Information and Privacy Commissioner of Ontario

Submission to the Ministry of Community Safety and Correctional Services on its Strategy for a Safer Ontario

Brian Beamish
Commissioner
April 29, 2016

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 pleased to participate in the Ministry of Community Safety and Correctional Services' (Ministry) public consultation on its Strategy for a Safer Ontario (the Strategy) which will include a review of the *Police Services Act* (*PSA*). We understand the consultation will support the provincial government's goal of ensuring effective, sustainable and community-based policing. We commend the Ministry for openly engaging with the public and other stakeholders on this important initiative.

To facilitate the process, the Ministry has published a discussion paper entitled *Strategy for a Safer Ontario: Public Discussion Paper* (Discussion Paper). In this submission, we address:

- collaborative community safety and well-being initiatives
- the expanded use of technology
- transparency and accountability
- the need to ensure ongoing stakeholder engagement

Modern day policing invariably involves the collection, use, retention and disclosure of personal information, for which police services are accountable. The Ministry and police services are subject to Ontario's access and privacy legislation (the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) or the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)). The IPC is responsible for overseeing this legislation, as well as the *Personal Health Information Protection Act, 2004* (*PHIPA*), and has statutory responsibility and expertise with respect to police matters that impact access and privacy rights of Ontarians.

As the Ministry notes, public safety objectives must be addressed in a manner that respects the fundamental human rights valued by society. These rights are codified in the *Canadian Charter of Rights and Freedoms* and the Ontario *Human Rights Code*, and include protecting individual privacy. In our experience, public safety can be enhanced while respecting human rights, including those protected under privacy legislation.

We recognize the challenges faced by police, including those associated with meeting the diverse needs of Ontarians. We agree that the key themes of public confidence, trust and relationships built on respect must be woven through all elements of the Strategy. Privacy and transparency are critical to building this trust, and we are committed to helping the Ministry ensure that its programs and initiatives reflect these core values.

COLLABORATIVE COMMUNITY SAFETY AND WELL-BEING INITIATIVES

The cornerstone of the Ministry's Strategy will be "community safety and well-being" and the improvement of "collaborative partnerships between the police, the public and other sectors."

The IPC is engaged with the Ministry and other stakeholders on one such collaborative approach, "situation tables." A situation table typically involves regular meetings among staff from agencies such as police, municipalities, hospitals, social services, and schools. Meetings are convened to identify and address individual cases that raise concerns about community safety or well-being that one agency cannot address alone. At these meetings, personal information and personal health information (personal information) may be collected, used and disclosed by a wide array of situation table partners for harm reduction purposes, often without the individual's consent.

While we acknowledge that good intentions motivate these collaborative partnerships, we also know that such an approach can present several risks to privacy. These risks include the excessive and unnecessary collection, use, retention and disclosure of personal information, which would contravene a fundamental principle at the heart of privacy legislation—the data minimization principle. Properly applied, data minimization supports compliance with privacy legislation.

The IPC is working with the Ministry and other stakeholders to develop guidelines for sharing personal information at situation tables in a privacy compliant manner. For example, we have focused on the need to use de-identified information to the greatest extent possible. Our goal is to support situation table participants in addressing community safety and well-being, while meeting their obligations under privacy legislation, including *PHIPA*.

Consistent with the advice we recently provided, the Ministry should take steps to ensure that all collaborative initiatives that involve the sharing of personal information are guided by clearly defined governance frameworks that comply with *FIPPA*, *MFIPPA* and *PHIPA*. In addition, any legislative reforms to support these collaborative initiatives should be based on data minimization. Harm reduction programs and initiatives must respect this principle if they are to ensure that privacy and other fundamental human rights are properly respected.

Recommendations:

1. Collaborative community safety and well-being initiatives should be supported by clearly defined governance frameworks that meet transparency and privacy best practices, as well as the requirements in *FIPPA*, *MFIPPA* and *PHIPA*.
2. The government should ensure that any legislative reforms governing collaborative community safety and well-being initiatives respect the data minimization principle.

THE EXPANDED USE OF TECHNOLOGY

The IPC supports police use of technologies to enhance community safety, provided they are implemented in a manner that respects privacy and access. Recent examples of technologies that have attracted public interest include body-worn cameras, automated licence plate recognition (ALPR) systems, and stingrays. While these technologies may be useful to police services, they can also pose significant risks to the rights of individuals.

