For-Distribution

Ontario Education: Best Practice Technology Governance

A Pandemic Case Study of EdTech Sept 2020

This report is produced as a contribution to the Standards Council Canada Data Governance Standards Collaborative and references a submission to SCC_DGSC_Use Case - Consented Surveillance Data & Identity Trust Case Study (pdf)

Providing a research snapshot of the identity, security and privacy risks of student surveillance during the pandemic
September 2020

Produced by

Smart Species

In coordination with **Tech for Good Canada & The Open Consent Group**

Ontario Education Technology Governance Security & Privacy Snapshot Sept 2020

TABLE OF CONTENTS

SCC- Standards Gap - Meaningful Consent(sus) for consented surveillance

Abstract

Online surveillance is a critical issue as Canadian children are rapidly on-boarded to eLearning systems. The Coronavirus pandemic has created an environment of experimentation. It has forced the educational sector to consider alternatives to in-classroom learning, new processes that need to consider disparities in technological access, keeping students engaged, testing students remotely, understanding of learning styles (especially with school-aged children), and the processes that mitigate digital identity risks and exposure among, schools, teachers, parents, and students.

The pandemic has forced educators and parents to make quick decisions and develop alternative remote learning solutions. As of this writing, the Ontario government has created options to allow parents remote learning for their children. As well, learning pods are being created as alternatives and in response to concerns about the Ontario Ministry Back-to-School plan's ability to offer safe and sustainable options and social opportunities.

This research assessed the quality and transparency of the security and privacy risks for children in schools within Toronto, Ontario. The analysis was run across a small sample set of schools within the Toronto District School Board (TDSB). This analysis also included a sample of 21 education e-learning applications and technologies within primary, middle, and high schools that have been referred by elementary and high school educators.

These questions led to disturbing findings, including a hidden lack of transparency and security concerns within pandemic-strained school systems.

About:

Tech for Good Canada This work was conducted in collaboration with Tech for Good Canada, a non-profit group based in Toronto, and located throughout Canada, comprised of technologists, entrepreneurs, researchers and communication experts which aims to shine light on technology that is both "good" transparent in-nature and on those that are "bad" undercover by design. This particular initiative looked into the privacy, transparency and communicative practices of a select group of software resources chosen for use throughout schools in the Greater Toronto Area. Subscribe to Tech for Good Canada News - Abonnez-vous aux news de Tech à Vous Canada

Report Research Objectives:

- Highlight data governance gaps by focusing on educational tech gaps in conformance with PIPEDA principles.
- Provide guidance on *Meaningful Consent*
- Address active surveillance risks to children, including cyber and physical security risks.

1) **Measure the Extent of notified Meaningful Parental Consent:** In Canada, organizations are required to be legally transparent online and legally accountable. Interpreted in this research by the guidance provided by the Information Commissioner; To provide a clear notice of privacy and surveillance risks to people before any identifier tracking occurs.
    - Technically: This means companies must receive acknowledgment (like a notice receipt) of the risk and acceptance of any tracking, surveilling, or personal data use before meaningful consent can be demonstrated by an (online access only) service provider. Ensuring that collection, or use of data takes place only after notification.
    - The Notice of Risk in addition to the Notice for Consent is considered here as '2-Factor Consent' (2FC). The following criteria aim to flush out the qualities of the two-factor consent (2FC): with a suggested best practice of a (linked) Consent and Notice Risk Receipt in order to demonstrate online proof of Notice.
    - Questions about the online privacy information points:
        A. Is there an accepted (legally compliant) notice of risk and consent prior to the processing of personal data?
        B. Secondary Questions
            a. Is this transparent (in proportion) to the parent and student after the initial explicitly notified consent has been granted?
            b. Are privacy controls accessible in context of data capture and, are these controls usable in technical proportion to the data processing ?
2) Determine if there is sufficient security for consent to be valid: (Is it Fake Consent?)
    - Is data (meta-data) collected before consent is provided for an explicit consent legal justification for processing? .
    - Secondary security questions
        i. reviewing the location and storage of personal data
        ii. if meta-data and its data governance risks are mitigated

iii. can consent be fast tracked with a recognised certification and if so is implied consent viable for continued use of the online service

Security Review

The initial assessment results revealed a lack of apparent security safeguards this led to a review of the security and privacy guidance and governance policies of the school services infrastructure.

In particular, the assessment was focused on extra territorial and inter provincial privacy and security risks to children created by lack of cohesive policy implementation in and amongst provinces.

