NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER

Review Recommendation 14-123
13-175-4
March 10, 2014

In November, 2013, I received a complaint from an individual with respect to what he considered to be an unauthorized use and/or disclosure of his personal information by an official with the Department of Transportation. The Complainant works as a truck driver for a private sector business and was hauling a load to Yellowknife from Fort Providence when he was pulled over by a Highway Transport Officer (HTO) employed by the Department of Transportation. He was given a warning for exceeding the speed limit by 12 km per hour. According to him, he told no one about the matter that day. However, the next day when he got to work, he was met with fellow co-workers teasing him about being pulled over for speeding. When he asked how his co-workers had heard about it, one of his co-workers, who is a room mate of the HTO, told him that the HTO had told him about it. He says that the same Highway Transport Officer made a joke about the warning for speeding again at a later date, this time at his place of employment and in front of a number of co-workers, when the Officer was at the Complainant's workplace to assist the employer to adjust his weigh scales.

The Complainant's letter also pointed to other concerns about statements made by the same Highway Transport Officer in other circumstances and about other matters which he would know about only as a result of his employment with the Department of Transportation.

The Complainant had filed a complaint directly with the Department of Transportation about this issue. In doing so, he met with a manager who recorded the conversation on a cell phone. The Complainant says the investigator did not ask him for his consent to record the conversation and expressed concern about the security of the recording, how the recording was going to be stored and retained.

THE PUBLIC BODY'S RESPONSE

The Department of Transportation conducted an internal investigation and that the "found no evidence to support" the allegations made.

They say:

a) in the course of their investigation, they found no one, other than the Complainant, who would confirm having heard statements made by the Highway Transport Officer;

b) that they could find no evidence that the Highway Transport Officer discussed work matters at home with his room mates.

With respect to the complainant's interview with the Department of Transportation about the incident:

c) the Complainant was informed, before the interview at the Department of Transportation took place, that the conversation would be recorded. According to the public body, the "mobile device was then placed in front of [the Complainant] and turned on";

d) the investigator "ensured his mobile device was password protected and remained in his possession until the recording was able to be stored on the DOT network. Once stored, the recordings were deleted from the mobile device".

e) the recording of statements such as the one given in this instance is "not a routine procedure" but is consistent with best investigative practices.

f) reference was made to the GNWT's Mobile Handheld Devices Policy with respect to appropriate security for mobile devices but there was no

confirmation whether or not the policy was, in this circumstance, complied with.

With respect to the training of HTOs on issues of confidentiality:

g) HTOs hired, including the one who was the subject of this complaint, all have law enforcement training “which includes the requirement for confidentiality” and all employees, including all HTOs sign an Oath of Office and Secrecy when joining the public service.

While the public body indicated that they had conducted an internal investigation, they did not, initially provide me with a copy of the investigation report. I asked for, and received a copy of that report as part of my review.

THE COMPLAINANT’S RESPONSE

The Complainant was not surprised to learn that the HTO involved in this situation, his room-mates or any of the others in the Complainant’s workplace did not confirm what was said to him in the workplace after he got the ticket. What he does know is that the day after he received a speeding ticket from the HTO, he was being teased about it at work by a co-worker who lives with the HTO and it was being talked about in the workplace. He knows that neither his co-worker nor the HTO are going to admit to inappropriate disclosure of personal information and, as for others in the workplace, he thinks that no one wanted to get involved and wouldn’t, therefore, comment.

With respect to the recording of his complaint at the Department of Transportation, the Complainant says that he was quite intimidated by the investigator and his approach to the interview. He says he was told that the mobile device “had” to be turned on and that the investigator “had” to record any and all conversations with respect to this matter. He was never asked if he consented and was not told that he had an option to decline to have the conversation recorded.

He finds it hard to accept the statement, without any backup, that the phone was password protected or that the recording has now been erased from the device. He raises the possibility that the recording may well have been shared with any number of other individuals.

Nor is the Complainant satisfied that the Oath of Office is sufficient to conclude that HTO did not inappropriately disclose his personal information. He is adamant that the HTO improperly disclosed his personal information and feels that he should lose his position as a consequence.

DISCUSSION

The Breach of Privacy Allegations

Section 47.1 of the *Access to Information and Protection of Privacy Act* sets out very clearly that employees of public bodies must not disclose any personal information which they acquire as a result of their employment:

> 47.1. An employee shall not, without authorization, disclose any personal information received by the employee in the performance of services for a public body.

