Province of Ontario
Promoting Trust and Confidence in Ontario's Data Economy:
Discussion Paper 1 Response

Submitted by Kris Joseph, MA, MLIS
kris@krisjoseph.ca
September 6, 2019

Introductory Comment

1. I am pleased to participate in the provincial discussion about Ontario's data economy strategy and have responded here to a selection of questions from the first discussion paper. My views are informed by my work as an academic librarian and by my education in the digital humanities. From this foundation, I place strong emphasis on issues of information policy as they apply to intellectual freedom, accessibility, equity and inclusion. The province's willingness to engage with the public about this critical topic is commendable.

2. My commentary on the first discussion paper could have been very broad, but I have chosen to focus on four of the questions presented in *Discussion Paper 1*.

Section 5.1.1.

QUESTION: How can the province ensure that privacy and data protection practices throughout Ontario's public sector…

- ***Put people and users first;***
- ***Enable digital transformation;***
- ***Promote effective, efficient program management; and,***
- ***Protect Ontarians from data-related harms?***

3. In 2018, the United Nations Human Rights Office of the High Commissioner released its Human Rights Based Approach to Data (HRBAD) framework[1] as part of the larger UN Sustainable Development Goals initiative. The province of Ontario's data strategy would benefit greatly from an alignment with the framework's key principles. By way of summary, the approach recommends the use of direct citizen engagement to design, implement, and monitor programs that collect and use data derived from people. Its six areas of focus are:

   i. **Participation**: people and groups who are the subjects of data collection should take part in every step of data-enabled processes from planning and collection through dissemination
   ii. **Data disaggregation**: contrary to some views on data collection, the framework asserts that "averages," derived from aggregated information, are of less value than data whose multiple facets can be used to highlight the effects of programs on marginalized or disadvantaged groups

[1] Office of the High Commissioner for Human Rights, "A Human Rights-Based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development," 2018, https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf.

iii. **Self-identification**: to prevent reinforcement of existing biases and stereotypes, parameters used to define and characterize groups should be defined by the groups themselves
iv. **Transparency**: collected data should not only be available to the public, but the processes used to gather it should be clear and accessible
v. **Privacy**: data that allows direct or indirect identification of individuals should not be made public. Acknowledging that this area must be balanced with transparency, the framework advocates for a consent-based disclosure model, procedures for disposing of data that is no longer required, and clear policies for handling breaches and leaks.
vi. **Accountability**: the state must be accountable to everyone who is affected by its actions. This includes consideration of the impacts of data collection and the ability for stakeholders to use data to hold the state to account.

4. The HRBAD's emphasis on openness, transparency, self-identification and engagement sets a high bar for data governance, but Ontario can be a leader in this area.

5. In a more local context, the UN's recommended approach to data governance reflects the work of the First Nations Information Governance Centre (FNIGC) and its principles for the collection and use of data derived from indigenous communities: the OCAP standard.[2] Though its four components were created to apply to research practices, and though adherence is critical in relation to work with any indigenous people, the framework is also fully compatible with the UN's HRBAD framework and can serve as a model for data collection and governance in other Ontario contexts. The OCAP framework advocates that First Nations people should **Own** information collectively, should be affirmed in their right to **Control** all aspects of research and information collection, that they must have **Access** to this data, and that they must **Possess** it. The framework, like the HRBAD model mentioned previously, emphasizes community engagement and reciprocity.

6. Concepts of ownership are central to the FNIGC model, and the foundation for that context is deeply connected to the ongoing work of reconciliation. From the narrower perspective of privacy, my views differ slightly and have been influenced by previous work of Ontario's Information and Privacy Commissioner. The province's longest-serving privacy commissioner, Ann Cavoukian, wrote a report in 1999[3] that contrasted privacy as an *economic right* (one where "ownership" is paramount) with one where privacy is viewed as a *human right*. I believe the conclusions in Dr. Cavoukian's report were prescient, and that the economic- and property-based model for both data and privacy is now dominant. In its conclusion, the report asserted that market-based data and

[2] FNIGC, "The First Nations Principles of OCAP," accessed September 3, 2019, https://fnigc.ca/ocap.
[3] Ann Cavoukian, "Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation" (Information and Privacy Commissioner, Ontario, September 1999), http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf.

