

PRIVACY OFFICER'S STATEMENT ON CAMPUS GROUPS

TO: COUNCIL
FROM: SHELDON GOLDFARB
November 20, 2020

Summary/Recommendations

- 1) CampusBase is a platform for clubs (and others) which replaced Clubhouse this year, but which differs from it in including personal information (email addresses, student numbers) for all UBC students instead of just for those joining clubs.
- 2) There is a Directory function in Campus Base which, if enabled, would allow all students to see each other's profiles. This is not allowed under privacy legislation.
- 3) The Directory function has been disabled. We must ensure that it remains disabled or, if possible, permanently removed.
- 4) To that end the AMS IT Department should begin to play a role in overseeing CampusBase.
- 5) There have been two privacy breaches in CampusBase since it was implemented in August.
- 6) We need to get more assurances, perhaps in writing, from Novalsys (the company behind CampusBase) that they are putting security measures in place to protect against further breaches.

Details

General Background

In January 2020 Clubhouse, the old platform for AMS clubs, shut down. Over the next few months the AMS eventually found a new platform from a company called Novalsys. (The platform's AMS version is known as CampusBase.)

There had been some privacy issues associated with Clubhouse, notably the fact that upon implementation it had published the names and email addresses of all members of AMS clubs. This problem was eventually fixed, but with that in mind my main concern with the new platform was to make sure that didn't happen with CampusBase – and it did not.

However, what I did not fully grasp at the time (spring 2020) was how different CampusBase would be from Clubhouse. Whereas Clubhouse was a platform only for those who wished to join an AMS club and thus held personal information (names and email addresses) only for those who joined clubs, CampusBase was going to host the personal information (names, email addresses, and student numbers) for all UBC students.

This in itself was not out of the ordinary. The AMS already possesses lists of its members, as indeed is required under the Societies Act. Such lists are provided by the University and used by the AMS to send out newsletters, conduct elections, etc. The only concern was that in this case the list of information supplied by the University would be hosted on an American server. The AMS as a private organization is allowed to do this, but the University, as a public body, is not. Therefore certain arrangements had to be made, which I believe was done: that is really a University privacy issue, not an AMS one, so is out of my purview, except some people are uneasy with using American servers, so the news I have recently heard about Novalsys planning to set up a Canadian server to host the personal information of UBC students is welcome.

One issue for the AMS did emerge, however: the fact that there was a function in CampusBase which, if enabled, would allow students to see each other's profiles. Since the students have not given their consent to let other students see their profiles, that would not be in accordance with the Personal Information Protection Act (PIPA). I therefore advised that we disable this function, which was done.

However, since a function that has been disabled could at some future date be enabled, we need something in place to prevent that. Since AMS Executives and their staffs change over every year, it has been suggested that permanent staff in the AMS IT Department take over responsibility for this, and I would strongly support that.

A similar issue arose concerning club executives. There was a function on the system that would have allowed them to see individual students on the system. This again seemed like a privacy violation, and I advised against that. My advice was taken, and the system in place now prevents club executives from seeing anyone except those who are in their club or who have applied to join their club. When people join a club, they are told that this will mean the club executives will be able to contact them. This is informed consent and thus complies with PIPA.

I am told that students can also withdraw from CampusBase altogether if they choose, so that again is in line with PIPA.

Privacy Breaches

There have been two privacy breaches concerning CampusBase since it was implemented in August 2020. The first occurred when the system was just about to go live, when student information was being uploaded into the system. During that process, the system crashed and made some student numbers accessible. As Privacy Officer, I evaluated the breach and as a result notified the students whose student numbers had been exposed. This seemed like a one-time incident, with personal information being exposed for only a limited time. We are still waiting to hear an explanation from Novalsys about why a server crash could have this result. This is something to pursue, along with assurances from Novalsys that such a thing will not happen again.

The second breach occurred in November 2020, when it was brought to our attention by a student that there was a bug in the system through which he had been able to access the email addresses and student numbers of all UBC students. He downloaded this information onto a USB which he handed over to the AMS, so it is no longer “out there,” as far as we can determine. He also shared the information with a Ubysey reporter, who wrote a story on the issue. According to Novalsys, only one person actually downloaded personal information, so the presumption is that the Ubysey reporter no longer has such information in their possession.

Novalsys fixed the bug within minutes once we brought it to their attention, but of course this is a serious issue, and there has been a meeting with Novalsys, which I attended, at which their CEO assured us that work is being done to safeguard their security. We will have to monitor this situation. I believe the plan is to have monthly meetings with Novalsys.

CampusBase, I am told, is a very effective platform for clubs (and others), so we would like to continue it. My recommendation is that we do so but that we also monitor the situation.