Body-worn cameras collect a large amount of personal information about members of the public, including both images and sound. ALPR systems can be configured to routinely collect personal information associated with the owners and drivers of motor vehicles. Stingrays are devices used for intercepting cell phone traffic and tracking the movement of cell phone users. They have the potential to collect a large amount of personal information about individual users, including who they communicate with and what they communicate about. These technologies may also generate metadata, such as the date, time, location and duration of the recorded activities.

Once personal information is collected, whether by a body-worn camera, an ALPR system, or a stingray, it may be retained in a police database. With the retention of personal information comes additional risks to the security of the information such as the potential for unauthorized access or inappropriate use.

Absent adequate safeguards, all three of these technologies have the potential to facilitate surveillance and profiling of law-abiding individuals going about their everyday activities. They may also reveal other sensitive information about individuals, such as information about their travel to and participation in lawful but sensitive activities (e.g. attendance at a doctor's office or a political protest).

A police service's use of technologies must be guided by policies, procedures, and related training programs. Together, these measures provide a governance framework that can help police meet privacy and transparency best practices, and comply with privacy and access legislation.

To ensure a consistent approach across the province, the government should enact province-wide standards governing the use of surveillance technologies in consultation with police, privacy and access, human rights, civil liberties, and criminal law experts. This approach, followed in relation to police record checks, will ensure that privacy, access and other fundamental rights will be accorded equal treatment in communities across Ontario.

Recommendation:

3. The government should enact province-wide standards governing the use of surveillance technologies.

TRANSPARENCY AND ACCOUNTABILITY

The Discussion Paper raises questions about transparency and accountability with respect to the use of surveillance technologies, the outcome of police conduct-related decisions (including those associated with Special Investigations Unit (SIU) investigations), and the manner in which police conduct themselves when dealing with members of the public.

By enacting province-wide standards on the use of surveillance technologies, the government will ensure that these technologies are implemented in a transparent and accountable way. As evidenced by recent controversies associated with police decisions to refuse to confirm or deny whether they have acquired stingray technology, there is substantial public interest in knowing whether police are using a surveillance technology, the privacy implications of its use, and the safeguards in place. The public has the right to know about the functionality of surveillance devices, like stingrays, and the range of information captured by their use.

The public also continues to show a significant interest in greater transparency and accountability with respect to how individual police officers conduct themselves, including with respect to incidents that require the involvement of the SIU. Greater transparency with respect to *PSA* hearing decisions, police chiefs' SIU-related investigation reports, and the SIU's investigation reports would assist the SIU, police services and police services boards in fulfilling their duties to provide transparent and accountable policing. Such transparency would also help to foster public confidence in policing in general, as well as in police discipline and oversight in particular.

The *PSA* requires that hearing decisions arising from *public* complaints about officer misconduct and unsatisfactory work performance be made public. This responsibility falls on police chiefs, police services boards and the Office of the Independent Police Review Director (OIPRD). The OIPRD is required to publish these decisions online. However, the *PSA* does not impose comparable duties with respect to hearing decisions arising from a *police chief's* complaint about misconduct and unsatisfactory work performance.

There is a strong public interest in requiring that, as a general rule, all hearing decisions about police misconduct and work performance be published. Such a requirement would be consistent with the fact that, subject to limited statutory exceptions, all Part V *PSA* hearings must be open to the public, including those arising from disciplinary proceedings initiated by a police chief's complaint. Accordingly, the IPC recommends that, subject to limited statutory exceptions, all *PSA* hearing decisions be made readily available to the public.

In addition, we recommend that a similar approach be applied to police chiefs' investigation reports regarding incidents subject to criminal investigation by the SIU. The SIU investigates "the circumstances of serious injuries and deaths that may have resulted from criminal offences committed by police officers." The *PSA* regulations require a police chief to conduct a parallel

investigation with respect to related policy and conduct issues. The *PSA* regulations allow, but do not require, a police services board to make a police chief's SIU-related investigation report available to the public. Few such reports are released.

We urge the government to amend the *PSA* to require greater transparency with respect to the SIU's investigation reports. While the public may be able to obtain access to some of the information in an SIU report, for example, through an SIU press release or an SIU access to information decision, the current legal and policy framework does not facilitate sufficient transparency.