privacy protections are only suitable within the private sector, that protection of fundamental privacy rights is the onus of government, and that we must be mindful that significant asymmetries exist between individuals and organizations. Individuals have far less access to information and bargaining power than the government agencies and corporate bodies from whom they derive services, and this imbalance must be corrected wherever possible. While the report expressed hope that ethical and competitive considerations would force commercial organizations to act responsibly with respect to data governance and privacy, recent events such as the Desjardins data breach,[4] the Equifax data breach,[5] and ongoing privacy abuses at the hands of Facebook[6] and Google/Alphabet[7] have demonstrated that regulators must intervene in a muscular and meaningful way.

7. The challenge inherent to the dominant, ownership-based approach to data and privacy lies in the space where the notion of ownership—an analog for possession of tangible or rival goods[8]—breaks down. For example, many would agree that information directly collected from an individual belongs to that individual, but the question of ownership is less clear when services or applications derive data from observations or patterns of personal behaviour. If Facebook collects and stores information on how people use its service, does that data belong to Facebook or does it belong to the person from whom the data derives? This is a thorny question, but it can be sidestepped by preferring a data governance model that biases the rights of individuals over the ownership of data. The HRBAD framework is a valuable shift in this direction, and the Information and Privacy Commissioner's 1999 report supports the idea that it would serve as a core component of a comprehensive, rights-focused approach to data governance in Ontario.

---

[4] Christopher Reynolds, "Desjardins Group Suffers Massive Data Breach of 2.9 Million Members by Rogue Employee," The Globe and Mail, June 20, 2019, https://www.theglobeandmail.com/business/article-desjardins-group-suffers-massive-data-breach-of-29-million-members-by/.

[5] CBC News, "Equifax Says 100,000 Canadians Impacted by Cybersecurity Breach," September 19, 2017, https://www.cbc.ca/news/business/equifax-canada-cyberbreach-1.4296475.

[6] Todd Spangler, "FTC Approves $5 Billion Fine Against Facebook for Privacy Violations – Variety," Variety, July 12, 2019, https://variety.com/2019/digital/news/ftc-5-billion-fine-facebook-privacy-violations-1203266388/#!; Alyssa Newcomb, "A Timeline of Facebook's Privacy Issues — and Its Responses," NBC News, March 24, 2018, https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651.

[7] Jon Porter, "Google Accused of GDPR Privacy Violations by Seven Countries," The Verge, November 27, 2018, https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive; Natasha Singer and Kate Conger, "Google Is Fined $170 Million for Violating Children's Privacy on YouTube," *The New York Times*, September 4, 2019, sec. Technology, https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html; CBC News, "'Not Good Enough': Toronto Privacy Expert Resigns from Sidewalk Labs over Data Concerns," CBC, October 21, 2018, https://www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223; Jared Lindzon, "How Toronto Locals Soured on Alphabet's Neighborhood of the Future," Fast Company, September 6, 2019, https://www.fastcompany.com/90390377/alphabet-wants-to-turn-toronto-into-a-digital-city-locals-arent-so-sure.

[8] Samuel E. Trosow, "The Commodification of Information and the Public Good.," *Progressive Librarian*, no. 43 (2014): 17–29.

QUESTION: How can Ontario promote privacy protective practices throughout the private sector, building on the principles underlying the federal government's private sector privacy legislation (the Personal Information Protection and Electronic Documents Act)?

8. Federal *PIPEDA* legislation applies to commercial activity, and the *Privacy Act* covers governmental organizations. Though most provinces have enacted legislation to cover health-related data and privacy practices, only three provinces have created other legislation that mirrors or supplements the federal acts.[9] Sadly, the federal acts have gaps: for example, they do not apply the work of non-profits or charities (including political parties), and *PIPEDA* imposes penalties for failing to report data breaches but includes no penalties for the breaches themselves.[10]

9. An Ontario approach to *PIPEDA*'s principles should take non-commercial activity into account and should incentivize the creation and maintenance of systems to *prevent* data breaches, rather than relying on penalties for failure to notify affected individuals. It should also vigorously defend an individual's use of Privacy-Enhancing Technologies (PETs) and ensure that a decision to opt out of non-essential data collection (required in order to provide the primary service on offer) does not restrict access to information, goods, or services.

