

**NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER**

Review Report 20-242

Citation: 2020 NTIPC 46

File: 19-264-4

September 21, 2020

BACKGROUND

The Complainant asked the Office of the Information and Privacy Commissioner to consider whether his privacy and the privacy of a class of Grade 9 students at a local high school had been had been improperly collected, used and disclosed by his employer, the Department of Education.

The alleged breach of privacy occurred when another employee (A.B.) recorded the Complainant and his co-worker making a presentation to a Grade 9 class. The Complainant indicated that he had asked that the presentation be recorded so that he “could review it, and learn from it as a reflective practitioner would”. His evidence was that when he made this request he also indicated that “we would have to ask permission to do this” and he asked A.B. to obtain the necessary consents. According to the Complainant, on the date of the presentation, no permission had been obtained from the school but A.B. recorded the presentation on his personal smart phone after announcing to the class that he would be recording the presentation from the back of the classroom.

The Complainant considered this recording to be a breach of his privacy, that of his co-presenter and that of all of the students in the room who had not provided their consent to the recording.

The Complainant also alleged that his privacy, that of his co-presenter and all of the students whose images appeared on the recording, was further breached when that

recording was shared by A.B. with the Complainant's supervisor. The supervisor had it formatted for use on the GNWT system, uploaded it to the ECE server and invited all co-workers in his division to review it. He insists that his intention when he asked for the presentation to be recorded was that he would be the only person who would have access to the recording and that it would be used only for his own self-evaluation.

The Complainant also contends that when his supervisor saw the video, she pulled the Complainant out of what he was doing for an "impromptu coaching session with [an] HR representative....to give me a full critique of my video performance in front of HR and this was done in a punitive manner". This sharing of the video with an HR employee was, the Complainant alleges, an inappropriate disclosure of his personal information.

THE DEPARTMENT'S EXPLANATION/RESPONSE

The Department of Education, in response to questions from my office during the review, indicated that the Department was aware that the presentation was going to be recorded before the recording was made. It is their position that the recording was requested by the Complainant "for training purposes" and so that it could be shared with the "team". According to A.B. and the Complainant's supervisor, the purpose of the recording was always so that it could be used by the "team" as a cross-training opportunity. For this reason, it was uploaded to the ECE server so that all members of the division's staff could access it. It is the Department's evidence that during a "team meeting" at which both the Complainant and his co-presenter were present shortly after the presentation there had been an announcement that the recording had been made and it was being made available on the network. The Department asserts that neither the Complainant nor his co-presenter raised any objection to this approach at the time.

According to the Department, A.B. had been directed to contact the school principal prior to the presentation to request permission for the recording. The Department

advised that A.B. did, in fact, contact the school principal “and received approval to video-tape the presentation for training purposes.” They did not indicate when that approval was obtained.

When asked what steps were taken to ensure that the recording was used only for the stated purpose of “training”, they advised that it was uploaded to a secure drive on the Department website that only the staff of the Complainant’s division had access to.

I asked if the Department had a policy or protocol in place for the making of such videos and was advised that there was no such policy, though the standard practice when using the video equipment was to get consent forms from each individual recorded.

I also asked if the Department had video-recording equipment available for its use and if so, how such recordings are normally processed, stored and maintained and for how long they are kept. I was advised that video recording equipment is available to all ECE divisions, but that the division involved in this matter did not use that equipment because they were unaware of its existence. Any recording, I was advised, “would be managed like any other electronic record as per the *GNWT Management of Electronic Information Policy*.”

Because the recording was done on a personally owned mobile device, I asked what policies/procedures were in place with respect to the use of such devices for undertaking GNWT work. I was advised that there are no such policies because the *Mobile Handheld Device Policy* provides that only mobile devices owned by the GNWT may access GNWT services and infrastructure. The Department acknowledged that this policy had not been followed in this instance. They advised, however, that the original recording had been deleted from the personal device used to make the recording.

