

Information and Privacy Commissioner,  
Ontario, Canada



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

---

## ORDER PO-3948

Appeal PA17-393

University of Ottawa

April 26, 2019

**Summary:** The appellant, a student, sought access to records relating to alleged security-related incidents in which he was involved. The university denied access to some information in the responsive records claiming it was excluded from the *Act* under section 65(6) (employment and labour relations) and, alternatively, exempt under section 49(b) (personal privacy). The university subsequently withdrew its reliance on the exclusion in section 65(6), claiming only the application of the personal privacy exemption in section 49(b). The adjudicator upholds the university's decision to withhold the records in part, but orders it to provide the appellant with severed copies of security videos.

**Statutes Considered:** *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, as amended, sections 2(1) (definition of personal information) and 49(b).

### OVERVIEW:

[1] The University of Ottawa (the university) received a request under *the Freedom of Information and Protection of Privacy Act* (the *Act*) for incident reports and other records relating to alleged security-related incidents involving the requester. Specifically, the requester sought access to:

Protection Services report numbers [two identified incident numbers]

Any other records from Protection Services mentioning [the requester's] name.

The camera footage from Financial Resources for the following dates and times:

- i) June 12, 2017 from 2:18 p.m. until 2:50 p.m.
- ii) June 13, 2017 from 10:11 a.m. until 10:15 a.m.
- iii) June 19, 2017 from 11:47 a.m. until 12:18 p.m.

[2] The requester's representative then amended the request to include access to all documents and/or records about the requester held by the offices of the dean of a specified faculty department, Protection Services and Financial Resources, and the office of the Associate Vice President of the Financial Resources office.

[3] Responding to the amended request, the university issued a decision in which it granted partial access to the requested records and provided an index of records. The university denied access to some records in full, claiming that they were excluded from the application of the *Act* pursuant to section 65(6) (employment or labour relations). The university claimed other records were exempt under section 49(a) (discretion to refuse requester's information), and section 19 (solicitor-client privilege) of the *Act*.

[4] The requester, now the appellant, appealed the university's decision. A mediator was appointed to explore the possibility of resolution. During mediation, the appellant advised the mediator that he was only appealing the university's denial of access to records under the exclusion in section 65(6) and that he was not seeking access to records claimed to be solicitor-client privileged. This removed sections 49(a) and 19 from the scope of the appeal.

[5] Also during mediation, the university's security office showed the withheld security videos to the appellant and his representative, but continued to claim that the records were excluded pursuant to section 65(6). The parties did not reach a mediated settlement.

[6] The appeal was then transferred to the adjudication stage of the appeal process, where an adjudicator may conduct a written inquiry. In a Notice of Inquiry, the adjudicator initially assigned to this appeal asked the university to consider alternative exemptions that might apply in the event that the records were not excluded from the application of the *Act* under section 65(6).

[7] In its representations, the university maintained that the records were excluded pursuant to section 65(6), but it did submit that, if this claim were not to be upheld, the records were exempt from disclosure pursuant to the mandatory personal privacy exemption at section 21.

[8] In a supplementary Notice of Inquiry, the adjudicator invited the university to elaborate on its section 21 claim, noting that, since the records also contain the

appellant's personal information, the relevant exemption is the discretionary personal privacy exemption in section 49(b) (unjustified invasion of another individual's personal privacy).

[9] With its supplementary representations, the university included a revised decision in which it wrote that it was no longer relying on section 65(6) of the *Act* to deny access to the records. As a result, the university granted full access to an incident report (Record 27), emails (Records 29, 34, 39, 41) and a security video (Record 53), as well as partial access to an incident report (Record 28), and more emails (Records 31-33, 35, 38 and 40).<sup>1</sup>

[10] The university maintained that section 21 applied to the information that it withheld from the incident report (Record 28) and the emails (Records 31-33, 35, 38 and 40) at issue in this appeal. The university also denied access in full to the security videos (Records 51, 52, 54 and 55), citing the exemption at section 49(b).

[11] The university's representations were shared with the appellant, and, although he was invited to make his own representations in support of his appeal, the appellant advised that he would not be submitting any.

