Information and Privacy Commissioner,
Ontario, Canada

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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PI16-3

Ministry of Community Safety and Correctional Services

September 13, 2017

Summary: The Office of the Information and Privacy Commissioner/Ontario opened a Commissioner Initiated Privacy Complaint under the *Freedom of Information and Protection of Privacy Act* (the *Act*), against the Ministry of Community Safety and Correctional Services (the ministry). The complaint relates to concerns regarding the collection and destruction of personal information contained in a recording which was made by a police officer with his personal cell phone during a traffic stop. In this Privacy Complaint Report I conclude that I am unable to make a finding as to whether the record at issue contained personal information as defined in section 2(1) of the *Act*, however, I conclude that if the recording had contained the personal information of the requester, it would have been an authorized collection under section 38(2).

This Report also considers whether the ministry has measures in place to ensure the preservation of records in its custody or control and recommends that the Ontario Provincial Police amend its Personal Electronic Device Policy.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*

Orders and Investigation Reports Considered: PO-1880, P-230, PO-3631, M-1053, MO-3287

BACKGROUND:

[1] On June 18, 2015, an access request was made to the Ministry of Community Safety and Correctional Services (the ministry) for a copy of a recording made by a

police constable (the Constable) of the Ontario Provincial Police (OPP) during a traffic stop on December 2, 2013. The request identified the Constable by name and badge number and indicated that the recording was made on the Constable's personal cell phone during a traffic stop. Information about the traffic stop was also recorded in the Constable's memo book, a copy of which the requester provided this office. The Constable's memo book indicated that in the midst of his preparing and providing a ticket to the requester, the Constable observed that she became "angry" and that he activated the "Iphone voice record" function on his personal cell phone.

[2] In response to the access request, the ministry issued a decision letter which advised the requester that the requested cell phone recording did not exist. After receiving this decision, the requester filed an appeal with this office and an appeal file was opened.

[3] During the processing of the appeal, the ministry explained to this office that the Constable had used his personal cell phone to record the interaction and that he did not download the recording (i.e. onto a ministry system). The ministry also advised that, sometime thereafter, the phone stopped functioning and the Constable disposed of it in the garbage.

[4] As there was no reasonable basis to believe the requested information exists, the requester agreed to close her appeal file. In order to deal with the privacy issues raised in this matter - including those associated with the collection of personal information and any related duties with respect to the preservation of records - the IPC initiated a privacy complaint under the *Freedom of Information and Protection of Privacy Act* (the *Act*).

INVESTIGATION

[5] During my investigation I requested and received representations from the ministry. In its representations, the ministry provided additional details regarding the circumstances that led to the recording. The ministry explained that the requester was stopped by the Constable during a traffic stop and subsequently issued *Provincial Offences Act* tickets. The ministry reported that during the encounter, the requester "screamed at the Constable, banged on his cruiser, ripped up the *Provincial Offences Act* tickets the Constable had issued, and threw the tickets all over the highway prior to departing".

[6] The ministry also stated the following in its representations:

> The Constable attempted to record the [requester's] voice on his personal electronic device, specifically due to his concern that the [requester] might initiate legal action, and generally due to the [requester's] abusive and enraged behaviour. The Constable was especially concerned as the

> incident occurred at night time, and there were no apparent witnesses. The circumstances that led to the Constable's decision to attempt to record the [requester's] voice were, in our submission, unusual, to say the least.

[7] The ministry also indicated that the personal electronic device did not contain recordings related to other OPP operational matters (e.g. other investigative matters), and that it is the belief of the Constable that it was neither password protected or protected by encryption.

[8] Lastly, the ministry stated that when the Constable attempted to listen to the recording, it was an inaudible voice and when the device later stopped working altogether, he disposed of it in the garbage.

[9] When asked what steps were taken by the ministry as a result of this incident, the ministry advised that the OPP revised its policies to "prohibit officers from using their personal electronic devices while they are at work."

RECORD:

[10] The record at issue in this matter is a voice recording.

ISSUES:

The following issues were identified from this investigation:

1. Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

2. Was the collection of the information authorized under section 38(2) of the *Act*?

3. Does the ministry have measures in place to ensure the preservation of records in its custody or control, and can those measures be improved upon so as to reduce the risk of similar incidents occurring in the future?

