DISCUSSION HANDOUT
STANDARDS FOR CHILDREN'S SURVEILLANCE – FUTURE USE CASE
FOR THE DATA GOVERNANCE STANDARDIZATION COLLABORATIVE
February 2021

ABOUT THE DISCUSSION

Today, due to COVID, in-person interactions have become restricted, so traditional sectors and institutions are having to react immediately to reshape their frameworks to adapt and compete in a digital environment. The COVID-19 pandemic has exposed weaknesses in the area of online surveillance which has become a critical issue as Canadian children adapt and are on-boarded to e-Learning systems.

Lack of data governance standards, enforced privacy regulation, and the implementation of consistent operational or security procedures in schools exposes children, parents, and Canadian society to risks. This is a critical issue as provinces have traditionally viewed privacy as a cultural point of distinction regionally and this is contributing to serious cyber security issues.

This is especially apparent with the onboarding of e-Learning systems in schools due to the pandemic. This raises resinous concerns for Canadians related to the processes that mitigate digital identity risks and exposure among schools, teachers, parents, and students.

We would like to continue to hear directly from stakeholders and Canadians on this important topic.

This future use case focuses on children's surveillance and e-Learning systems. Results from this discussion will be combined into a report that will be incorporated in the final Data Governance Standardization Roadmap under "On the Horizon", pointing to the need for continued vertical discussions on data governance as it impacts different sectors, with recommendations that this sector could be a potential use case for future versions of the Data Governance Standardization Collaborative Roadmap.

This discussion will allow the Standards Council of Canada (SCC) and participants to learn about Canadian's perspectives, and to learn more about work being done in this area. The conversation will revolve around two main areas. The first will focus on the current state of online surveillance in Canada and their data governance frameworks:

- What are the current challenges for technology governance with regards to online surveillance (i.e., what information is required, how secure is the information, who has access)?
- What rules, regulations, or standards currently exist, that you are aware of, to regulate online surveillance?
- What rules and regulations are relied on now?

The second topic will focus specifically on the future of technology governance and online surveillance:

- What is the ideal future situation of online surveillance in Canada (i.e., what are the ideal opportunities, what benefits can consumers/service providers reap from increased use of online surveillance)?

- What does Parental consent look like with the PIPEDA (privacy law) update and with the use of emerging data governance standards?
- What rules, regulations or standards are necessary for a technology governance and online surveillance framework in Canada?

The conversation will feature a brief presentation on the role of the Data Governance Standardization Collaborative (DGSC) and future use cases, as well as the importance of standards and the current state of online surveillance in Canada.

For more information on the Standards Council of Canada or to learn more about standards, please visit https://www.scc.ca/en/about-scc/what-we-do.

BACKGROUND

The Standards Council of Canada (SCC) established the Canadian Data Governance Standardization Collaboration (DGSC) in late 2019, in support of Canada's Digital Charter. Debate is growing in Canada about who will own, control, and benefit from the massive amounts of data generated across the economy. The Federal government's new Digital Charter is looking for standardization to help ensure that Canadian businesses prosper in this new environment and for Canada "**to be proactive and take a leadership role in emerging areas in digital and data management, helping to establish benchmarks or global standards**."[1]

SCC, as a crown corporation that reports to ISED, established a Collaborative to identify standardization priorities for Data Governance in Canada, which include delivering a roadmap describing the current and desired Canadian standardization landscape. This roadmap will include recommendations on "**how codes of practice, certification and standards can be used to adapt principles-based law to particular sectors, activities, or technologies, and to make frameworks more agile"** and more trusted by Canadians. More information on this effort can be found here: https://www.scc.ca/en/flagships/data-governance.

However, with abstract concepts such as data governance and the role standardization can play in collection, sharing, and use of data, it can be challenging to understand the impact or relate to it from an every day perspective, especially when data is an "intangible" asset. To help stakeholders understand the role standards can have in supporting data governance and trust, use cases are being used as relatable examples or stories stakeholders can talk to.