Reviewing policies for inter-territorial gaps at:

iv. School-level
v. School Board-level
vi. City of Toronto-level
vii. Ministry of Education/Province of Ontario-level
viii. Federal-level

The rationale: These two measurements used to provide a determination of current state of risk for all stakeholders and wether the implementation of internationally standardised consent notice receipts would address the standards gaps identified. In addition to the actual risks to students, parents, teachers, services, the province and even to Canada's digital borders.

Note: The security analysis has been removed from this report due to its sensitive nature and potential to increase risks of harm.

Ethnographic Research:

1. Ascertain if the individual (Parent or Student) using the services of an application or technology platform has an understanding of the risk in the context of providing explicit consent.
2. Explore the privacy impacts from a lack of understanding through the experiences of a parent a teacher and most importantly a child.
3.

Ontario Education Technology Governance Security & Privacy Snapshot Sept 2020

The rationale: By focusing on meaningful consent in cybersecurity and physical security policies, we begin to identify and expose the layers of risk in the education system.

Smart Species

Mark Lizar: CEO of Smart Species - trust@smartspecies.com
Sal D'Agostino : CISO OpenConsent Group Sal@openconsent.com

(Special Shout Out to Researcher & Investigator Hessie Jones for all the great work !)

Supported by Tech for Good Canada Advisory Board

Caroline Isautier : Founder, Tech for Good Canada
Digital marketer turned advocate for using Tech for good
Techforgoodcanada.com
https://carolineisautier.medium.com/

Smart Species, Open Consent Group, Arcade Consulting, York University and Ar Company:

Kate Tilliczek : Professor & Canada Research Chair
Youth, Education & Global Good
Director, Young Lives Research Laboratory
Faculty of Education, York University
https://younglivesresearch.ca

Catherine Halprin : CEO, Children's Media Consultant
Kid-Safe Ads, Diversity, Programming
arcadeconsulting.com | childrensmediainstitute.com

Heesie Jones: CEO ArCompany
AI Ethics and Privacy Technologist
Writer, AI technology and transformation Forbes and Grit Daily
Women in AI Ethics Collective, Arcompany

Assessment Methods

Assessing *Parental Consent* for education requires a parental perspective as well as a compliance perspective.

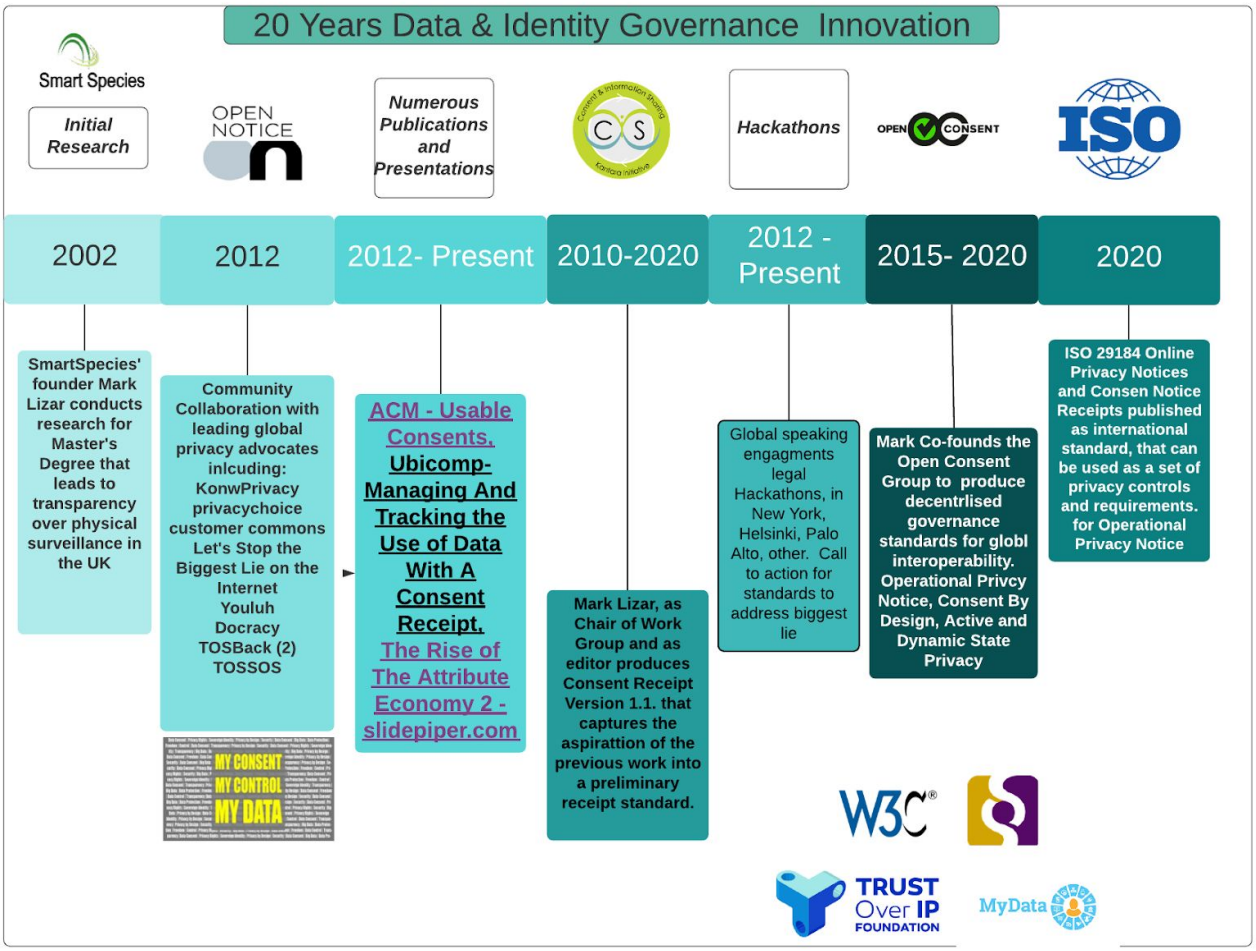
It requires a focus on defined legal requirements, for example;