[12] In this order, I uphold the university's decision to withhold access to portions of the incident report (Record 28) and the emails (Records 31-33, 35, 38, 40 and 42) because I find that the withheld information is the personal information of other identifiable individuals and is exempt from disclosure pursuant to the personal privacy exemption at section 49(b). I order the university to disclose copies of the security videos (Records 51, 52, 54 and 55) after blurring the images of individuals other than the appellant and university employees.

## **RECORDS:**

[13] The 11 records at issue in this appeal consist of reports, emails and security videos. They are identified as Records 28, 31-33, 35, 38, 40, 42, 51, 52, 54 and 55 in the university's index of records. The information at issue is contained in the withheld portions of Records 28, 31-33, 35, 38, 40, and 42. The entire security videos (Records 51, 52, 54 and 55) are at issue.

## **ISSUES:**

- A. Do the records contain "personal information" as defined in section 2(1) and, if so, to whom does it relate?

---

<sup>1</sup> The records are identified by number in the university's index of records that accompanied its decision.

- B. Does the discretionary exemption at section 49(b) apply to the information at issue?
- C. Did the university exercise its discretion under section 49(b)? If so, should this office uphold the exercise of discretion?

## **DISCUSSION:**

### **Issue A: Do the records contain “personal information” as defined in section 2(1) and, if so, to whom does it relate?**

[14] Under the *Act*, where records contain the appellant’s own personal information as well as that of other identifiable individuals, access to the records is considered under Part III of the *Act*, and the exemptions found at section 49 may apply. By contrast, where a record only contains personal information belonging to individuals other than the appellant, access to the records is considered under Part II, and the exemptions found at sections 12 through 22 may apply. The correct approach is to review the entire record, not only the portions remaining at issue, to determine whether access should be considered under Part II or Part III.<sup>2</sup>

[15] Therefore, in order to determine which sections of the *Act* may apply, it is necessary to determine whether the records contain “personal information” and, if so, whose. Personal information is defined in section 2(1) as recorded information about an identifiable individual, and includes:

(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,

...

(d) the address, telephone number, fingerprints or blood type of the individual,

...

---

<sup>2</sup> Order M-352.

(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.

[16] The list of examples of personal information under section 2(1) is not exhaustive, so information not listed in section 2(1) may still qualify as personal information.<sup>3</sup>

[17] Section 2(3) is also relevant to the definition of personal information. This section states:

Personal information does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

[18] Personal information must be about the individual in a personal capacity. As a general rule, information associated with an individual in a professional, official or business capacity will not be considered to be "about" the individual.<sup>4</sup> Even if information relates to an individual in a professional, official or business capacity, it may still qualify as personal information if the information reveals something of a personal nature about the individual.<sup>5</sup>

[19] To qualify as personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed.<sup>6</sup>

### ***Representations***

[20] The university submits that it withheld portions of Records 28, 31, 32, 33, 40 and 42 that consist of personal information of one of its employees, and portions of Records 32, 33, 35 and 38 that contain what it says is an employee's private cell phone number.

[21] With respect to Records 51, 52, 54 and 55 (collectively, the security videos), to which the university denied access in full pursuant to section 49(b), the university submits that they contain images depicting the faces of students entering and exiting the university's financial resources office. The university says that the financial resources office is responsible for the management and administration of all aspects of

---

<sup>3</sup> Order 11.

<sup>4</sup> Orders P-257, P-427, P-1412, P-1621, R-980015, MO-1550-F and PO-2225.

<sup>5</sup> Orders P-1409, R-980015, PO-2225 and MO-2344.

<sup>6</sup> Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 (C.A.).

students' financial accounts with the university, including matters relating to tuition and fees, financial relief, overdue accounts, payment agreements and other forms of financial assistance.

[22] The university says that the financial resources office is not a general information kiosk and that students attend this office for specific and potentially sensitive matters relating to their financial accounts with the university. The university claims that disclosure of the security videos would reveal these students' personal information, including information relating to their educational and financial history. The university submits that it is not in a position to disclose their images without consent, nor could it obtain their consent because it would be very difficult to ascertain their identity, yet they may be identifiable to others if the videos were fully disclosed.

[23] As noted above, the appellant did not submit representations, including on the question of whether or not the records contain personal information.

### ***Analysis and Findings***

[24] I find that all the records contain the appellant's personal information, including his name, university employees' descriptions of his conduct while at the financial resources office, as well as his image on the security videos. This is the appellant's personal information that falls within the definition of that term in the introductory wording of section 2(1), as well as paragraphs (b), (g) and (h) of section 2(1).