Educational technology (EdTech) has long posed privacy concerns and equality problems. With the increase in EdTech and e-Learning systems to support remote learning during the COVID-19 pandemic, there is a need to develop initiatives and common operational procedures to support online surveillance and mitigate the significant risks associated with digital identity, security, and privacy. Schools are often not fully aware of the risks and implications of online privacy and security such as the sale of student data to third parties for the purpose of advertising, tracking of student activities inside and outside of the classroom, and loss of student autonomy due to ongoing monitoring of their activities[2]. Online surveillance for e-Learning systems needs to become a priority for policymakers, politicians, and business leaders to bring online surveillance into government,

[1] Government of Canada. Canada's Digital Charter in Action: A Plan by Canadians, for Canadians. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html.

[2] Jane Bailey. RSC. https://rsc-src.ca/en/voices/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus

address privacy and security problems in digitally networked environments, and ensure that individuals apart of the various communities in Canada are accommodated.

ONLINE SURVEILLANCE AND STANDARDIZATION

In the age of COVID, in-person interactions have become restricted, so traditional sectors and institutions are having to react immediately to reshape their frameworks to adapt and compete in a digital environment. The COVID-19 pandemic has exposed weaknesses in education data governance policy. Lack of regulation, standards, operational procedures, and a common policy to support online surveillance, especially with the recent increase in e-Learning systems due to the pandemic, raise concerns for Canadians related to the processes that mitigate digital identity risks and exposure among schools, teachers, parents, and students.

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. For example, education data governance policy in Ontario does exist for Ontario School Records, yet it does not extend to third party service providers. Therefore, many applications are not actively reviewed or audited beforehand. EdTech applications are often not vetted by school administrators for privacy compliance, which can result in misleading privacy claims. Combining these EdTech applications with the fact that cyber and physical security policies are inconsistently applied across schools results in an education system leaving children more exposed, parents unaware of the risks, teachers faced with pressure to deliver effective curriculums without understanding the impacts of these applications, and IT administrators stretched to deliver services at the expense of policy mandates. There has been significant regional variation in the K-12 systems in Canada with respect to the implementation of EdTech, and has resulted in some platforms and services, such as Zoom and Skype, used for education even if they have not been designed for educational purposes[3]. These types of services and platforms often collect a great deal of personal information about students, such as a student's school, name, and use of the platform, which can pose long-term risks[4] to student privacy and autonomy.

In addition, the research study supporting this sector found that most EdTech companies did not provide meaningful consent for parents and notice of risks. Data security, transparency and protection of children's e-Learning identifiers (metadata) that is associated with children to satisfy PIPEDA Principle 7, safeguards and meaningful consent notice of risk.

This is a concern for Canadians as it has indicated that e-Learning platforms and education technology companies do not provide meaningful parent consent or best practices for 2 Factor Consent (2FC), referring to both prior notice of risk and notice of consent. Parents are unable to identify risks to their children before data is collected or used. Sufficient best practices as demonstrated by 2FC is important for an e-Learning platform as it ensures the education technologies provide legal parental consent and conforms to industry best practices. These concerns are particularly visible in questions related to the security of personal information; where it was found that only one-fifth of the technologies had or provided visible security and data protection policies relevant to Canada.

With the pivot to education through e-Learning platforms and other virtual means to support in-classroom learning, there is a need to evaluate harms to vulnerable children by the virtual platforms used to support the educational sector. Most, if not all, technologies and e-Learning

[3] Jane Bailey. RSC. https://rsc-src.ca/en/voices/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus

[4] Jane Bailey. RSC. https://rsc-src.ca/en/voices/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus

applications used have not been properly secured to combat and mitigate online surveillance concerns, digital identity risks faced by schools, teachers, students, and parents. Ensuring coherence among the policy and operational procedures of education and social media technology in Canada is a critical concern. Not only for parents but for Canadian society.

The use of Canadian metadata without consent highlights that service providers have been profiling Canadians' data and aggregating this data to build social media products without safeguards to protect Canadians. Aggregating data to build products, that give service access to this data, in contravention of Canadian privacy law, culture, and expectations.

The protection of children's meta-data in e-Learning is imperative in mitigating the significant risks posed by factors such as disparate levels of training, different policy across schools and boards, lack of implementation of existing policies and recommendation, different policy at the federal level as well as across service providers and operators.

With these challenges in mind, standardization is required for consented online surveillance frameworks to reflect the values of Canadians and to support the needs of children when exposed to online surveillance. This possible future Data Governance use case could champion best practices for the provision of physical and cyber security services and countermeasures for the future of digital Canada.