> "Put it front and center, and emphasize the what, why, how and when of information collection, use and disclosure, and the possible (unmitigated)[1] risks of harm to which your customer is exposed if they give the consent."[2]

In order to assess the risk quality of "Parental" Meaningful Consent for children and youth we approached the research from the perspective of a parent as well as measuring the performance of privacy compliance. Recording policy and notice indicators of surveillance by design (e.g. surveillance before consent is provided)

[1] in ISO 29184 the notice requires is only for the (unmitigated) risks, like those not mitigated with standards.

[2] https://www.mcinnescooper.com/publications/what-the-privacy-commissioners-new-pipeda-meaningful-consent-guidelines-mean-for-organizations/



Auditing: 2 Factors of Notice for Meaningful Consent

Researcher Note: There are many factors to an explicit consent depending on the content and the type of consent provided in context for a human. Online notice often needs to be multi-factor, to ensure knowledgeable, informed, and explicit consent entailing a hybrid online and offline approach.

For this assessment consent was interpreted as the initial grant of human permission “required to obtain meaningful consent for the collection, use and disclosure of personal information with digital identifiers. Consent is considered meaningful in this context when individuals are provided with clear information explaining what organizations are doing with their information.”[3]

3

First Factor: is a prior notice of the risks for data collection from the service provider for the data which is being collected and its purpose of use. We look for a read receipt, then an additional notice for the purpose of consent and the capture of the consent grant for use in identifier based systems.

Second Factor: an individual receives a second notice with a receipt for explicit grant of consent to process personal data and a record / notice and consent receipt with the permissions established in the system to process personal data.

As of this writing, September 2020, the Ontario government has created options for parents to allow remote learning for their children. Concerns continue to loom among teachers and parents regarding the safety and efficacy of Ontario's back to school plan. Parent groups across Canada are offering learning pod alternatives that offer safe and sustainable options for children. Regardless, the dependence on education technology and the increasingly networked classrooms means that wether kids can access, use and learn with these tools or not, we re all being what is known in the identity management industry as "on-boarded" invisible data breach is applicable and present for all current options.

Generated Insights for Peer Review

This research provides a snapshot into the data governance state of education technology in Canada. The findings include the Toronto District School Board, and in Ontario and a random sample of 21 education applications and technologies utilized within primary, middle and high schools

Teachers and Peer Interview Insights

- What's been communicated by educators is the need to find free applications and anything that can "fly under the radar" to support their curriculum development, and avoids going through the channels for approval. Based on anecdotal research, the TDSB does not have specific criteria for evaluating third party service providers, although they provide a specific list of applications that are blocked. In Ontario, education data governance policy does exist for Ontario School Records (OSR) but does not extend to third party service providers. Therefore, many applications are not actively reviewed or audited beforehand. What's clear is the disparity between the policies and addressing the pressing needs of teachers to provide processes and solutions that will work.
- While there are clear policies at the provincial, school board level, and the national level, there is also a lack of enforcement at the school level. All too often teachers use education technology that has been peer-recommended. As well, given the layers of approval required to get software approved, teachers may turn a blind eye to this process.
- EdTech applications are not vetted by school administrators for privacy compliance and more often than not, are flying in around the governance radar, with mis-leading claims of privacy. Adding to this are cyber and physical security policies inconsistently applied across schools. The result is an education system that leaves children more exposed, parents largely unaware, teachers' pressed to deliver effective curriculums without understanding the impacts of these applications, and IT administrators, stretched to deliver services at the expense of policy mandates.

eLearning Platform: Transparency Compliance

- Both D2L and Google platform technologies were unable to confirm best practice by providing prior notice of risk for processing personal data nor providing separate notice of consent.
    - D2L and Google were unable to overall satisfy the conditions for 2FC (2 Factor Consent). Despite the extensive privacy policy and security disclosures on their public facing site, they did not conform to best practice in providing notice of risk prior to processing of personal data. This user experience is surveillance by default.
    - As well, both were unable to satisfy the question: Did the company provide a separate notice of consent to parents (with children under the age of consent) and students?