Section 5.2.1.

QUESTION: How can the province help businesses – particularly small and medium-sized businesses – better protect their consumers' data and use data-driven practices responsibly?

10. A provincial investment into a public utility for self-sovereign identity would be forward-thinking. Systems of this type emphasize privacy-centred control and access to personal information, wrapped in an open and transparent framework.

11. An open-source project like Sovrin[11] offers a forward-thinking and nuanced approach to identity, credential, and privacy management that is designed for the increasingly complex, networked information landscape. The architecture, which is built on advanced cryptographic "zero knowledge" techniques, allows individuals or organizations to assert that something is true without revealing any of the underlying information. This model is easily demonstrated with a common use case: to prove that someone is over the age of 18, the current paradigm involves sharing photo-

[9] Office of the Privacy Commissioner of Canada, "Summary of Privacy Laws in Canada," May 15, 2014, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.
[10] Office of the Privacy Commissioner of Canada, "What You Need to Know about Mandatory Reporting of Breaches of Security Safeguards," October 29, 2018, https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.
[11] Sovrin Foundation, "Sovrin," Sovrin, 2019, https://sovrin.org/.

identification or other documentation that reveals multiple personal characteristics. The self-sovereign identity method allows the system to assert that an individual is at least 18 years of age (and therefore able to access an age-restricted service) without disclosing a birthdate, address, license number, photograph, or any other personally identifiable information. Systems like this remove the need for third parties to collect and store identifying information, resulting in two critical advantages:

i. Preserving the privacy rights of individuals, and
ii. Eliminating the risk of data breaches and penalties for organizations that use data derived from individuals, since they need not store any of it to begin with

12. Ontario does not have to reinvent the wheel to benefit from these novel technologies. The province could leverage existing work and influence ongoing efforts by joining the Sovrin Alliance.[12]

QUESTION: How might the province help ensure that consumers are more meaningfully informed and protected when agreeing to internet-based contracts (including terms of service and privacy policies) involving transactions of their data?

13. Recent analyses of privacy and terms of use policies has shown that informed consent is nearly impossible to obtain from consumers, since nobody reads these policies[13] and since the amount of time required to fully-digest them verges on absurdity.[14] Sadly, the intent to add transparency to online services has increased to volume of "required reading" so much that it has become habitually ignored by almost all of us.

14. The problem seems intractable, but one suggested approach warrants further exploration: a system of standardized visual labels or simplified informational fields, similar to a nutrition label, that can provide at-a-glance information for individuals curious about the policy to which they are agreeing. Kelley et. al. proposed a design methodology for such as system in 2009[15] and studied the effectiveness of such a

[12] https://sovrin.org/join-the-sovrin-alliance/
[13] David Kravets, "TOS Agreements Require Giving up First Born—and Users Gladly Consent," Ars Technica, July 7, 2016, https://arstechnica.com/tech-policy/2016/07/nobody-reads-tos-agreements-even-ones-that-demand-first-born-as-payment/.
[14] Guido Noto La Diega and Ian Walden, "Contracting for the 'Internet of Things': Looking into the Nest," Queen Mary School of Law Legal Studies Research Paper, February 1, 2016, https://ssrn.com/abstract=2725913; Alexis C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," The Atlantic, March 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.
[15] Patrick Gage Kelley et al., "A 'Nutrition Label' for Privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09* (the 5th Symposium, Mountain View, California: ACM Press, 2009), https://doi.org/10.1145/1572532.1572538.

system in 2010.[16] Their work concluded that a combination of a standardized "short text" policy format and a visual system, presented in a graphical table format, provided an understandable and even enjoyable experience for users. Ontario could mandate such an approach for organizations that work in the province, following the model of the *Healthy Menu Choices Act, 2015*.[17]

Respectfully submitted,

Kris Joseph, MA, MLIS
kris@krisjoseph.ca
September 6, 2019

[16] Patrick Gage Kelley et al., "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach," in *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10* (the 28th international conference, Atlanta, Georgia, USA: ACM Press, 2010), 1573, https://doi.org/10.1145/1753326.1753561.
[17] *Healthy Menu Choices Act*, *Statutes of Ontario* 2015, c.7, Sched. 1. https://www.ontario.ca/laws/statute/15h07