The Department took the position that the consent of the students captured in the video recording was not required because “the recording was not of the student participants.” Rather, they say, the recording was of the presenters and that the direction and approval of the Principal was, therefore, sufficient. Further, they say that before making the recording, A.B. “sought approval from the students by asking them if anyone objected to the recording of the presentation” and no one objected. The students were advised that the recording would be “for internal training purposes”. No information was given to the students about the Department’s legal authority to collect the information or who they could contact if they had questions about the recording because “the focus of the recording was not the students; it was the presenters.”

The Department could not tell me how many times the video had been viewed since being put on the ECE server, but could only confirm that access was limited to those in the Complainant’s division.

With respect to the consent of the Complainant and his co-presenter to the recording being done, the Department indicates that they relied on the implied consent of both employees, who were both aware that the recording was being made as it was being made but took no steps to stop the recording.

The Department conceded, in the end, that errors were made:

Based on this subsequent investigation that I undertook, it is clear that where policies and procedures do exist, they were not adhered to in relation to this situation. The Department commits to communicating these policies and procedures to all staff so that awareness and utilization increases. It is also clear that the Department needs to establish a standard operating procedure for the use of communications equipment

and that this policy should be communicated to all staff within the Department.

THE COMPLAINANT'S RESPONSE

After receiving the Department's submissions, the Complainant provided additional evidence, including a statement from the Complainant's co-presenter that suggested that he knew nothing of the intention to record the presentation until it was announced by A.B. before the presentation began. In his statement, the co-presenter also indicated that, contrary to what the Department had advised, he had raised concerns directly with his supervisor after the meeting at which it was announced that the recording would be uploaded to the ECE server and be made available to the "team". He says that he was rebuffed and told that the Complainant "seemed fine with it" and suggested he speak with the Complainant. The Complainant, for his part, says that he made it absolutely clear to the supervisor in the "impromptu coaching session with HR" the previous day that he was very uncomfortable with the recording being made available to other members of the "team".

The Complainant further questioned the statement that A.B. did not know about the existence of video and camera equipment for the use of Departmental employees. He suggested, in fact, that A.B. had used that very equipment in the recent past to take photographs of all of the employees in the division.

With respect to the Department's statement that the consent of the students was not necessary because they were not being recorded, the Complainant notes that

Students were recorded on the video. In fact, [the Complainant's supervisor] chastised me in our coaching meeting....with HR, stating that she could tell from the video that students were rambunctious, overly

stimulated, and wound-up as a result of my presentation with [his co-presenter] and expressed the concern that this engagement with the presentation would be disruptive to their classes. She also explicitly described that she could see that the students were physically excited and moving around in their seats on the video and that the students were leaping over one another's seats to look at one another's electronic devices when playing the [video] game! – a popular, interactive game that [the Complainant's co-presenter] and I would use in our presentations to reinforce learning outcomes. [The Complainant's supervisor] would not be able to see these students and would not be able to criticize me for how engaged the students were during the presentation and with the ... game if they were not on the recording.

ISSUES

A number of issues come to mind when reviewing the submissions received from each of the parties.

The first, and ultimately the determinative issue, is whether the recording of the presentation involving a class of Grade 9 student was an authorized collection of personal information pursuant to section 40 of the *Access to Information and Protection of Privacy Act*.

A second issue is whether the use of the recording was authorized under section 43 of the Act. Ancillary to this question is what, in this case, constitutes a “use” of the information under the Act.

A third issue is whether there was a disclosure of personal information as contemplated by section 48 of the legislation and, if so, was this an authorized disclosure.

DISCUSSION

There are three distinct actions contemplated in the *Access to Information and Protection of Privacy Act* with respect to personal information. The first is the “collection” of person information. Section 40 sets out when a public body can collect personal information.

The second is “use” of personal information by a public body. While there is no specific definition of the term “use” in the Act, it is helpful to refer to the definition used in the *Health Information Act*, in which the word “use” in relation to information “means to handle, deal with or apply information for a purpose, including to reproduce or transform it, but does not mean to collect or disclose information”. “Use” would include a viewing of information. Generally speaking, “use” relates to how personal information is handled within the public body or the division of the public body which collects it. The authorized “uses” of personal information are set out in section 43 of the Act.

