1. Executive Summary:

Ontario K-12 classrooms increasingly use digital applications and platforms. Consequently, private companiescollect more personal information, posing a potential threat to student privacy. Current privacy legislation does not specifically address education technology or its use by children, and current policies and practices do not sufficiently support schools and teachers. Because educational practices and legislative compliance are variable, Ontario schools cannot provide students with consistent personal information protection.

This brief considers a privacy pledge, provincial legislation, and a Ministry of Education commission as policy alternatives. In the interest of supporting student privacy, adapting to changing conditions, and providing both clear standards and flexibility to stakeholders, this brief recommends that a Ministry of Education commission be created to review and approve digital applications and platforms for classroom use.

Keywords:
Public education, Privacy, Policy, Ontario, Edtech
2. Scope of the Issue

Even before the current pandemic, digital applications and platforms were prevalent in schools. In 2019, 97% of Ontario elementary schools and 100% of high schools reported communicating with students using technology, including: email, class websites, web applications, and online classrooms (Kapoor, 2019, p.2). Interactivity of online platforms generates more data, which can be processed in greater detail (Zeide, 2017). Specifically, applications and platforms may collect information about when and how students interact with the platform, assignments and grades, and posts and communications (Reidenberg & Schaub, 2018). Massive data collection, and the profiles created with this data, pose privacy risks (Reidenberg & Schaub, 2018). These technologies collect more information than traditional classroom practices, posing a new threat to student privacy.

Private sector organizations, including those that provide education technologies, are covered by the Federal Personal Information Protection and Electronic Documents Act (PIPEDA). According to the rules set out by PIPEDA, organizations must: identify the purpose for collection, gain meaningful consent, collect only necessary information, retain information only as long as necessary, and be transparent about their information practices (OPC, 2019). Meaningful consent is especially complicated when the individuals in question are children. Consent is only valid if the individual can be reasonably expected to understand the collection (OPC, 2017a). Private sector organizations’ compliance with PIPEDA is open to doubt. The Office of the Privacy Commissioner of Canada (OPC) and the Information and Privacy Commissioner of Ontario (IPC) participated in a ‘sweep’ of educational applications in 2017. This sweep found that more than a third did not seek consent, and more than a third of the apps did not enable deletion of personal information (OPC, 2017a). Both contravene PIPEDA (OPC, 2017a). If PIPEDA is insufficiently enforced, children and teenagers are unfairly burdened with protecting their own privacy from intrusive personal information practices (Fric, 2014).

The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) covers personal information in Ontario schools (IPC, 2019a). MFIPPA defines the appropriate treatment of personal information (MGCS, 2018). Information is personal if an individual can be identified from that information on its own, or, in combination with other information (MGCS, 2018, p.133). School boards are accountable for online education services used in their schools. They must verify these services do not collect, use, or disclose student information improperly (IPC, 2019a, p.34). Again, compliance cannot be assumed. The IPC observed that some online applications
used by schools collect and retain information for their own purposes, track students, use information for marketing, and sell information, all of which may not comply with MFIPPA (IPC, 2016).

Directions from the Ontario Ministry of Education also cover digital applications and platforms. Between 2010 and 2011, the Ministry assessed digital learning in Ontario schools and released guidelines stating school boards need to make approved technology plans (CODE, 2011). However, school board practices do not follow policy. Burkell, Bailey, and Regan found variation across boards, schools, and classrooms in technology selection and use (2020). A sample review demonstrates the school board disparity; Toronto District School Board specifically addresses MFIPPA and security in their policies and procedures (2019a,b), whereas James Bay Lowlands Secondary School Board (n.d.) does not. The varying sizes of school boards and their respective budgets partially explain inconsistent digital technology practices.

Another source of variation is the behavior of individual educators. The IPC notes that Ontario educators often use online education, evaluation, and communication tools without knowledge or approval of the school or school board (2016). The IPC directs teachers to consult with the school and/or school board before using online services (2016). Unfortunately, a study found less than half of teachers felt sufficiently supported by their school/district in using networked technologies (Johnson, Riel, & Frose-Germain, 2016, p.43). Thus, there is variation between boards, between schools, and even between teachers.