[25] I also find that the records contain the personal information of other identifiable individuals.

[26] Record 28 is a nine-page incident report prepared by the university's protection services that contains a sentence relating to a university employee. In partially disclosing Record 28 to the appellant, the university withheld two instances of the sentence, at pages 2 and 8 of the report.

[27] Although Record 28 includes information about the employee in her employment capacity, the withheld sentence contains the views of another individual about the employee. I find that the views of another individual about the employee meets the definition of the employee's personal information pursuant to the definition of personal information in paragraph (g) of section 2(1). I also find that the sentence contains information regarding the employee that falls within the definition of her personal information under paragraph (b) (and that to describe the sentence further would be to disclose its content that is personal to her) of section 2(1).

[28] Records 31-33, 35, 38, 40 and 42 are email chains from which the university withheld two sentences that it says also contain an employee's personal information in the form of a description, as well as another employee's cell phone number. I will refer to these records collectively as the emails.

[29] Page 1 of Record 35 and pages 1 and 2 of Record 38 contain a telephone number that is identified as a cell phone number. The university submits that it is an employee's private cell phone number. This number appears at the bottom of an email signature that sets out the employee's name, business telephone and address. This contact information, with the exception of the cell phone number, was disclosed. The emails at issue appear to be internal emails, so it is not clear whether this individual uses the cell phone number publicly as a business contact number. However, in the circumstances, namely that the emails appear to be internal emails, that the university disclosed the remaining contact information, and in the absence of representations from the appellant, I accept the university's position that the cell phone number is a personal or private number and that it therefore qualifies as personal information pursuant to paragraph (d) of the definition of personal information in section 2(1) of the *Act*.

[30] I also find that two sentences that the university severed from the emails contain an employee's personal information. As with Record 28, above, these sentences appear in emails documenting an incident involving the appellant and contain information about that employee in an employment context; however, they contain views of another individual about the employee as well as a description of the employee that I find meets the definition of her personal information pursuant to paragraphs (b) and (g) of the definition of personal information in section 2(1) of the *Act*.

[31] Finally, Records 51, 52, 54 and 55 (collectively the security videos) are security videos that the university withheld in full. The security videos contain footage of the appellant as well as various other individuals, presumably students, who attended at or were served by staff in the financial resources office.

[32] I accept the university's evidence that the individuals in the security videos may be identifiable to others if the security videos were to be fully disclosed. I find that the images qualify as personal information pursuant to the introductory wording of the definition of personal information in section 2(1) because they are recorded information about identifiable individuals. I also find that security video footage of their attendance at a financial resources office may disclose information regarding financial transactions that qualifies as their personal information under paragraph (b) of the definition in section 2(1)(b).

[33] For these reasons, I find that the records contain information of the appellant as well as other identifiable individuals that meets the definition of personal information in the introductory wording and paragraphs (b), (d) and (g) of section 2(1).

**Issue B: Does the discretionary exemption at section 49(b) apply to the information at issue?**

[34] In this case, the university applied section 21 to withhold the personal information of individuals other than the appellant, when the records also contain the appellant's personal information. Because I have found that the records contain the personal information of the appellant as well as other identifiable individuals, section

47(1) of the *Act* applies to this appeal. Section 47(1) gives individuals a general right of access to their own personal information held by an institution. Section 49 provides a number of exemptions from this right.

[35] Under section 49(b), where a record contains personal information of both the appellant and another individual, and disclosure of the information would be an “unjustified invasion” of the other individual’s personal privacy, the university may refuse to disclose that information to the requester. Since the section 49(b) exemption is discretionary, the university may also decide to disclose the information to the appellant.<sup>7</sup> Section 49(b) contains a balancing principle, which involves weighing an appellant’s right of access to his own personal information against the other individuals’ right to protection of their privacy. To uphold the application of section 49(b) to deny access, I must be satisfied that disclosure of the information would constitute an unjustified invasion of the personal privacy of those individuals.<sup>8</sup>

[36] In the circumstances of this appeal, I must determine:

- whether disclosing the description of an employee in an incident report (Record 28) and emails (Records 31-33, 35, 38, 40 and 42) would constitute an unjustified invasion of that individual’s personal privacy under section 49(b);
- whether disclosing the personal cell phone number of an individual identified in the emails would constitute an unjustified invasion of that individual’s personal privacy under section 49(b); and,
- whether disclosing the personal information of the other individuals in the security videos (Records 51, 52, 54 and 55) would constitute an unjustified invasion of those individuals’ personal privacy under section 49(b).

