Information and Privacy Commissioner of Ontario

Submission to the Standing Committee on the Legislative Assembly

e-Petitions

Brian Beamish
Commissioner
October 21, 2015

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

INTRODUCTION

The Office of the Information and Privacy Commissioner of Ontario (IPC) is responsible for ensuring compliance with the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), which applies to the provincial public sector, and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), which applies to the municipal public sector. In accordance with these statutes, the IPC acts independently of government to uphold and promote open government and the protection of personal privacy.

While this submission deals specifically with the privacy implications of e-petitions and the protection of individuals' personal information, I would like to begin with a few words on the role and importance of e-petitions from the perspective of the IPC's other mandate—the promotion of open and transparent government.

SUPPORTING OPEN AND ACCESSIBLE GOVERNMENT

Benefits of e-Petitions

Public petitions are one of the most direct means by which a group of individuals can communicate with their government and participate in the development of public policy. By enabling individuals to give voice to their grievances and concerns and bring these to the attention of the government, public petitions foster an engaged citizenry and a responsive government.

Paper petitions have a long-standing tradition in the Legislative Assembly of Ontario and should continue to play a role in the Legislative Assembly's petition procedures. However, it is clear that this medium is no longer the preferred means of communication for increasingly large numbers of Ontarians and has been superseded by other, predominantly online forms of communication. If e-petitions were integrated into the Legislative Assembly's existing petition procedures, Ontarians would stand to benefit in important ways. Not only would their preference for online forms of communication be better supported but, consistent with the findings and recommendations in the "Open by Default" report prepared by the Open Government Engagement Team,[1] barriers in the existing paper-based process would be removed, potentially leading to more opportunities for public engagement, increased numbers of participants, greater geographic diversity and a more engaged youth. E-petitions also support more open and responsive governments by increasing opportunities for groups of individuals to receive feedback on issues that are important to them.

The IPC is a strong supporter of open government. We believe that e-petitions, if implemented properly, have the potential to improve the quality and level of engagement by Ontarians, resulting in increased government transparency and accountability. They will also support Ontarians'

1 See **http://www.ontario.ca/document/open-default-new-way-forward-ontario**

desire for more convenient access to government services. Further, unlike the current paper process, the public will have far greater accessibility to petitions that have been filed and the corresponding government response.

Designing an e-Petition Process

Given the potential increase in public engagement, an important consideration in designing an e-petition program is the number of signatures required for certain actions to be taken. The Legislative Assembly should consider establishing a minimum threshold for the number of signatories that must be reached before an e-petition is made publicly available on the e-petition website. Consideration should also be given to establishing an appropriate second, higher threshold that would trigger the requirement for further MPP support or a response from the government, taking into account the diversity of the various regions of Ontario in terms of their size and population.

In addition, a governance framework similar to that which is available for the current process should be put in place articulating the methodology and criteria for filing an online petition. The criteria should set out the required content of the petition's request, as well as rules about terminology or requests that would violate the framework, such as abusive or offensive language and frivolous or vexatious proposals, and the rules regarding sponsorship by a member, responses from the government and tabling in the House.

The Legislative Assembly should consider establishing a screening process consistent with those in jurisdictions such as Quebec, Northwest Territories, Australia and the United Kingdom (UK) where petitions are reviewed before they are published online. For example, in the Northwest Territories, petitions must be approved by the Office of the Clerk before they are posted. Similarly, in the UK, the Petitions Committee of the House of Commons reviews all petitions that have received five signatures before they are published to ensure relevant standards have been followed.

In contrast, petitions posted on the United States' e-petition platform do not appear to be screened; rather, they are reviewed periodically for compliance with the Terms of Participation after they are posted. Petitions may also be flagged for removal by other users of the website who believe that a particular petition violates the terms of use.

Another important consideration given the online aspect of e-petitions is ensuring the legitimacy of the process for signing e-petitions and protecting them from abuse. Online petitions may be vulnerable to individuals who design automated programs to replicate the steps of the online signing process and forge large numbers of signatures. Different tools and techniques may be used to protect against such attacks. For example, one tool used to detect and prevent automated programs from interacting with online resources is CAPTCHA,[2] which uses a kind of

2 CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."

challenge-and-response test to determine whether the user is a human or not. Another technique involves collecting and analyzing information about the agent or web browser used in the signing process—for example, the IP address—and analyzing that information for suspicious activity such as when a large number of signatures originate from the same source in a short amount of time.

A final design consideration that I will mention is the length of petitions. Placing limits on the character or word count of petitions may act as a deterrent to frivolous or vexatious proposals. This may also improve the quality of legitimate proposals by forcing the creators of the petition to focus on the core issues. At the same time, the maximum length of petitions should not be so small so as to prevent an informed presentation of the issues.

PROTECTION OF PERSONAL PRIVACY

While it is true that e-petitions offer many benefits, it is equally true that they raise concerns regarding the collection, use and disclosure of individuals' personal information. I will now turn to a discussion of the privacy issues they raise with respect to the protection of personal privacy.

