Case Study for Notice & Consent Receipts (ISO 27560) to govern Consented Surveillance

Ontario Case Study Contribution: Canadian Data Governance Standardization Collaborative (DGSC) - WG1 - Meaningful Consent (and Consensus)

Educational Data Trust Use Case for Children and Youth Data Record Governance	*Description* Common to all of these issues a common theme or component, the transparency and security of consent(ed) or consensus-based surveillance know as Meaningful Consent. With respect to the Data Governance Gaps identified by the collaborative, this use case is for a very specific item for Data Management Governance, which is the governance of surveillance consented to, or consensus-based (legally justified) like Covid tracking. A personal data tracking and surveillance activity, which is undertaken for safety of the public. Referred often as in the public interest. Consented and transparent disclosure of data is an extremely valuable resource that is used to address data governance gaps. *Scope of Use Case focus* This use case takes an operational research approach under the gap identified in Issue: 16 Data Privacy, focusing on (standardised) transparency for who is accountable owner of data processing services, who benefits from data processing, who is the beneficial owner of the processing organisation are key questions impacting cyber security online. This gap use case is further focused with a Provincial Case Study for Issue 50: Secondary use of Data, including metadata and its current forms of governance. By reviewing the implementation of privacy / policy frameworks based on PIPEDA and the Canada Act, in the Ontario education ecosystem. Specific objective is to draw attention to research depicting this governance gap with an initial set of recommendations to protect vulnerable Canadians and provide an ethical approach to addressing this gap with trial of best practices with standards in Phase 2 of the SCC Road map. One output will be the development of targeted and specific guidance on implementing standards for the trustworthy and ethical secondary use of data in open data trusts as this is a consistently presented data governance gaps across issues identified. **Key Issues** issue: 16 Data Privacy Issue: 50 Secondary use of data

	Problems There is an urgency regarding the regulation and protection of the processing of personal data in Canada at all levels of governance. Canadians' privacy expectations are not respected by most services based online. The privacy compliance for PIPEDA and the provinces are not clear; they are also overly complex for services to comply with or for adequacy interoperability with external jurisdictions. As a result services do not respect (or are unaware of) the Canadian privacy compliance requirements, thus revealing the surveillance transparency gap for operational implementation of PIPEDA by provinces to co-regulate services. *Context of Case Study* Apply standards to enable compliance with PIPEDA: Our approach to apply standards is to conduct the data governance case study of ed-tech, use this case study to recommend best practices, utilising the standards identified. The research of consented surveillance then focused on the implementation of the strong Meaningful Consent Guidance (Jan 2019) arguably setting the highest online transparency legal baseline in the world. For the most sensitive of data governance use cases. Exploring why there is very little implementation of meaningful consent by school services. The case study research revealed opertionl privacy gaps that are twofold: A) Lack of operational data governance standard for the implementation of Canadian Notice and Consent for online services - e.g. Parental Consent. B) The implementation of PIPEDA by the provinces has extra and intra-territorial tensions and frictions. Meaning a multi-stakeholder, multi-provincial approach is required along side a National and *concerted* provincial effort leading the call to Action. For example, Quebec Bill 64 and the Ontario Privacy Reform Initiative.
Key Words:	ethical use of data, responsible use of data, data lifecycle, data actors, check and balance mechanisms, tracking (data), data decentralization, transparency, accountability, data collection, responsible collection of data, data ethics, digital ethics, data rights, digital rights, data protection, data trust,

	data accountability, governance of data,data responsibility, data strategy, data acquisition, data performance, data conformance, data storage,
Published Standards:	**SC27 ISO/IEC - 29100/29184**
In-Development Standards:	**I**SO/IEC 27560 (draft) from the AdvCIS + Kantara Initiative Consent Receipt Notice and Consent Receipt v1.2
Title of the Gap:	Consensus & Consented; Governed Personal Data Processing Surveillance
Gap Statement:	A key Data Governance Management Standards Gap, focused on in this use case, is *Consented Surveillance*: inferred and observed data, and data control transparency over secondary use. This data governance gap in standards is reflected in digital/online service delivery, in which identity management technology is used to surveill attributes and identifiers that are linked to an Individual, without proportional (Principle 7) individual transparency or control over this processing in context . Illustrating the consented surveillance gap. Security/Liability & Privacy Risks include: - Profiling identifiers, data aggregation from public sources (enhanced profiling, metadata capture from observed data is used for resale and reuse for the benefit of third parties (meta-data profiling), - Third parties provide weak transparency over their legal entity identity, - The beneficial owner of the data processing services and the business / value model to which one's own personal data is being used. - New technologies COVID driven adoption or hacking, enabling access to data formerly thought protected, is allowing greater data leaks or full capture. e.g. psychological profiling for mis-information and cyber attacks - Evidence of harmful use of identifiers who promise but fail to deliver privacy. Create critical cyber security holes. These represent the current landscape and a renewed interest in data trust. Cyber Security Risks include: - Weak transparency over the legal entities in control, and accountable for, identifier surveillance and its purpose of use. eg. the Alphabet/Google ecosystem.