[37] Sections 21(1) to (4) provide guidance in determining whether disclosure of the information would be an unjustified invasion of personal privacy under section 49(b), as follows:

- if the information fits within any of paragraphs (a) to (e) of section 21(1), disclosure is not an unjustified invasion of personal privacy and the information is not exempt under section 49(b);
- section 21(2) lists “relevant circumstances” or factors that must be considered;

---

<sup>7</sup> See below, under the “Exercise of Discretion” section for a more detailed discussion of the university’s discretion under section 49(b).

<sup>8</sup> Order M-1146.



- section 21(3) lists circumstances in which the disclosure of personal information is presumed to constitute an unjustified invasion of personal privacy; and,
- section 21(4) lists circumstances where disclosure of personal information does not constitute an unjustified invasion of personal privacy, despite section 21(3).

[38] For records not covered by a presumption in section 21(3), section 21(2) lists various factors that may be relevant in determining whether disclosure of the personal information would be an unjustified invasion of personal privacy and the information will be exempt unless the circumstances favour disclosure.<sup>9</sup>

[39] The following subsections of section 21 are relevant in this appeal:

(1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,

(a) upon the prior written request or consent of the individual, if the record is one to which the individual is entitled to have access;

(2) A head, in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy, shall consider all the relevant circumstances, including whether,

(g) the personal information is unlikely to be accurate or reliable;

(h) the personal information has been supplied by the individual to whom the information relates in confidence.

(3) A disclosure of personal information is presumed to constitute an unjustified invasion of personal privacy where the personal information,

(a) relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;

(d) relates to employment or educational history;

(f) describes an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness.

### ***Representations***

[40] The university submits that the presumptions in paragraphs (a) and/or (d) apply

---

<sup>9</sup> Order P-239.

to its employees' personal information in the report and emails, and to the footage of other students using the financial resources office, so that disclosure of any of this information is presumed to be an unjustified invasion of those individuals' personal privacy. Citing section 49(b), the university says that the personal information of other identifiable individuals in the security videos cannot reasonably be severed and cannot be disclosed without their consent.

[41] As above, the appellant has made no representations regarding any factors that might support his claim that the withheld information should be disclosed, nor did he assert that any unlisted factors might apply to favour disclosure.

### ***Analysis and Findings***

[42] For the following reasons, I find that disclosure of the employees' personal information constitutes an unjustified invasion of their personal privacy. I find that the same is true of footage of other students using or accessing the financial resources office contained in the security videos.

[43] Although neither the university nor the appellant made submissions regarding the factors in section 21(2),<sup>10</sup> in my view, the factors at paragraph (f) and (g) are relevant to the records in this appeal.

[44] The incident report and emails contains a description of an employee that is personal and, on balance, highly sensitive to her, so that the factor at section 21(2)(f) is relevant and weighs against disclosure.

[45] With respect to the security videos, it is my view that the factor at paragraph (g) is relevant and weighs against disclosure. The security videos show students accessing the university's financial resources offices for undisclosed reasons. Given the university's submissions that the financial resources offices is used for specific, potentially sensitive matters, snapshots of student images using this office can be subject to inaccurate or unreliable inferences if disclosed without their consent.

[46] I also find that an unlisted factor, namely fairness, weighs against disclosure of the affected parties' personal information. In my view, it would be reasonable to conclude that students accessing the financial resources office likely did so with the expectation that the video footage of them doing so would not be disclosed. In the circumstances, where these individuals' presence in the financial services offices is incidental or entirely unrelated to the appellant's issues with the university, I find that their privacy interests outweigh the appellant's right to access their information in the security videos.

---

<sup>10</sup> The university referred to the existence of the factors in section 21(2) but did not make substantive submissions on them.

