

College contact-tracing app readily leaked personal data, report finds

Enlarge / A surveillance camera mounted on a wall on a sunny day.

Thomas Winz / Getty

reader comments

32 with 25 posters participating

Share this story

In an attempt to mitigate the potential spread of COVID-19, one Michigan college is requiring all students to install an app that will track their live locations at all times. Unfortunately, researchers have already found two major vulnerabilities in the app that can expose students' personal and health data.

Albion College informed students two weeks before the start of the fall term that they would be required to install and run the contact tracing app, called Aura.

Exposure notification apps being deployed by states, based on the iOS and Android framework that Apple and Google announced earlier this year, are designed to minimize harms to privacy. That framework basically uses a phone's Bluetooth capabilities as a proximity sensor, to see if the phone it's installed on has been near a phone of someone who reports having tested positive for COVID-19.

Aura, however, goes all in on real-time location-tracking

instead, as TechCrunch reports. The app collects students' names, location, and COVID-19 status, then generates a QR code containing that information. The code either comes up "certified" if the data indicates a student has tested negative, or "denied" if the student has a positive test or no test data. In addition to tracking students' COVID-19 status, the app will also lock a student's ID card and revoke access to campus buildings if it detects that a student has left campus "without permission."

TechCrunch used a network analysis tool to discover that the code was not generated on a device but rather on a hidden Aura website—and that TechCrunch could then easily change the account number in the URL to generate new QR codes for other accounts and receive access to other individuals' personal data.

A student at Albion, looking into the app's source code, also found hard-coded security keys for the app's backend servers. A researcher took a look and verified that those keys gave access to "patient data, including COVID-19 test results with names, addresses, and dates of birth," TechCrunch reports.

Aura's developer, Nucleus Careers, fixed both vulnerabilities after the researchers and TechCrunch contacted them about the vulnerabilities. Students and parents, however, are still not enthusiastic. "I think it's more creepy than anything and has caused me a lot of anxiety about going back," one Albion student told the site.

Campus complications

Colleges and universities around the nation are struggling desperately to find ways to manage the fall 2020 semester. Many are only offering online education this fall. Some tried opening as usual this month but quickly had to abandon their plans and switch to distance learning after clusters of COVID-19 cases popped up among the student body. Others are

trying cautiously to find in-between paths that allow students to return to classrooms more safely.

Oakland University, also in Michigan, plans to deploy wearable health-tracking tech—a BioButton—to track symptoms and the potential spread of COVID-19 among the campus population. Initially the university planned to make the BioButton mandatory for all students living on-campus, but school leadership walked that back following a petition from students.

College campuses are an ideal test ground for an array of COVID contact-tracing efforts. Schools can require students to download and install apps in a way that health officials cannot with the general population—although, as Politico notes, students’ participation and compliance may be less than full and enthusiastic, particularly when it comes to disclosing contacts who may have been drinking while underage.

College surveillance

COVID-19 lends an aura of urgency to the matter, but invasive location tracking on college campuses is not new. Schools around the country have been building out tracking systems for several years.

In 2019, for example, the University of Alabama began using location-tracking technology to see which students were leaving football games early. Students who remained through the fourth quarter were more likely to be able to get tickets for championship games.

Other schools rely on Bluetooth beacons and campus WiFi networks to track students around campus, as The Washington Post reported last year. The data not only thoroughly tracks students and compares their behavior to “norms” generated by peers in their cohorts but also may be used for grading and attendance purposes. Students can’t opt out by, for example,

leaving their phones turned off because then they are marked absent and face penalties. One student from Temple University also told the Post that the app his school tracked him with didn't work, and administrators would not believe his word over the faulty data.

Facial recognition, too, is coming to higher education. Advocacy group Fight For the Future identified 10 campuses, out of a list of about 100, that are already using facial recognition technology on campus, with another 30 or so indicating they may choose to deploy it in the future.

School administrators are not the only ones desperate to follow students' movement on, off, and around campus. Some worried parents have also turned to location tracking to keep a remote eye on their kids when those kids become adults and leave for college.

<https://arstechnica.com/?p=1700210>