Finally, the Act contemplates the disclosure of personal information. “Disclosure” involves the delivery of information to a third party, including another public body or another division of the public body that collected the information. Again, while there is no definition of the term in the ATIPP Act, the *Health Information Act* provides some useful guidance, defining the term “disclose” to mean “to release information or make information available in any manner, including verbally or visually, to a person or organization”.

1. Collection

Part II of the *Access to Information and Protection of Privacy Act* sets out rules for the collection, use and disclosure of personal information.

By way of preliminary observation, the video recording of the activities of an individual resulting in a record which includes images of that individual constitutes a collection of their personal information. Personal information is defined as being information about an identifiable individual. That would include images of the individual which are of sufficient quality that another person viewing the image could identify them. I am satisfied that the images collected of the Complainant, his co-presenter and the students constitute the personal information of those individuals. The act of making the recording was, therefore, a collection of personal information.

Section 40 prohibits the collection of personal information unless:

- (a) the collection of the information is expressly authorized by an enactment;
- (b) the information is collected for the purposes of law enforcement; or
- (c) the information relates directly to and is necessary for
 - i) an existing program or activity of the public body, or
 - ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council.

There is nothing in the submissions of either the public body or the Complainant that suggests that the video recording in this case was “expressly authorized by an enactment”. Nor can I think of any piece of legislation which might do so. In my opinion, section 40(a) does not provide the Department with authorization to collect the information in this case.

Nor was the information about the students being collected for the purposes of law enforcement and section 40(b) therefore does not apply so as to authorize the collection.

Similarly, the information was not collected because it related directly to a *proposed* program or activity. The program or activity (the Department's presentation to school children in connection with a Departmental program) was already active. Section 40(c)(ii) does not, therefore, justify the collection of the video images in this case.

The question, then, is whether the personal information collected (i.e. the recording of the presentation which included images of Grade 9 students in attendance) was directly related to and necessary for an existing program.

The presentation to the Grade 9 class was, apparently a part of an existing program run by the Department of Education, Culture and Employment and the first requirement for an authorized collection under section 40(c)(i) has been met. The focus, however, is on the second part of the requirement - was the collection **necessary** for the existing program. There is no evidence from which I can conclude that the collection of either the presenter's or the student's personal information in the form of a video recording was **necessary** for providing this Departmental program. Based on the background information provided and the apparent agreement on the part of both the Complainant and the Department that the video recording was not a normal part of the presentation, I have to conclude that the collection of personal information by means of video was not **necessary** to the project or program in question. From the information at hand, the presentation made to the Grade 9 class on this occasion was not the first time the presentation had been made but it was the first time it was recorded. Clearly, therefore, no recording was "necessary" for the purpose of the program.

The public body might argue that the collection of the presenter's images was necessary to evaluate their performance (management of personnel) which is another existing activity of the public body. However, while it might have been a useful tool, collection of this information was not **necessary** for this purpose. The same presentation had apparently been made many times in the past without recording it for

the purpose of employee management so clearly, recording for this purpose was not **necessary** for the purpose of managing personnel. Whether the intention was that the recording be used solely for the purposes of the Complainant's own personal evaluation or for use by the "team" for training or evaluation, it was not "necessary" to the success of the program nor was it "necessary" for the purpose of employee management. The recording may have been helpful for either of these purposes, but was not **necessary** such that the purpose could not be achieved without the recording of third party personal information.

Both the Complainant and the Department have focussed much attention on the question of whether or not either the presenters or the students consented to the collection of their images in this instance. Much could be said about what constitutes a valid consent. However, it is important in this case to point out that section 40 does not authorize the collection of personal information just because the public body has consent for that collection. Consent, at the collection stage, is not a factor which authorizes a public body to collect personal information. A public body cannot validly collect an individual's personal information merely because that person has consented to the collection. The collection must meet the criteria set out in section 40.

I therefore find that the collection of the personal information of both the presenters and the students by way of the video recording was an unauthorized collection of personal information, whether or not there was consent to the collection.