This report finds unreliable handling of personal information by education technologies and inconsistent technology use in classrooms combine to create unreliable privacy protection. Current policies and practices do not adequately protect student personal information, and it is in the public interest that student privacy is sufficient and consistent.

2.1 Stakeholders

This brief considers five stakeholder groups. First, the school boards are given most of the responsibility for evaluating applications and platforms and protecting student information, as mentioned. This is challenging for smaller school boards. Therefore, clearer external guidance is in their interest. Second, teachers have an interest continuing to shape their own classroom practice through technology selection (Young, 2018). However, they lack actionable guidance for these selections. Currently, some school boards, schools, and teachers are providing consent on behalf of students, which they are not authorized to do (Burkell et al., 2020).

Children, parents, and privacy advocates are considered as the third group because they
share interests in student privacy and serviceable education. The United Nations’ Convention for
the Rights of the Child (1989) bestows children with the right to participate in decisions that affect
them in addition to protection from privacy interference. However, Burkell, Bailey, and Regan
argue that this right is not currently respected (2020). PIPEDA requires that children give mean-
ingful consent, and the OPC notes that this requires adapted processes if the children are 13 to 17
years old, or, parental consent if the children are under 13 years old (OPC, 2017a). Despite adapt-
ed consent processes, teenage consent is unlikely to be meaningful. A MediaSmarts study found
that when teenagers agree to terms of use, they do not perceive themselves to be giving consent
(McAleese et al., 2020). Parental consent is also not meaningful, because they feel unable to opt
out of using platforms (Desson, 2018). Furthermore, they worry schools cannot protect student
personal information (Pfeffer-Gillett, 2018, p.105). As such, parents and students have little influ-
ence over the technology they must use.

The fourth group, the provincial government, currently sets the guidelines for the use of
personal information. The fifth group, private sector application and platform producers, are driv-
en by profit motivations (Selwyn, 2018). Currently, industry choices have extensive control over
student information protection. Selwyn argues that policy for technology in education always in-
volves the private sector, because state agencies do not have the necessary resources to build these
tools (2018). This group’s interests do not necessarily align with the public interest, but they must
be considered.

3. Policy Alternatives

3.1 Privacy Pledge

One alternative comes from the Student Privacy Pledge, which is an American set of stan-
dards for education technology providers to voluntarily adopt. Since it was introduced in 2014,
more than 300 companies have signed (Pfeffer-Gillett, 2018). The pledge protects student infor-
mation through purpose limitation and required procedures for handling information (Pfeffer-Gil-
lett, 2018). However, a comparison found that signatory companies were no less likely to be in
violation of the pledge standards than non-signatory companies (Pfeffer-Gillett, 2018). With no
meaningful oversight or enforcement, the pledge allows companies to gain public approval and
disclaim liability for data use that violates the pledge (Pfeffer-Gillett, 2018). While this suits pri-
vate interests, it does not empower teachers, guide school boards, allow the provincial government
to maintain control over privacy standards, or protect students.
3.2 PIPEDA Replacement

Bill C-11 (2020), the Digital Charter Implementation Act, proposes the Consumer Privacy Protection Act, a replacement for PIPEDA that makes significant changes, and the Data Protection Tribunal Act, to oversee enforcement. The CPPA would introduce a requirement for plain language when asking for consent, which could increase the likelihood of meeting the requirements for meaningful consent, but still does not address children specifically. Through the creation of a specific enforcement body, the DPTA would likely increase compliance with legislation. However, the proposed acts would be broad, and therefore require significant translation and guidance for effective implementation in the classroom, where technology decisions are made by a complicated network of students, parents, teachers, schools, and school boards.