DISCUSSION:

Issue 1: Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

[11] Section 2(1) of the *Act* states in part:

"personal information" means recorded information about an identifiable individual, including,

> a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> c) any identifying number, symbol or other particular assigned to the individual,
>
> d) the address, telephone number, fingerprints or blood type of the individual,
>
> e) the personal opinions or views of the individual except where they relate to another individual,
>
> f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> g) the views or opinions of another individual about the individual, and
>
> h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[12] The list of examples of personal information under section 2(1) is not exhaustive. Information that does not fall under paragraphs (1)(a) to (h) may still qualify as personal information.

[13] To qualify as personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed.[1]

[14] The record at issue in this matter is a recording made by the Constable on his personal electronic device. The ministry has taken the position that based on what the

---

[1] Order PO-1880 upheld in *Ontario (Attorney General) v. Pascoe*, [2002 O.J. No 4300 (C.A.)], Order P-230

Constable has said, the recording taken by him was inaudible and as such the recording did not contain personal information. Specifically, the ministry stated the following in this regard:

> We conclude that the recording contained an inaudible voice. We therefore take the position that the recording did not contain personal information.

[15] As previously indicated, the personal electronic device which contained the recording is no longer available because it was thrown into the garbage when it stopped working. Because of the disposal of the phone, I am unable to review the recording in order to determine whether the requester's words were in fact inaudible.

[16] However, the ministry has indicated that there was a voice captured in the recording. In light of this fact, it is my view that even if the requester's words were in fact inaudible, her voice may still have been recognizable. In addition, the Constable knew the identity of the requester and recorded in his memo book that, in the midst of his preparing and providing a ticket her, he observed that she became "angry" and that he activated the "Iphone voice record" function on his personal cell phone. Accordingly, it is my view that regardless of the fact the recording may have been inaudible vis-à-vis her words, the recording may still have met the definition of personal information to the extent that her voice may have been recognizable on its own or in combination with other records created by the Constable.[2] In other words, the recording may have contained the information of an identifiable individual.

[17] Since the recording is no longer available, I am unable to determine whether the information contained in the recording would qualify as "personal information" as defined in the *Act*.

[18] However, since there is no dispute that the Constable attempted to collect personal information in the form of a voice recording of his interaction with the requester, I have decided that it is important to assess whether the collection would have been authorized if the information was in fact "personal information" as defined in the *Act*, as well as whether the ministry has the requisite measures in place to preserve any such records in its custody or control.

Issue 2: Was the collection of the information authorized under section 38(2) of the *Act*?

[19] Section 38(2) of the *Act* states the following:

> **Collection of personal information**

---

[2] PO-3631

> (2) No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[20] Section 2(1) of the *Act* defines the meaning of law enforcement as:

> (a) policing,
>
> (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
>
> (c) the conduct of proceedings referred to in clause (b);

[21] The definition of "law enforcement" in section 2(1) of the *Act* includes "policing" and the ministry has explained that the recording was made during a traffic stop where the Constable issued *Provincial Offenses Act* tickets while performing traffic stop related duties. The evidence indicates that the recording function of the phone was activated for the purpose of creating a record of that roadside stop, including should it be needed in any related legal proceeding.

[22] During this investigation, the ministry provided this office with copies of the OPP's *Personal Electronic Device Policy* in place at the time of this incident as well as the current policy.

Personal Electronic Device Policy

[23] The policy in place at the time of the incident stated the following in part:

> A uniform member should not routinely use his/her personal cell phone for OPP business related matters. If utilized, his/her personal phone records could be subject to judicial disclosure.

[24] Given the circumstances, I am satisfied that it was not a breach of the OPP's policy to use a personal electronic device for OPP business at the time of the incident.

[25] For all of the reasons set out above, I am satisfied that any personal information collected by the Constable would have been "used for the purposes of law enforcement," and thus the collection would have been in compliance with section 38(2) of the *Act*.

ISSUE 3: Does the ministry have measures in place to ensure the preservation of records in its custody or control, and can those measures be improved upon so as to reduce the risk of similar incidents occurring in the future?

[26] Section 10.1 of the *Act* states the following:

> **Measures to ensure preservation of records**
>
> Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution.

[27] As indicated above, the ministry provided this office with a copy of the *Personal Electronic Device Policy* which was in place at the time of the incident.

[28] On May 1, 2015, this policy was revised and as a result of the revision, using personal electronic devices for operational purposes is now not permitted by the OPP. The policy states that "A uniform member who carries a personal electronic device while on duty: SHALL NOT USE IT: for operational purposes e.g. text messaging, photographs, video, phone calls…"

[29] I note that despite this prohibition, the policy recognizes that the use of a personal electronic device may still occur and addresses any breach of the policy by stating that "…disregarding this policy may result in: discipline; or seizure/disclosure of the device, e.g. Professional Standards Bureau (PSB) investigations, Special Investigations Unit (SIU) investigations, judicial orders, etc."