	Inter-Territorial - The collection and capture of metadata is of significant value to Canadians and Canadian society. The intra provincial data disclosure and sharing provides a model for co-data regulation collaboration provides opportunity and . (cyber-security) risks where unregulated and noncompliant data processing occur with non-Canadian services, not subject to same protections or regulation. - Inter-territorial data transfer framed by federal law should be further extended to drive world leading Canadian Standard. - WIth proposed privacy laws being different among provinces, these pose greater cyber-security risks for services and business in Ontario while increasing the privacy risks and the harm to children and youths. - The gap between PIPEDA and current service delivery governance is clear. Rather than a single legal standard being available for eacb service in Canada, a different legal standard for each province, like the US model increases the risks and complexity for all stakeholders. Requiring services to design bespoke policy for each school, province and jurisdiction. *Use Case Research to find out: Why is this happening?* - An audit of these policies and the actual data governance practices demonstrate that both non-Canadian and Canadian service providers do not comply with meaningful consent practices for online services within a Canadian privacy law, specialised to protect Canadian culture and society. - The challenge to the provinces has become increasingly clear as the service economy is attacked with inexpensive/free services that don't abide by the same cultural and legal standards that Canadians expect and need to secure their way of life. *Extra-Territorial* Non-Canadian Countries - e.g. The U.S. supplies most online services. does not provide privacy protections to this data under the Foreign Intelligence Surveillance Act (FISA) - e.g. The lack of legal protections for genetic information in the U.S. is a striking example of its limitations. In Canada, sectoral laws (like those in the U.S.) are used to complement

	comprehensive federal with provincial privacy legislation, providing a layered governance framework for detailed protections over special categories of shared information, such as police files, consumer credit records and school education records. - Genetic metadata is used to identify an entire family not just the person, illustrating a serious security breach for families, who are unaware of the profound and life-shaping risks of harm to others that the metadata creates. - Examples of this territorial friction include: - The EU fine of Google for lack of compliant notice and consent. - The EU Privacy Shield was found to provide inadequate protections and was recently struck down.
Case Study & Active Research for this Use case	Ontario Case Study for Education Data and Records Trust (Case study of current gaps and vulnerabilities in education data governance
Initial Draft Recommendations (dont harm :	First set of recommendations are aimed at protecting vulnerable children & youth; 1. A vulnerable child and youth education-technology policy assessment 2. A transition to ed-tech-4-good of children and youths - using the vulnerable person assessment, with a proposed marketing campaign to promote an impact assessment focused on the school community, parents and provinces. (can children be too young for zoom?) 3. Update provincial ed-tech data trust policy e.g. regional policy /standard for educational data trust that expands provincial control over ed-tech data from school records to include the security and use of children's meta-data, which is a key factor for personal data control and government innovation (a prickly topic).This use case and Ontario case study reveals critical cyber security transparency breaches of children's data by U.S. educational technology used by schools (and most/all sectors of Canadian society). As these services are subject to FISA (Foregin Intelligence Surveillance Act) while meta-data is not protected. - potentially combined with website tracking data by Alphabet/Google for tracking out of school context (ref) Recommendation for Best Practice Development - Two Factor Notice for Meaningful Consent
Priority:Issues for WG to discuss and Address:	- Review assessment of applicable provincial legislation (in draft for review) - Review (and call) for recommendations to address gap - Reviews critical transparency gap(s) to recommended Phase 2 interventions through an Ontario Case study (currently in point form) - Review standards for the implementation of meaningful notice & consent - Phase 2: apply standards for innovation with (federated co-regulation) and strong transparency / cybersecurity
Organization(s):	Smart Species, Mark Lizar - Proposing Organisation, with support from research group, including;

	Dr. Kate Tilleczek Professor & Canada Research Chair *Youth, Education & Global Good.* Kate is also the Director of Young Lives Research Laboratory in the Faculty of Education, York University, who is contributing to reviewed and supports the recommendation we propose presenting.
	https://younglivesresearch.ca
	
	- Next Steps - invite Interest via DGCG Oct 14
	  - inviting the public/private sector to support and participate in Phase 2 implementations of standards.
	  - Inviting the provinces, starting with the Ontario & Federal Government to sponsor the SCC Roadmap and implement security for digital identity.
	  - support the public / private partnership needed to address territorial data governance.