3.3 Provincial Legislation Targeting Education

A second alternative is supplementing provincial legislation with additional regulation for children’s data. Regan and Bailey (2020) suggest regulatory initiatives prohibiting corporate use of data from learning processes (p.77-78). Selwyn argues that effective state governance is possible if institutions are knowledgeable about digital technology in education (Selwyn, 2018). One example of direct government regulation is the US Student Digital Privacy Act, which was introduced to congress in 2015 to ensure data collection was only for educational purposes (Fitzpatrick, 2015, p.311). Such legislation may be too inflexible for the constantly changing trends in education technology, leading to inadequate protection for students. This alternative also does not guide teachers or school boards.

3.4 Ministry of Education Commission

A third alternative is the creation of a commission within the Ministry of Education to approve education applications and platforms. This is based on a report from the 40th International Conference of Data Protection & Privacy Commissioners, which outlines recommendations for improving e-learning platforms and suggests educational authorities create, “policies and procedures to approve platforms” (ICDPPC, 2018, p.3). This would be an ongoing project, where individual applications and platforms would be evaluated as required, and therefore, more adaptable to changing technological circumstances. This alternative would provide much-needed guidance to school boards and teachers. Centralizing the approval of education technologies would also increase student privacy, because larger collections of school boards have leverage to negotiate privacy protections that individual school boards lack (Regan & Bailey, 2020). Technology providers would benefit from clear approval across the province. Finally, with a list of approved applications...
and platforms to select from, teachers would retain control over teaching methods.

4. Policy Recommendation

Based on the alternatives, this report recommends the creation of a commission within the Ontario Ministry of Education. This commission would be responsible for:

- Creating and maintaining a panel of experts and representatives of students, parents, teachers, school boards, and education technology organizations;
- Performing an initial review to identify the most commonly used applications and platforms;
- Identifying standards for applications and platforms considering:
  1. MFIPPA,
  2. PIPEDA, and
  3. Recommendations from the 40th ICDPPC; and
- Reviewing and approving applications and platforms based on said standards.

This recommendation protects student privacy, respects educators’ autonomy, allows for innovation in the education technology sector, supports school boards, allows for flexibility going forward, and aligns with standards set by the provincial and national governments.

References

Bill C-11: An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to Make Consequential and Related Amendments to other Acts. (2020). 1st Reading November 17, 2020, 43rd Parliament, 2nd Session. https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

Burkell, J., Bailey, J., Regan, P., & Steeves, V. (2020, April 21). Children’s privacy is at risk with rapid shifts to online schooling under coronavirus. The Conversation. http://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787

Council of Ontario Directors of Education. (2011, June 30). Effective use of technology [Advisory No.3]. http://www.ontariodirectors.ca/CODE_Advisories/Downloads/CODE%20Advisory%20No%203%20WEB.pdf

Desson, C. (2018, June 11). As Google for Education tools enter classrooms across Canada, some parents are asking to opt-out. CBC Radio Spark. https://www.cbc.ca/radio/spark/401-google-for-education-1.4694935/as-google-for-education-tools-enter-classrooms-across-canada-some-parents-are-asking-to-opt-out-1.4694939

Fitzpatrick, K. C. (2015). Student data at risk: A multi-tiered approach for Massachusetts to mit-
igate privacy risks while utilizing innovative education technology in schools. *Journal of High Technology Law, 16* (1.5), 294–339.

Fric, A. (2014). Access of evil? Legislating online youth privacy in the information age. *Canadian Journal of Law and Technology, 12*, 141-170. [https://ojs.library.dal.ca/CJLT/article/view/6613/5798](https://ojs.library.dal.ca/CJLT/article/view/6613/5798)

Information and Privacy Commissioner of Ontario. (2016). *Online educational services: What educators need to know* [Brochure]. [https://www.ipc.on.ca/privacy-organizations/data-and-technology-management/online-educational-services-what-educators-need-to-know/](https://www.ipc.on.ca/privacy-organizations/data-and-technology-management/online-educational-services-what-educators-need-to-know/)

Information and Privacy Commissioner of Ontario. (2019a). *A guide to privacy and access to information in Ontario schools*. [https://www.ipc.on.ca/wp-content/uploads/2019/01/guide-to-privacy-access-in-ont-schools.pdf](https://www.ipc.on.ca/wp-content/uploads/2019/01/guide-to-privacy-access-in-ont-schools.pdf)