Expectation of Privacy

The privacy protections set out in *FIPPA* and *MFIPPA* do not apply to the Legislative Assembly, its members or political parties. Nevertheless, individuals have a reasonable expectation of privacy which has been recognized by the Supreme Court of Canada as a fundamental right under the *Canadian Charter of Rights and Freedoms*. Moreover, in Ontario, violations of privacy may form the basis of a common law right of action. While the Legislative Assembly and political parties fall outside the scope of *FIPPA* and *MFIPPA*, privacy is a fundamental value of Ontarians and forms the basis of their expectation that government agencies and elected officials will handle their personal information with care and respect.

By way of example, in September 2012, thousands of individuals received an unsolicited bulk email from the office of the federal Minister of Citizenship and Immigration titled "LGBT (lesbian, gay, bisexual and transgender) Refugees in Iran." It is alleged that the email addresses used by the office belonged to individuals who signed an online petition in support of a gay artist who was facing deportation. While the email contained a positive message about Canada's efforts to protect the rights of gay and lesbian refugees, it received a negative response from many individuals and groups. Some individuals felt "targeted," "disturbed" and "frightened" by the fact that the government was "stockpiling lists of particular constituencies of Canadians." Signatories objected to the use of their email addresses for a different, arguably political, purpose.

A complaint was subsequently filed with the federal Privacy Commissioner, although it did not go forward due to the inapplicability of privacy laws to political parties.[3]

Sensitive, Attractive Digital Information

The above example illustrates the type of personal information that may be at issue with respect to e-petitions. It is not only contact information that can be used to verify the residency, authenticity and non-duplication of individuals who signed the petition, such as name, email address, location and postal code. It may also include the issues, causes or beliefs with which the individual identifies and which can be used to infer additional, sensitive information about the individual, including his/her political views, sexual orientation or religion.

The example also illustrates how attractive this information can be to political parties, special interest groups or even commercial enterprises. The potential sensitivity of subject matters and the social-political nature of e-petitions make the individuals who create or sign them particularly susceptible to voter and consumer profiling. Once profiled, these individuals may be identified and targeted for unsolicited political messaging or other unrelated secondary uses of their personal information. In addition, although the potential for increased participation from a greater and more diverse cross section of the public is likely to improve the quality and quantity of petitions, this same characteristic of e-petitions would allow larger portions of the population to be profiled.

A third and final point to draw from the above example is the relative ease and speed with which an e-petition with a large number of signatures can be transferred, transformed and repurposed into a usable database. This is due primarily to the digital nature of the information that lends itself to automated processing. While paper petitions contain the same sensitive information as e-petitions, the physicality of the medium acts as an important safeguard, reducing the availability, replicability and transformability of the information. This kind of practical obscurity is not present in the digital medium of e-petitions.

Necessary Privacy and Security Controls

Because of the sensitivity, attractiveness and digital nature of the personal information contained in e-petitions, it is important that any integration of e-petitions into the Legislative Assembly's existing petition procedures have in place the necessary controls to protect the privacy of the individuals involved in the process.

3 See "Minister's email to gay community sparks privacy complaints," *CBC News*, September 22, 2012, **http://www.cbc.ca/news/politics/minister-s-email-to-gay-community-sparks-privacy-complaints-1.1207146**; Glen McGregor, "Jason Kenney's office mined web petition to target message to gay Canadians," *National Post*, September 24, 2012, **http://news.nationalpost.com/news/canada/jason-kenneys-office-mined-web-petition-to-target-message-to-gay-canadians**.

What personal information should be collected?

The collection of personal information should be limited to that which is necessary to fulfil the purposes of the program. This concept of "data minimization" is a basic tenet of privacy protection. An e-petition program requires the collection of personal information only for the purposes of verifying the residency, authenticity and non-duplication of individuals, and for contacting individuals, with their consent, with updates to the e-petitions with which they are associated. Accordingly, the collection of personal information involved in the Legislative Assembly's e-petition program should be limited to that which is necessary to fulfil those purposes.

At the same time, the amount and type of personal information collected for the purposes of verifying the residency, authenticity and non-duplication of individuals should be proportionate to the purpose of the e-petition program, which is to promote engagement and encourage or solicit a non-binding government response to the request. While some jurisdictions require signatories to provide their first and last name, city, province, country, postal code and email address, others, such as the United States, require signatories to provide only their first and last name and email address, with the individual's ZIP code being optional. Based on our review of current practices and given the non-binding nature of the government's response, the collection of first and last name, email address and postal code should suffice for verification purposes. As noted above, however, techniques used to protect the process for signing e-petitions from abuse by hackers may require additional information.

Who should have access to the personal information collected?

The personal information collected should not be used or disclosed for purposes other than those of implementing an effective and transparent e-petition program. Access to the personal information of individuals who sign e-petitions should be limited to administrative and IT staff at the Legislative Assembly who are responsible for administering the program. Accordingly, access to, or use of, signatories' personal information by other staff, MPPs or third parties, including political parties, special interest groups and commercial enterprises, should be strictly prohibited.

What personal information should appear on the website?

