior)
☐ Elementary (intermediate)
☐ Secondary

Do you have any of the following qualifications?
Please check all that apply

☐ Special Education (part 1, 2 or Specialist)
☐ Guidance (part 1, 2 or Specialist)
☐ Principal Qualifications (PQP1 and/or PQP2)

Digital Tool Use
The following questions help to provide an overview of the type and frequency of digital tools being used in the classroom.

For the purpose of this survey, the term digital tools will be considered to be any internet connected tool where the student needs to have an account in order to proceed. This would encompass web based applications, iPad/Android apps, smartphone apps and Learning Management Systems (LMS).

Which of the following types of digital tools are you using in your class or have used? *
Please check all that apply

☐ Parental communication apps (e.g., Remind)
☐ Google Apps for Education (Docs, Sheets, Slides, Forms, Draw, Classroom)
☐ Social Media (e.g., Twitter, Instagram, Facebook)
☐ Apps already installed on school network (e.g., MS Office Suite, subject specific tools)
☐ iPad/Android apps (for student creation purposes)
☐ iPad/Android apps (for documentation of student work)
☐ OSAPAC tools (e.g., Comiclife, gizmos)
What purposes do digital tools play in your classroom? * 
Please check all that apply 
*Check all that apply.*

☐ Creative purposes by students to create products to demonstrate learning (e.g., creation of videos, animation) 
☐ Classroom management purposes (including attendance, learning skills tracking, seating plans) 
☐ Content purposes (e.g., online textbooks) 
☐ Assessment purposes - for learning (e.g. online quizzes) 
☐ Assessment purposes - of learning (self/peer assessment) 
☐ Assessment purposes - as learning (documenting student learning) 
☐ Presentation purposes by students or the teacher (e.g., deliver content) 
☐ Curation purposes by students (e.g., gathering images, etc. to put together an assignment)

How often are you using digital tools to communicate with parents/guardians other than through email? * 
*Mark only one oval per row.*

<table>
<thead>
<tr>
<th></th>
<th>Daily</th>
<th>A few times a week</th>
<th>A few times a month</th>
<th>Once a semester/term</th>
<th>Only when necessary</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remind/Seesaw</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class blog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Digital Privacy

Smart Notebook
☐ Office 365 (Cloud based suite of tools)
☐ Learning Management Systems (LMS) (eg. Moodle, D2L, Google Classroom, Edmodo, Edsby)

Other: ________________________________
How often are digital tools (as per the definition at the top of this page) used by the students in your class as part of their learning? *

*Mark only one oval.*

- On a daily basis (3-5 times a week)
- On a weekly basis (1-2 times a week)
- On a monthly basis (1-3 times a month)
- On a semester/term basis (1-2 times every few months)
- Other:

<table>
<thead>
<tr>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter</td>
</tr>
<tr>
<td>Class website</td>
</tr>
<tr>
<td>LMS (eg. Moodle, D2L, Google Classroom, Edmodo, Edsby)</td>
</tr>
<tr>
<td>Facebook/Facebook Messenger</td>
</tr>
<tr>
<td>Text message</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>
Appendix C: Digital Tools

**Google Suite for Education (G-Suite)** - A collection of 6 main applications (Gmail, Drive, Docs, Sheets, Slides, Forms) that are housed within a district school board’s network. Accessed through a school board email login, each student and staff are given a gmail account. Allows for online collaboration and flexibility of access by logging in through the Google Chrome web browser.

**Smart Notebook** - Software for use with a Smartboard or interactive whiteboard display. Creates interactive presentations that allow for physical manipulation of objects on the screen. Part of the Smart Learning Suite of tools.

**Remind** - Mobile app that sends out announcements as text messages to students and parents. Teachers can also send files, have conversations and obtain read receipts of messages. Teacher phone numbers are not shown, and there is the ability to have one way or two way conversations.

**Seesaw** - Mobile (tablet/smartphone) app which functions as a documentation tool that allows teachers to upload pictures, videos or notes of student learning and then send updates to parents. Teachers are also able to assess student work through the app.

**LMS** - Learning Management System. Most popular at Desire2Learn (D2L), Moodle, Blackboard, Chalkboard, Edsby and Edmodo. Web-based platform where files, discussions, assessments, a calendar among other functions, are housed for each course a student is enrolled in. Allows students to submit work electronically.

**Kidblog** - Student blogging and portfolio app. Teacher controls to whom, when and how posts are published. Ability to see other classes work and comment. Allows for the integration of G Suite tools by students.

**Ideceo** - Mobile app for teachers which encompasses a daily planner, diary, gradebook, schedule and seating plan.

**Powtoon** - Online content creation tool to make animated presentation in a video format.

**Class Dojo** - Mobile app that tracks student behaviour and participation and give points. Parent communication tool through messaging, story of the day, videos and pictures. Schools can create communities to share broader.

**Clicker 6** - A web based visual literacy tool to scaffold the writing process for students. It helps increase writing fluency and vocabulary.
References


Bill 13, Accepting Schools Act, S.O. 2012 c.5.


Digital Privacy


Digital Privacy Act, S.C. 2015, c. 32.


Duckworth, S. [sylviaduckworth]. (2015, April 20). New #sketchnote: The 9 Elements of Digital Citizenship https://www.flickr.com/photos/15664662@N02/17190424026/... @dougpete @ICTEvangelist @alicekeeler. Image. [Tweet]. Retrieved from https://twitter.com/sylviaduckworth/status/590262107842617344


Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31


Human Rights Code, R.S.O 1990, c. H. 19


The Ontario College of Teachers Act, S.O. 1996, c.12.


The Personal Information Protection and Electronic Documents Act, S.C. 2015, c. 5.


Personal Health Information Protection Act, S.O. 2004, c. 3, Sched. A.


Students Online Personal Information Protection Act, S.B.1179, c. 839, s.22584.