As explained in the 2003 "Review Report on the SIU Reforms prepared for the Attorney General of Ontario by the Honourable Justice Adams, Q.C.," greater transparency with respect to these reports is "central to providing necessary accountability and community confidence." At that time, police services told Justice Adams that making SIU reports public when no charges are laid can also help to "clear the air in respect of their involvement" in incidents involving serious injury or death of a member of the public.

That reasoning is consistent with current thinking with respect to open and accountable government. To their credit, the Premier and the Attorney General have also signaled their agreement that greater transparency is required. Accordingly, we recommend that the SIU investigation reports be made public. We acknowledge that such reports may contain some information that is properly subject to redaction, for example, the name of a civilian witness. However, the right to make redactions should be limited under the *PSA*.

In support of the government's goal of enhancing oversight and accountability, we understand that the Ontario Human Rights Commission (OHRC) is recommending that the Government of Ontario:

- require police services to establish data collection and permanent retention systems to record human rights based-data on all stops of civilians, use of force incidents, and interactions where officers ask about immigration status or conduct immigration status checks, and

- ensure that the data be "standardized, disaggregated, tabulated and publicly-reported by each police service."

We support these recommendations. The information in any such data collection and retention systems should be de-identified as soon as the personal information is no longer required for an authorized purpose. In addition, it is critical that any public report not include personally identifiable information. We would be pleased to work with the Ministry, the OHRC, and other stakeholders on the development of necessary standards and procedures.

Recommendations:

4. The government should enact rules to ensure transparency and accountability with respect to the use of surveillance technologies.

5. The government should amend the *PSA* and its regulations to require that, subject to limited statutory exceptions, all *PSA* hearing decisions, police chiefs' SIU-related disciplinary investigation reports, and SIU investigation reports be made available to the public.

6. In requiring police services to establish data collection and retention systems to record human rights based-data on all stops of civilians, use of force incidents, and interactions where officers ask about immigration status or conduct immigration status checks, the government should mandate that the data be standardized, disaggregated, tabulated and publicly-reported by each police service.

7. The information in any such data collection and retention systems should be de-identified as soon as the personal information is no longer required for an authorized purpose. The resulting public reports must not include personally identifiable information.

THE NEED TO ENSURE ONGOING STAKEHOLDER ENGAGEMENT

Prior to developing a new program, initiative or legislative reform that may implicate privacy or access to information and other fundamental rights, we ask that the Ministry consult with the IPC, as well as other key stakeholders, such as the OHRC. This consultation should occur early on in the Ministry's process.

Recommendation:

8. The Ministry should engage with the IPC, the OHRC and other key stakeholders early on in the development of any initiatives, programs or legislative reforms that may impact privacy or access to information, and other fundamental rights.

CONCLUSION

We look forward to continued engagement with the Ministry, and to further opportunities for dialogue on these and other important policing issues. Consistent with the open nature of these consultations, we will be posting this submission on our website.

LIST OF RECOMMENDATIONS

1. Collaborative community safety and well-being initiatives should be supported by clearly defined governance frameworks that meet transparency and privacy best practices, as well as the requirements in *FIPPA*, *MFIPPA* and *PHIPA*.

2. The government should ensure that any legislative reforms governing collaborative community safety and well-being initiatives respect the data minimization principle.

3. The government should enact province-wide standards governing the use of surveillance technologies.

4. The government should enact rules to ensure transparency and accountability with respect to the use of surveillance technologies.

5. The government should amend the *PSA* and its regulations to require that, subject to limited statutory exceptions, all *PSA* hearing decisions, police chiefs' SIU-related disciplinary investigation reports, and SIU investigation reports be made available to the public.

6. In requiring police services to establish data collection and retention systems to record human rights based-data on all stops of civilians, use of force incidents, and interactions where officers ask about immigration status or conduct immigration status checks, the government should mandate that the data be standardized, disaggregated, tabulated and publicly-reported by each police service.

7. The information in any such data collection and retention systems should be de-identified as soon as the personal information is no longer required for an authorized purpose. The resulting public reports must not include personally identifiable information.

8. The Ministry should engage with the IPC, the OHRC and other key stakeholders early on in the development of any initiatives, programs or legislative reforms that may impact privacy or access to information, and other fundamental rights.

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