Information and Privacy Commissioner of Ontario

Office of the Privacy Commissioner of Canada

Commission d'accès à l'information du Québec

Office of the Information and Privacy Commissioner for Nova Scotia

Manitoba Ombudsman

Office of the Information and Privacy Commissioner for British Columbia

Office of the Information and Privacy Commissioner of Prince Edward Island

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner of Newfoundland and Labrador

Office of the Information and Privacy Commissioner of the Northwest Territories

Yukon Information and Privacy Commissioner

Office of the Information and Privacy Commissioner of Nunavut

Office of the Saskatchewan Information and Privacy Commissioner

April 24, 2018

The Honourable Amarjeet Sohi
Minister of Infrastructure and Communities
180 Kent Street, Suite 1100
Ottawa, ON K1P 0B6

Sent by email

Subject: Smart Cities Challenge

Dear Minister:

As federal, provincial, and territorial privacy protection authorities, we are writing to urge you to proactively take steps to ensure that privacy and security of personal information are specifically considered in the selection, design, and implementation of the winning proposals in Infrastructure Canada's Smart Cities Challenge, recently launched under the Government of Canada's Impact Canada Initiative.

We understand that the department has invited communities across Canada, including municipalities, local or regional governments as well as indigenous communities, to develop proposals for "innovative solutions to their most pressing challenges using data and connected technologies." Winning communities will be awarded with prize money to help implement their proposals.

We appreciate the potential value of innovative smart city initiatives, such as allowing communities to more effectively address the challenges of urbanization and allocate resources accordingly. We do however urge you to ensure that this initiative, in supporting and encouraging innovation, requires project proposals to directly build in privacy protections. This is especially the case given that finalists from most jurisdictions will be subject to applicable access and privacy laws. In those jurisdictions yet to include municipalities under their access and privacy legislation, the insistence on these protections is even more vital.

Privacy Risks

The data that smart technologies collect and use can come from many sources, such as sensors that interact with people or with their personal devices as they go about their daily lives – often without any positive action required on the part of the individual, or even opportunity to opt out.

These systems can be used to generate large amounts of data which may include highly sensitive personal information. This data can enable privacy-invasive activities, such as surveillance or profiling, and may entice communities and private sector partners to use the personal information for different purposes without consent, contrary to Canadian privacy laws, and without public input. Such risks can compromise public trust, a key element for the success of any smart city initiative.

In addition, without appropriate measures to secure personal information collected by these systems, individuals' personal information may be exposed to cybersecurity risks. Effective safeguards are especially complex to implement in the smart cities context given the diverse forms of technology deployed. As a general rule, the more points of data collection, processing, and access, the greater the risks of a security failure.

The media have reported on smart cities projects that have failed, in part because of their impact on privacy rights or because the public trust in the systems was lacking. We should learn from the lessons of other cities when emulating their practices and designing new initiatives.

Mitigating controls

To ensure that privacy and security are protected in any smart city initiative, communities will need to build into the systems a number of important privacy and security measures, such as:

- Data-minimization – systems must not collect, use or disclose personal information unless it is necessary to do so to achieve the outcomes of the initiative. In all cases, where the goals can be achieved using less privacy invasive alternatives, those alternatives should be pursued.
- De-identification – systems must endeavor to de-identify personal information at the earliest opportunity and include measures to mitigate the high risk of re-identification that is inherent with connected devices. As well, systems should only retain, use and disclose de-identified information.
- Data governance and Privacy Management program – initiatives must be supported by policies that address privacy and security requirements including appointing a privacy lead, monitoring and auditing for compliance, and breach response. There must also be contractual protections and accountability for all of the diverse parties involved in the initiative. This is especially important given that the department is encouraging communities to develop proposals in conjunction with other partners.
- Privacy impact assessments and threat risk assessments – these are widely recognized as important tools to help ensure that privacy and security risks are identified and adequately addressed in the design of new technologies and programs. In some jurisdictions, they are required.
- Community engagement and project transparency - communities must ensure full transparency of the information practices of their initiatives to help community members understand how they might be affected. Transparency is reflected in Canadian provincial and federal access and privacy laws.
- Consent – systems must ensure individuals' meaningful consent where required by law, including the opportunity to opt out of participation, where feasible.

…/2

Conclusion

We are calling on you to help ensure that government resources are not expended on initiatives that either infringe on the fundamental right to privacy or risk failing because the public's confidence in the systems is lacking. We strongly encourage you to require that the finalists commit to the preparation of privacy impact and threat risk assessments at the design stage and also commit to applying any resulting recommendations at the implementation stage. Innovation and privacy can be simultaneously promoted.

We note that the evaluation criteria for final proposals will be announced in the summer. We strongly recommend that the final criteria include a consideration of the privacy implications of the proposals advanced by the finalists. Our offices would be pleased to proactively engage with your department, by supporting the development of such criteria, and at a later point, an evaluation of the projects scoring on these criteria. We invite you to contact Renee Barrette, Director of Policy with the Information and Privacy Commissioner of Ontario at Renee.Barrette@ipc.on.ca, to discuss how we can collectively be of assistance in this regard.

This is an important issue to our offices and we plan to post this letter on our websites on Thursday in order to raise awareness of the access and privacy implications of smart city initiatives.

Sincerely,

Original signed by

Brian Beamish
Information and Privacy Commissioner of Ontario

Original signed by

Daniel Therrien
Privacy Commissioner of Canada

Original signed by

M^{e} Jean Chartier
Chair of the Commission d'accès à l'information du Québec

Original signed by

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Original signed by

Charlene Paquin
Manitoba Ombudsman

Original signed by

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Original signed by

Karen A. Rose
Information and Privacy Commissioner of Prince Edward Island

Original signed by

Jill Clayton
Information and Privacy Commissioner of Alberta

Original signed by

Donovan Molloy, QC
Information and Privacy Commissioner of Newfoundland and Labrador

Original signed by

Elaine Keenan-Bengts
Information and Privacy Commissioner of the Northwest Territories

Original signed by

Elaine Keenan-Bengts
Information and Privacy Commissioner of Nunavut

Original signed by

Diane McLeod-McKay
Yukon Information and Privacy Commissioner

Original signed by

Ronald J. Kruzeniski, QC
Saskatchewan Information and Privacy Commissioner