[30] While I need not decide whether the ministry had custody or control of the voice recording on the Constable's phone, I note that the IPC has established criteria to decide if a record is in the custody or control of an institution. These go beyond the physical location of a record and involve factors such as the purpose of the record, who created it, and whether or not it relates to the institution's mandate or functions. A record does not need to be both in the custody and control of an institution, but rather one or the other. Therefore, in those cases where a record is not in the custody of the institution, the question is whether it is under the institution's control. In deciding this, the IPC considers the following[3]:

1. Do the contents of the record relate to the institution's business?

---

[3] MO-3287

2. Could the institution reasonably expect to obtain a copy of the record on request?

[31] In asserting its authority to seize and disclose a personal electronic device, the OPP policy provides some indication of the ministry's ability to obtain a copy of a record contained in an officer's personal electronic device, at least when that record relates to OPP operational matters.

[32] What the policy does not address however, is the process that should be followed when a personal electronic device is used to communicate or record OPP operational information. In my view, both the current and previous policy fall short as neither address the requirement to *preserve* operational information communicated or captured on a personal electronic device.

[33] In June 2016, this office issued a paper entitled, *Instant Messaging and Non-Institutional Email Accounts: Meeting your access and Privacy Obligations.* This document sets out best practices and guidelines in order to meet access and privacy obligations under the *Act* and its municipal counterpart. Although this paper is about instant messaging and non-institutional email accounts, the issue regarding the use of personal electronic tools, accounts or *devices* is addressed.

[34] Page 4 of this paper states the following in part:

> DEVELOP AND IMPLEMENT CLEAR POLICIES
>
> You must develop clear and consistent policies on the appropriate use of communications tools. These policies should include:
>
> • identify which instant messaging tools and email accounts are permitted for business-related communications, and clearly prohibit the use of other tools and accounts.
>
> • require staff, if they have sent or received business-related communications using unauthorized tools or accounts, to immediately, or within a reasonable time, copy records to their official or authorized email account or the institution's computer or network. This can be as simple as saving a copy to a shared drive or forwarding it to an institutional email account.
>
> • inform staff that all business-related communications are subject to disclosure and retention requirements, regardless of the tool, account or device used, and that they will have to provide a copy of all business-related communications upon request.
>
> • Remind staff that when they are collecting records in response to an access to information request, they must search for and produce

> any relevant records from instant messaging and personal email accounts.

[35] In Order M-1053, Assistant Commissioner Tom Mitchinson addressed the premature destruction of records by a particular police service. He found in that case, which concerned the destruction of records following receipt of the request, that the practices employed by that police service had compromised the integrity of the access process.

[36] In this case, the record at issue was deleted before an access request was made. It is my view that despite this fact, the ministry still has an obligation, as set out in section 10.1 of the *Act*, to ensure measures are in place to ensure the preservation of a record in an officer's personal electronic device when that record contains information relating to an OPP operational matter.

[37] It is also my view that, regardless of whether the OPP's policy prohibits use of a personal electronic device, the moment a personal electronic device is used to record, send or receive OPP operational information, there is an obligation to preserve this information in order to meet the ministry's access and privacy obligations as set out in the *Act*.

[38] The current policy does not address this obligation and since these requirements are not set out in the policy, I will recommend that the *Personal Electronic Device Policy* be amended to require that if a personal electronic device is used to record, send or receive OPP operational information, the information must immediately, or within a reasonable time, be copied to an authorized OPP system or device.

CONCLUSION:

I have reached the following conclusions based on the results of my investigation.

1. I am unable to make a finding as to whether the record at issue contained personal information as defined by section 2(1) of the *Act*.

2. If the recording had contained the personal information of the requester, it would have been an authorized collection under section 38(2) of the *Act*.

3. The OPP's *Personal Electronic Device Policy* should be amended to ensure that the obligations set out in section 10.1 of the *Act* are met.

RECOMMENDATIONS:

I recommend that the ministry ensure that the OPP amend its *Personal Electronic Device Policy* to include a requirement that if a personal electronic device is used to

record, send or receive OPP operational information, the information must immediately, or within a reasonable time, be copied to an authorized OPP system or device.

Within six months of receiving this Report the ministry should provide this office with proof of compliance with the above recommendation.

Original Signed by: September 13, 2017

Lucy Costa
Investigator