2. Other Issues - Consent

This conclusion effectively ends the discussion because there can be no lawful use or disclosure of personal information unlawfully collected. To conclude otherwise would be antithetical to the purposes of the legislation set out in Section 1 of the Act:

1. The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by...
 - (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies;

It is not, therefore, necessary for me to comment on any of the other issues raised in this review. However, because of the Department's reliance on implied consent with respect to the collection of information in this case, I think it is important to provide some brief additional comments on this issue.

As noted above, consent is not a consideration in relation to a public body's authority to collect personal information. It is, however, relevant and one of the factors which would authorize a public body to use or disclose personal information legally collected. Both section 43, which deals with authorised uses of personal information, and section 48, which addresses authorised disclosures of personal information, allow for the use/disclosure of personal information for any purpose where the person the information about consents to the use/disclosure. However, even here, I refer to section 5 of the Regulations under the ATIPP Act, which states:

5. The consent of an individual to a public body's use or disclosure of his or her personal information under paragraphs 23(4)(a), 43(b) and 48(b) of the Act
 - (a) must be in writing; and
 - (b) must specify to whom the personal information may be disclosed or how the personal information may be used.

The Department cannot, therefore, rely on implied consent for the use or disclosure of the personal information of the students or the presenters. The consent must be in writing.

3. Other Issues - Use of Personally Owned Devices

I also feel it is important to briefly comment on the use of a personal electronic device for the purpose of collecting personal information for public purposes. The GNWT's official policies do not address the use of personal devices for the purpose of undertaking GNWT work. The only policy currently in existence merely prevents personal devices from having direct access to GNWT servers and equipment. The genesis of this policy was the need to protect GNWT systems from cyber threats. It was not about the privacy implications of the use of such devices. I have previously recommended that the GNWT establish a clear policy on the use of personal devices for doing government work because in today's world it is inevitable that employees will use their own laptops or smart phones or other devices to conduct GNWT business from time to time. The current pandemic response is a glaring example of why such a policy is necessary. GNWT staff were sent home to continue work by whatever means necessary which I am fairly certain included the use of personally owned equipment. Nunavut recently experienced a similar issue when they were hit with a ransomware attack which put all government owned electronic hardware out of commission and resulted in employees resorting to the use of their own devices to continue their important work. This has huge implications for privacy and there needs to be clear guidelines and policies in place to ensure, to the extent possible, that privacy continues to be protected in unusual or unexpected circumstances which results in the use of personally owned equipment to conduct government business. In this case, the use of a personal device to record citizens was not only contrary to existing policy and put the privacy of those recorded at risk, but was contrary to even the most basic of good privacy practices.

CONCLUSIONS / RECOMMENDATIONS

I find that the Department of Education, Culture and Employment inappropriately collected, used and disclosed the personal information of two of its employees and a class of Grade 9 students when it made a video recording of a presentation to the Grade 9 class. I further find that the use of a personally owned smart phone for the purpose of making this video recording was not only contrary to privacy best practices and existing policy, but also created a significant risk to the privacy of those recorded.

I make the following recommendations:

1. That the Department extend an apology to the Complainant, his co-presenter and the students who were in the room for the unauthorized collection of their personal information in the recording made of the presentation in question.
2. That the video recording in question be fully deleted from ECE servers.
3. That the Department develop a policy, in consultation with the Department of Finance and the Department of Justice, for the acceptable use of personal electronic devices for the purpose of conducting GNWT business. Such a policy should include direction with respect to:
 - a) restrictions on the use of such devices for GNWT work unless specifically authorized by senior management;
 - b) circumstances in which such uses may be authorized and circumstances in which such uses will not be authorized;
 - c) prohibiting the storing of GNWT owned personal information on a privately owned device in any circumstances;
 - d) requirements for ensuring that any information related to GNWT business stored on a personal device is appropriately secured and, once transferred

to a secured server, fully and properly deleted from the personal device and any cloud storage associated with the device.

Elaine Keenan Bengts
Information and Privacy Commissioner