I have reviewed the report prepared by the public body which concludes that there is "no evidence" that the HTO in this case revealed anything about the Complainant. Firstly, I do not agree with the conclusion that there is "no evidence" that a breach occurred. There is, in fact, some evidence, including the Complainant's own statements. Is there enough evidence to determine for certain that the HTO breached the Complainant's privacy? No. However, this is not a court of law in which an allegation must be proven beyond a reasonable doubt or even on a balance of probabilities. While there can and should be an attempt to determine whether or not an alleged breach of privacy actually occurred, this should not be the sole focus of a public body facing a complaint about a breach of privacy. It is not about whether or not there is

concrete evidence which confirms that the breach took place in the manner which has been alleged. It is more about whether or not the allegations can be disproved. Is it **possible** that a breach occurred and, if so, what can be done to address it so that it won't happen in the future? What can be done to improve the policies, procedures and training of staff? Public bodies are responsible for ensuring that personal information gathered or obtained by employees during the course of their employment is protected from unauthorized use and/or disclosure. This doesn't mean that they can rest easy if the breach cannot be proven with certainty. It means that, unless the allegation can be clearly disproved, they need to look at what happened with an objective eye to see if there can be more done to protect individual privacy.

In this case, I am not prepared to conclude that there was no breach of privacy. That's not to say, however, that I am concluding that there was a breach of privacy. What I can determine from the information provided to me is that there is a possibility that the HTO discussed matters arising in his workplace with his room mates at home, who then chose to use that information to tease the Complainant at work. From the materials provided, it also seems fairly probable that the same HTO made comments in the Complainant's workplace about the speeding incident in another instance (though again, this cannot be proven with certainty).

Communities in the north are small. Communities within communities (like the trucking community) are even smaller. Information which GNWT employees receive, obtain or become privy to as a result of their employment must remain solidly within the confines of the workplace and be used only for the purpose for which the information was collected in the first place. It should never be disclosed, except in accordance with the *Access to Information and Protection of Privacy Act*. While I appreciate that every employee working for the GNWT signs an Oath of Office and Secrecy when they begin their employment, this is no a guarantee that the employee will comply with the oath and should not be relied on as evidence that no privacy was breached. Human nature, in fact, guarantees that the oath will be breached at some point by many employees, especially if the message is not emphasized and repeated again and again. There must

be more done in the workplace to emphasize and re-emphasize the employee's obligations pursuant to section 47 of the Act.

The Recording of the Complainant's Interview

I am provided with two very different views of what happened when the Complainant went into the Department of Transportation's offices to file a formal complaint against the HTO. There is some indication that the Complainant's original contact with the department, through an agent, did not go well and that this might have coloured the way in which the department dealt with both the Complainant and with the investigation. For whatever reason, the department felt that it was necessary to record the Complainant's statement, which is, as noted, an acceptable practice in investigative procedures. The Complainant, however, says he felt intimidated by the way in which the investigator dealt with him. I can understand why he might have felt that way. That said, he's a grown man and the complaint was his. This was not his employer and his job was not at risk. The situation was not so intimidating that he couldn't have walked away from it or chosen not to allow the conversation to be recorded, even if he was told that it had to be. The choice was his. He knew the conversation was being recorded and he chose not to ask any further questions about the recording and chose to continue with the interview. In the circumstances of this case, I would conclude that the Complainant provided an implied consent to the recording.

That said, I do have significant concerns about the recording device and how the recording was dealt with after it was made. It is not clear whether the cell phone used to make the recording was a personal cell phone of the investigator or was a government issued one. Either way, a cell phone is not the appropriate device for such recordings. If the cell phone was a personal device, my concerns are obviously more serious, but any cell phone creates concerns about security. The public body says the cell phone was password protected and I accept that. However, I share the Complainant's concerns about what happened to the recording after it was made. Even a password protected device is often accessible to those other than the owners. It is not unknown for passwords to be shared with others, particularly if the device is a personal device.

Passwords are often shared with spouses, children and friends for any number of reasons. I am also concerned about how the recording was managed after it was made. Was it handled in accordance with proper information management procedures? The original recording was, apparently, erased after being "stored on the DOT network". Is it good information practices to be erasing original recordings? Is that within established information management rules? I suspect not. Which only goes to emphasize why recording this kind of interview on a portable device with the intent that it be then transferred and erased is not a good idea.

RECOMMENDATIONS

I cannot conclude with certainty whether or not the Highway Transport Officer in this case breached the Complainant's privacy by talking about his traffic stop among his friends and acquaintances. Even if I could find, with any certainty, that a breach had occurred, there is nothing that can be done to fix that breach after the fact. What can be done, however, is to point out how such a breach might have occurred and address how to avoid the possibility of such breaches in the future. I therefore recommend:

a) that the Department of Transportation provide mandatory ATIPP training to all of its HTOs and senior managers on an ongoing basis;

b) that the Department of Transportation (and all other public bodies) provide ongoing and consistent messaging to all of its employees about confidentiality, and about appropriate and inappropriate uses and disclosures of personal information which employees receive as a result of their employment with the GNWT;

c) that the department create policies and procedures with respect to the use of cell phones and other mobile devices for the purposes of recording either video or voice files in the investigative process and ensure that all information management rules are complied with in the making of such recordings, including providing for appropriate retention methods.

d) that all departments establish specific policies, procedures and rules with respect to the use of personal cell phones or mobile devices for the purpose of conducting public business.

Elaine Keenan Bengts
Information and Privacy Commissioner