[47] If the presumptions in sections 21(3)(a), (d) and (f) apply, I find that they should be given little weight. Paragraphs (a), (d) and (f) of section 21(3) state that disclosure of information that relates to an individual's employment, educational or financial "history" is presumed to constitute an unjustified invasion of personal privacy. In this appeal, even though the report and emails disclose something about an employee's employment, previous orders of this office have found that the employment history presumption is more commonly applied to a narrower range of records that reveal employment history over time, such as a resume, CV or a record that contains details about a specific incident or disciplinary matter, rather than single comments or snapshots captured in records prepared for other purposes (such as a security report). In my view, the same is true for educational and financial histories: I am not persuaded that video footage of students entering, exiting or accessing a financial resources offices captured in a snapshot in time would disclose information about their educational or financial histories that would trigger the presumptions in section 21(3) on which the university relies.

[48] Finally, I find that no factors, listed or unlisted, weigh in favour of disclosing a private cell phone number, especially when business contact information was fully disclosed.

[49] Weighing these factors and presumptions, I uphold the university's decision to deny access to the withheld portions of Records 28, 31-33, 35, 38, 40 and 42.

[50] Section 10(2) of the *Act*, however, requires the university to disclose as much of a responsive record as can reasonably be severed without disclosing material that is exempt. In this regard, I must determine whether the videos can reasonably be severed to provide the appellant with his own personal information without disclosing the personal information of other individuals that is exempt under section 49(b).

[51] The university submits that this information "cannot reasonably be severed" and "cannot be disclosed without the consent of these other individuals." However, it has otherwise offered no persuasive explanation for why the security videos cannot be severed by applying face-blurring or other obscuring technology to withhold the exempt images of the other individuals who were incidentally in the financial resources office with the appellant on the dates in question. As a result, I will order the university to disclose a severed version of the security videos at Records 51, 52, 54 and 55 to the appellant, applying face blurring or other obscuring technology to the images of all individuals entering, exiting or using the financial resources office, except the appellant and university employees acting in the course of their employment.

**Issue C: Did the institution exercise its discretion under section 49(b)? If so, should this office uphold the exercise of discretion?**

[52] As noted above, the section 49(b) exemption is discretionary, and permits an institution to disclose information despite the fact that it could withhold it. An institution must exercise its discretion. On appeal, the Commissioner may determine whether the

institution failed to do so. The Commissioner may also find that the institution erred in exercising its discretion where, for example, it has:

- done so in bad faith or for an improper purpose
- taken into account irrelevant considerations
- failed to take into account relevant considerations.

[53] In either case, this office may send the matter back to the institution for an exercise of its discretion based on proper considerations.<sup>11</sup> This office may not, however, substitute its own discretion for that of the institution.<sup>12</sup>

[54] The university submits that, when exercising its discretion, it did not act in bad faith or for improper purposes. It says it gave consideration to the factors and presumptions set out in the *Act*, including whether the appellant was seeking his own personal information, whether he had a sympathetic or compelling need to receive the information, and whether disclosure would increase public confidence in the operation of the university.

[55] I have also taken into account that the university disclosed a large number of responsive records and withheld little information from the records at issue. With the exception of the security videos, the university disclosed the records at issue almost entirely to the appellant. I am satisfied that the university did not act in bad faith in withholding the information that it did, considering that it was required to protect the interests of other identifiable individuals whose privacy interests would be affected by disclosure. I accept that the university's exercise of discretion was reasonable, that the university considered relevant factors, and that it did not exercise its discretion in bad faith or for an improper purpose.

[56] While I have found that additional records – severed security videos – must be disclosed to the appellant, this does not affect my conclusion that the university acted appropriately in exercising its discretion. I uphold the university's exercise of its discretion.

## **ORDER:**

1. I uphold the university's decision to deny access to the personal information severed from Records 28, 31-33, 35, 38, 40 and 42.

---

<sup>11</sup> Order MO-1573.

<sup>12</sup> Section 54(2) of the *Act*.

2. I order the university to disclose to the appellant severed copies of the security videos at Records 51, 52, 54 and 55 by **June 3, 2019** but not before **May 28, 2019**. These records shall be disclosed with the following redactions:
  - a. the images of all individuals other than the appellant and university employees acting in their employment capacity are to be obscured using blurring or other obscuring technology.
3. In order to verify compliance with provisions 1 and 2 of this order, I reserve the right to require the university to provide me with a copy of the records that it sends to the appellant.

Original signed by \_\_\_\_\_

Jessica Kowalski  
Adjudicator

\_\_\_\_\_  
April 26, 2019