- Education technologies, in aggregate, were unable to sufficiently provide best practice for 2FC (2 Factor Consent). These 21 companies averaged a score of 15.02% out of a possible 100% for the first criteria (prior notice) for 2FC and 12.7% out of a possible 100% for the second (notice of consent) criteria. A perfect score means companies were able to conform to industry best practice, and usually may meet the applicable legal requirements. The low average scores imply all companies were unable to conform to best practice and/or were unable to identify risks to person(s) before the data collection or use. This was particularly visible in the questions that dealt with the security of personal information. Only one-fifth of the technologies had or provided visible security and data protection policies.
- All technology applications including both D2L and Google when URL is entered on Brave Browser reveal the existence of ad trackers or tags. None of the technologies have provided prior notice or this risk. In addition, there is no clear cookie notification displayed on the home page or parts of the sites.
- Most of the EdTech companies were unable to satisfy the meaningful notice of risk criteria and did not specifically point to clear policies about data security and protection of identifiers and metadata associated with children' to satisfy PIPEDA principle 7 safeguards and meaningful consent notice of risk criteria.

Avenues to Explore

How effective are the ISO 29184 and related Consent Receipts standard for governance of data portability for the purpose of individual controlled data sources? How effective are privacy rights and moving data control to people?

Recommendation:
Utilise transborder and technical domain standards to address the significant territorial risks, work to unify notice and consent practices

lack of standards are apparent in the observed difficulty all stakeholders are experiencing in implementing proportional safeguards.

This struggle is Visible through:

- Disparate levels of training
- Different policy across schools and boards
- Lack of implementation of existing policies and recommendation such as the 2018 audit report in Ontario
- Different policy across services providers and operators
- Different policy at the federal level
- Lack of effective implementation of industry codes of conduct and practice for the provision of physical and cyber security services and countermeasures.

Appendix Assessment Questions Two-Factor Notice for Parental Consent: (2FC)

1. **Is there a notice of the risk prior to the processing of personal data? Applicable Questions:**
    c. Why are you collecting this information and what are you using it for?
    d. Has a third party audited this to ensure the company has complied?
    e. How is the information protected?
    f. Is your child's data is being stored, is it encrypted?
    g. Can the company detail how they're protecting your information?
    h. How is the company protecting your information from malware?
    i. How are the encryption keys being stored or protected?
    j. Are there Information technology and Security and Data protection policies provided by the organization?
    k. Does the organization provide information about protections against unintended disclosure of PII in public reports?
    l. Does the company provide Data retention policies including how they retain records in identifiable, redacted, and/or de-identified form?
    m. Does the company share information with third parties?
        i. If so, with whom and for what purpose?
2. **Do parents or data subjects (within legal age of consent) receive a separate notice of consent?**
    n. Does consent happen when you sign up?
    o. Do you, as a parent, have enough information to provide consent on behalf of a child who has not reached the age of consent?
    p. What was your experience in getting the questions answered?
        i. Were the responses sufficient and provided to you in a timely manner?

Each of these questions have been applied to the Education Tech vendors by review of the existing publicly available Privacy Policy and Terms of Service, and a follow-up (if required) through a subject access request.

*Notes: the sampling of Education technology used for the purposes of this report were provided by education professionals and teachers within the TDSB

Nota Bene: Smart Species was an active participant in the 2016 consultation on the issue of consent under PIPEDA, and representing the Kantara Initiative. The goal of the consultation was to identify improvements to the current consent model and bring clearer definition to the roles and responsibilities of the various players who could implement them. This helped lead to the announcement Jan 2019, that businesses must follow more robust guidelines on meaningful consent for personal information[4] .

[4] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181221/

References -

PIPEDA - Consent Explained as :“Consent is a key element of the Personal Information Protection and Electronic Documents Act (PIPEDA)[5], Canada’s federal private sector privacy law. Under PIPEDA, organizations are ”

Smart Species - SCC-Consent Surveillance Case Study

*****

[5] PIPEDA https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/