The amount and type of information concerning individual e-petitions that is published online should also be limited. With respect to signatories of e-petitions, I see no reason for any of their personal information to appear online. On the other hand, with respect to creators of e-petitions, consideration could be given to publishing their names online alongside the e-petition they created. Because the creator is inviting other members of the public to support a cause or issue he or she is promoting, it is reasonable to assume that the public would have an interest, if not a right, in knowing the identity of the creator.

What security safeguards should be in place?

Reasonable measures to protect the personal information involved against loss or theft as well as unauthorized access, disclosure, copying, use or modification should be put in place, taking into account the nature of the personal information involved. The Legislative Assembly's e-petition program should include measures, such as:

- strongly encrypting personal information at rest and in transit,
- establishing controls to limit all access to personal information on a need-to-know basis and
- keeping auditable logs of all accesses, uses and disclosures of personal information.

For how long should personal information be retained?

In general, the personal information involved should be retained for only as long as is necessary to fulfil the purposes of the e-petition program. With respect to signatories of e-petitions, while there may be archival reasons for retaining their personal information for e-petitions that meet the threshold for a government response, the most privacy-protective approach to retention would involve securely destroying the personal information of signatories once the information is no longer required for the purposes of verifying their signature and providing a response to the e-petition.

With respect to creators of e-petitions, as noted above, there may be valid reasons for publishing their names online alongside the e-petition they created. The Legislative Assembly's approach to retention with respect to the personal information of creators of e-petitions would be informed by those same reasons. In other words, if the publishing of creators' names online is deemed valid, then so would the retention of that personal information.

Accountability

As the organization that determines the manner in which individuals' personal information will be collected, used, disclosed, published, secured and retained for the purposes of an e-petition program, the Legislative Assembly is accountable for developing policies and procedures that support and give effect to its data handling practices.

Privacy Policy

The Legislative Assembly should develop and implement a comprehensive privacy policy to assist in achieving and maintaining compliance with its management and handling of personal information, as well as to provide individuals with specific information about those practices. This privacy policy should be easy to locate on the Legislative Assembly's website and made

available to individuals who participate in the Legislative Assembly's e-petition program. It should include information about the issues raised in the previous section, such as:

- the rationale, objectives and justification for implementing an e-petition program,
- a description of the nature of the personal information collected,
- limitations placed on access to and use of personal information by employees, including the individuals that can view the information and under what circumstances it may be viewed,
- a description of what information will be published online,
- the administrative, technical and physical safeguards implemented to protect personal information from loss or theft as well as unauthorized access, disclosure, copying, use or modification,
- the retention periods of personal information and
- the title, business address and business telephone number of a senior staff member who is responsible for the Legislative Assembly's privacy obligations and who is available to answer individuals' questions about the e-petition program.

Training

It is important that the administrative and IT staff at the Legislative Assembly who are responsible for administering the e-petition program undergo appropriate training to educate them on their roles, duties and responsibilities. Specifically, employees should attend an initial privacy orientation as well as regular training. These training programs should contain detailed information about the policies and procedures that have been implemented by the Legislative Assembly, including the following:

- The duties and responsibilities of employees in implementing the administrative, technical and physical safeguards put in place. This includes the signing of a written agreement to adhere to these duties, including an undertaking of confidentiality, and to undergo initial and ongoing privacy training;
- An explanation of the process for responding to privacy breaches and the duties and responsibilities imposed on employees in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches;
- The potential consequences to employees if they breach policies or procedures.

Privacy Impact Assessment

A privacy impact assessment (PIA) is a risk management tool that helps to identify the effects of a given program or other activity on an individual's privacy, and the safeguards or strategies that may be employed to eliminate the adverse outcomes of those effects or reduce them to an acceptable level. These safeguards and strategies can then be incorporated into the institution's program, policies and procedures. PIAs also serve to identify risks to organizations and have become an accepted and necessary tool throughout government and the private sector for addressing privacy issues. I note that the Ministry of Government and Consumer Services has developed an excellent PIA document and expertise in this area.

Many of the issues raised in the previous section will be addressed in the course of conducting a PIA. Accordingly, it is important that the Legislative Assembly conduct a PIA prior to any integration of e-petitions into its existing petition procedures and whenever significant changes are made to those procedures. My office would be pleased to act as a resource during this process.

CONCLUSION

The IPC believes that e-petitions have the potential to improve the quality and level of engagement by Ontarians, resulting in increased government transparency and accountability. They will also increase citizen access, make the petition process more convenient and allow citizens to interact with their government in a manner they have come to expect. However, due to the sensitivity, attractiveness and digital nature of the personal information contained in e-petitions, any integration of e-petitions into the Legislative Assembly's existing petition procedures should have in place the necessary controls to protect the privacy of individuals. In addition, the Legislative Assembly should develop organizational practices and procedures to remain accountable for its management and handling of personal information and to assist in achieving and maintaining compliance.

I thank you for the opportunity to provide the Standing Committee on the Legislative Assembly with advice on the privacy implications of e-petitions. The IPC is available for further consultation to discuss any questions or concerns the Legislative Assembly may have about this submission. Please feel free to contact us should you require further information or assistance.

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca