Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 170-2020

University of Regina

March 22, 2021

Summary: The Complainant sent their instructor at the University of Regina (U of R) an email that contained their personal information, which the instructor later forwarded to 117 students in the same course. The U of R responded to the privacy breach, stating the instructor forwarded the email in error. The Commissioner found the U of R took appropriate steps to manage and address the privacy breach. The Commissioner also recommended that, in the future, the U of R take timelier steps to notify recipients of an errant email to disregard and delete it, and to ensure it asks recipients to confirm they have disregarded and deleted the errant email.

I BACKGROUND

[1] On December 11, 2018, the Complainant sent an email to their instructor at the University of Regina (U of R) that, as the Complainant stated, "disclosed personal information about my health and wellness as well as personal academic information".

[2] On December 12, 2018, the Complainant's instructor forwarded the email in question to the U of R email accounts of 117 students also in the same course as the Complainant.

[3] On December 21, 2018, the U of R responded to the Complainant's privacy breach complaint.

[4] On June 5, 2019, the Complainant's legal counsel sent a letter to the U of R seeking remedy. The U of R responded to the Complainant's legal counsel on July 3, 2019, stating what

steps it had taken to mitigate the privacy breach and that it felt there was no civil liability. The U of R further stated the Complainant has the right to raise their concerns with my office.

[5] On July 24, 2020, the Complainant asked my office to investigate the matter.

[6] On August 4, 2020, my office notified both the Complainant and the U of R of its intent to undertake an investigation.

[7] In undertaking this investigation, I need to clarify its purpose is to assess the steps the U of R took to manage and address the privacy breach and to make recommendations, if any, for improvement.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[8] The U of R is a local authority as defined by subsection 2(f)(xii) of LA FOIP. Therefore, I have jurisdiction to conduct this review.

2. Is the *Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) engaged?

[9] The Complainant stated the email in question (the errant email) contained information on their academic information and their personal health. Upon review of the errant email, I note the Complainant discussed an academic paper, an academic option, and a health matter that was impacting them.

[10] Pursuant to LA FOIP, *academic information* and *health information* are "personal information" pursuant to subsections 23(1)(b) and (c) of LA FOIP, which provide as follows:

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> …
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> (c) information that relates to health care that has been received by the individual or to the health history of the individual;

[11] Based on the aforementioned, I find "personal information" is involved pursuant to subsections 23(1)(b) and (c) of LA FOIP and that LA FOIP is engaged on this matter.

[12] Because the U of R does not dispute a privacy breach occurred, I will move on to assess if the U of R appropriately responded to the privacy breach.

3. Did the U of R respond appropriately to the privacy breach?

[13] My office suggests that local authorities undertake the following steps when responding to a privacy breach:

1. Contain the breach;
2. Notify affected individuals;
3. Investigate the privacy breach; and
4. Prevent future privacy breaches.

[14] What follows is an analysis of each step.

Contain the breach

[15] To contain a privacy breach is to ensure the personal information is no longer at risk. This may include recovering records, revoking access to personal information, and/or stopping the unauthorized practice.

[16] To understand what occurred, it is useful to note the instructor forwarded the errant email from within "UR Courses". According to U of R's website, UR Courses is an online learning environment used by the U of R. The UR Courses *Student Guide* (https://urcourses.uregina.ca/guides/student) explains that a UR Courses account is linked to a student's uregina.ca email account. Within UR Courses, students can manage their courses, as well as communicate with their instructors and other members of their class. Instructors can respond to students from within UR Courses.

[17] It is also useful to note that, at the time of the privacy breach, students could set their preference within UR Courses to have their uregina.ca emails simultaneously forwarded to a chosen outside email account, such as their own personal email account.

[18] When the instructor forwarded the errant email within UR Courses, it was also automatically forwarded to email accounts outside the U of R email system. The Associate Dean, in an email to the Complainant dated December 12, 2018, acknowledged the U of R had no way of recalling the errant email outside the U of R email system, and did not know how many students set their preference to forward their uregina.ca emails to their outside email accounts. The Complainant provided proof, though, that at least one classmate received the errant email this way. The U of R subsequently changed the way this functionality works, which I will outline later in this Report.