International Conference of Data Protection & Privacy Commissioners. (2018). *Resolution on e-learning platforms* [40th International Conference]. [http://enimerosi.moec.gov.cy/archeia/1/yp-p11157b](http://enimerosi.moec.gov.cy/archeia/1/yp-p11157b)

James Bay Lowlands Secondary School Board. (n.d.). *Policies*. [http://www.jblssb.ca/boardroom/policies/](http://www.jblssb.ca/boardroom/policies/)

Johnson, M., Riel, R., & Froese-Germain, B. (2016). *Connected to learn: Teachers’ experiences with networked technologies in the classroom*. MediaSmarts. [https://mediasmarts.ca/sites/default/files/publication-report/full/ycwwiii_connected_to_learn.pdf](https://mediasmarts.ca/sites/default/files/publication-report/full/ycwwiii_connected_to_learn.pdf)

Kapoor, A. (2019). *Connecting to success: Technology in Ontario schools*. People for Education. [https://peopleforeducation.ca/wp-content/uploads/2019/04/PFE_TechnologyReport_Apr2019-online-final.pdf](https://peopleforeducation.ca/wp-content/uploads/2019/04/PFE_TechnologyReport_Apr2019-online-final.pdf)

McAleese, S., Johnson, M., & Ladouceur, M. (2020). *Young Canadians speak out: A qualitative research project on privacy and consent*. MediaSmarts. [https://mediasmarts.ca/sites/default/files/publication-report/full/report_young_canadians_speak_out.pdf](https://mediasmarts.ca/sites/default/files/publication-report/full/report_young_canadians_speak_out.pdf)

Ministry of Government and Consumer Services, Information, Privacy and Archives Division. (2018). *Freedom of Information and Protection of Privacy Manual*. Queen’s Printer for Ontario. [https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual](https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual)

Office of the Privacy Commissioner of Canada. (2017a, October 24). *Key takeaways for online educational services and tools*. Global Privacy Enforcement Network Sweep. [https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-sweep/2017_result/](https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-sweep/2017_result/)

Office of the Privacy Commissioner of Canada. (2019, May 31). *PIPEDA fair information principles*. [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/)

Pfeffer-Gillett, A. (2018). Peeling back the student privacy pledge. *Technology Review, 16*(1), 100–140. [https://doi.org/10.1177/1477878518805308](https://doi.org/10.1177/1477878518805308)

Regan, P. M., & Bailey, J. (2020). Big data, privacy, and education applications. *Education and Law Journal, 29* (1), 55-78. [https://doi.org/10.2139/ssrn.3501191](https://doi.org/10.2139/ssrn.3501191)

Reidenberg, J. R. & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Practice Journal, Vol 6, No. 2,*
search in Education, 16(3), 263-279. http://journals.sagepub.com/doi/10.1177/1477878518805308

Selwyn, N. (2018). Technology as a focus of education policy. In R. Papa & S. W. J. Armfield (Eds.), The Wiley Handbook of Educational Policy. 457-477. https://doi.org/10.1002/9781119218456.ch20

The United Nations. (1989, November 20). Convention on the Rights of the Child. 1577 U.N.T.S. 3. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

Toronto District School Board. (2019a, July 11). Cyber risk and security. (Operational Procedure PR725). http://ppf.tdsb.on.ca/uploads/files/live/96/2213.pdf

Toronto District School Board. (2019b, April 17). Freedom of information and protection of privacy. [Policy P094]. http://ppf.tdsb.on.ca/uploads/files/live/96/2083.pdf

Young, N. (Host). (2018, June 8). Google for Education (401) [Audio podcast episode]. In Spark. CBC Radio. https://www.cbc.ca/radio/spark/401-google-for-education-1.4694935

Zeide, E. (2017). The limits of education purpose limitations. University of Miami Law Review, 71(2), 494-526.