[19] The U of R stated the instructor noticed they forwarded the errant email to all students in the course immediately after doing so. The U of R stated this time was 1:07pm on December 12, 2018. Upon noticing their error, the instructor notified Information Services (who manage the email system) and the Associate Dean. At 1:29pm, or 22 minutes after the incident occurred, Information Services shut down UR Courses access to this class and deleted the errant email from within UR Courses. During this time, students in the class who received the errant email did not have access to it through UR Courses, although the U of R stated that prior to shutting down access, it found two students had already accessed the email. The Associate Dean notified the U of R's privacy officer at approximately 2:15pm the same day.

[20] The Associate Dean also sent out a notice to all students to disregard and delete the errant email, which is another important step to take when a privacy breach of this nature occurs. This notice occurred on December 14, 2018 at 10:23am as follows:

> Dear [name of course] Students,
>
> I am writing to each of you today to express my sincere apologies. I am aware you received an email on December 12, 2018, which inadvertently and erroneously shared personal and private information. This error is entirely our fault and I am profoundly sorry for the stress it has caused. I would ask each of you to delete the email including all copies of the email and also ask that you not forward it. The University of Regina is taking this issue very seriously and is investigating the circumstances that led to this breach of privacy.
>
> Sincerely,
>
> [Associate Dean]

[21] The instructor also sent out the following email to the class on December 14, 2018 at 5:08 pm:

> Hello everyone
>
> You have received an email from me with personal information that was inadvertently shared. I apologize for this and ask you to delete my email and not share the information contained in it to others. I apologize for the error.
>
> [Instructor]

[22] I find the U of R took appropriate steps to contain the privacy breach.

[23] I wish to add, however, I am mindful the errant email was forwarded outside the uregina.ca email system without the ability to recall it. This meant the errant email was not fully contained. As such, it was important the U of R took timely action in sending notice to course participants instructing them to delete and disregard the email. Additionally, when it did provide this notice, the U of R should have also asked course participants to confirm they had followed instructions (whether or not they responded). Timeliness can help minimize the impacts of a privacy breach. So, while I find the U of R took appropriate steps to contain the breach, I recommend in the future the U of R: 1) follows up with notice

to recipients to disregard and delete an errant email as soon as possible after discovering the privacy breach; and 2) asks recipients of an errant email to confirm they have followed instructions to disregard and delete it.

Notify affected individuals

[24] Notifying the affected individual of the privacy breach is important so they can determine how they have been impacted and take steps to protect themselves. My office recommends that a notification contain the following:

- a description of what happened;
- a detailed description of the personal information/personal health information involved;
- if known, a description of the possible types of harm that may come to them as a result of the breach;
- steps the individual can take to mitigate harm;
- steps the organization is taking to prevent similar breaches from occurring in the future;
- the contact information of an individual within the organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner (IPC);
- the contact information of the IPC;
- where appropriate, recognition of the impacts of the breach on affected individuals; and
- an apology.

[25] The Associate Dean emailed the Complainant on December 12, 2018, as a "quick follow up to the phone conversation we had earlier this afternoon…" In the email, the Associate Dean outlined to the Complainant what occurred, what actions the U of R took to contain the breach, the likelihood that the errant email had been automatically forwarded outside the U of R email system, the U of R's intent to notify others in the class about the breach, and an apology. The Associate Dean also stated the U of R will consider what steps it needs to take in order to prevent the same type of breach from occurring in the future and update the Complainant on those steps.

[26] In a letter dated December 21, 2018, the Associate Dean followed up with the Applicant outlining the U of R's "summary of the events and our resultant actions". The letter summarized the details of what had occurred to date, including an in-person meeting the U of R had with the Complainant and their family on December 13, 2018. The letter also offered the Associate Dean's recommendations for preventing the same type of breach from occurring in the future, and also acknowledged the impacts the breach may have on the Complainant's "well being now or in the future".

[27] The Complainant stated that in a meeting with the U of R privacy office on January 16, 2019, they were advised of their right to contact my office. While not mandatory to do so, my office always recommends that local authorities advise affected individuals of this right as a best practice because earlier intervention by my office can often help affected parties resolve an issue and avoid a written report. Although it did not occur in this case, the U of R may also proactively report privacy breaches to my office when they occur.

[28] I find the U of R provided appropriate notification to the Complainant.

Investigate the privacy breach

[29] Identifying a privacy breach helps identify the root cause, which is key to understanding what happened and how to prevent similar breaches from occurring in the future.

[30] In its *Privacy Breach Investigation Questionnaire*, the U of R stated the breach, "resulted from an inadvertent error by the professor, but that improvements could be made to the UR Courses system to avoid similar breaches in the future". In terms of what enabled the breach, the U of R stated as follows:

> The functionality of the UR Courses system at the time of the breach allowed message distribution beyond the UR Courses system, due to the settings related to email forwarding. This has since been corrected in order to prevent a similar breach from occurring in the future.

[31] In response to its meeting with the Complainant on January 16, 2019, the U of R added as follows:

> …
>
> (2) [Instructor] responded to your email the next day. [They] intended to copy the teaching assistant (TA) in the "Teachers" section of the address book on [their] reply to you, but inadvertently selected "Students" from the drop-down list in the email module of UR Courses as well. From my conversation with [instructor], it appears that this occurred due to a slip in the alignment using his laptop's touchpad, and a double-click to pick up both categories. Regardless, I confirmed directly with [instructor] that this was a completely inadvertent error, and [they] informed both Information Services and [Associate Dean] of the mistake as soon as [they] noticed.
>
> In answer to the question raised at our meeting about the inclusion of the TA in [instructor's] response, it is typical to alert TAs when there are decisions and discussions with students impacting… I acknowledge that your email to [instructor] contained information about a personal health issue. It would have been more appropriate for [instructor] to inform the TA of his response to your question about the course, while excluding the personal information you provided. I have advised [instructor] of the same.

[32] In this matter, the instructor intended to copy only their teaching assistant (TA) in their response to the Complainant. The instructor also inadvertently selected the option to forward the Complainant's email to all students in the course. This action contributed to the privacy breach, although the U of R pointed out to the Complainant that the instructor should have been mindful to exclude "the personal information you provided" when they were briefing the TA on the Complainant's status. At any rate, the instructor's actions appear to have occurred without malicious intent. The U of R also acknowledged that, as a result of the breach, further safeguards were required to prevent similar breaches from occurring in the future. I will discuss such safeguards in the next section.

[33] I find the U of R conducted an appropriate privacy breach investigation.

Prevent future privacy breaches

[34] Preventing future privacy breaches means to implement measures to prevent similar breaches from occurring.

[35] In terms of preventing similar breaches from occurring in the future, the U of R stated as follows:

> Additional actions were taken to try to avoid a similar situation from occurring in the future:
>
> - UR Courses email functionality was modified to send only a "notice of a notice" to UR Courses users when an email is available.
> - Only the subject line is now "pushed" to non-UR Courses email accounts and users have to go into the UR Courses system to view email content. In this way, if an error is discovered quickly, UR Courses can be locked and the email deleted to avoid widespread dissemination.
> - A second control has been implemented to ensure that users confirm their intention to send an email to a large number of recipients.
> - These additional functionalities will assist in guarding against inadvertent information-sharing going forward.

[36] The U of R also noted the instructor had participated in privacy and access training on December 12 and 13, 2018.

[37] Based on the changes it implemented to its email system within UR Courses, I find the U of R took reasonable steps to prevent similar privacy breaches from occurring in the future.

III FINDINGS

[38] I find LA FOIP is engaged and that a privacy breach occurred.

[39] I find the U of R took appropriate steps to contain the breach.

[40] I find the U of R provided appropriate notification to the Complainant.

[41] I find the U of R conducted an appropriate privacy breach investigation.

[42] I find the U of R took reasonable steps to prevent similar privacy breaches from occurring in the future.

IV RECOMMENDATION

[43] While I find the U of R took appropriate steps to contain the breach, I recommend in the future the U of R: 1) follows up with notice to recipients to disregard and delete an errant email as soon as possible after discovering the privacy breach; and 2) asks recipients of an errant email to confirm they have followed instructions to disregard and delete it.

Dated at Regina, in the Province of Saskatchewan, this 22nd day of March, 2021.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner