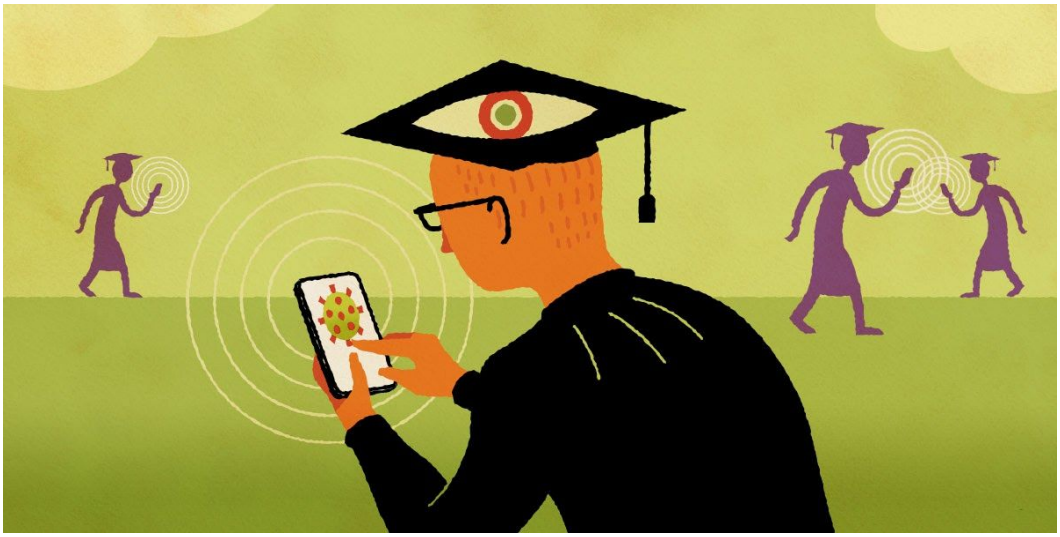
# End University App Mandates



EFF One-Pager
Revised 11.13.20

Learn more:
eff.org/app-mandate

Support our work on net neutrality:
eff.org/donate

Since the Spring of 2020, universities across the country have rushed to adopt new apps and devices to monitor public health on campus. While we applaud the intent to support public health workers in their efforts to prevent community transmission, implementing technical solutions with little transparency, and unproven efficacy, raises a range of privacy and security concerns.

These novel applications are no panacea. They ultimately rely on widespread testing and human follow up with manual contact tracing to provide any value. In order for students, faculty, and staff to have trust in local public health officials, these programs must operate transparently and ensure each member of the campus community is provided the opportunity to offer informed opt-in consent to any surveillance measures put in place—absent any coercion or fear of retribution.

### What are COVID tracking apps?

There is a huge variety of apps being implemented on college campuses. These solutions range greatly in how invasive they are, and how well they have been tested for vulnerabilities and efficacy. Some are developed by the university themselves, while others are in coordination with third-party vendors.

Common uses for these apps include self-screening surveys, all the way to wearable devices which collect sensitive biometrics about the user. Some collect location data by means of GPS, which is not precise enough to show COVID-19 transmission; but can expose other sensitive information, like whether someone has been to a church or a bar. Other programs collect less invasive user proximity data by means of Bluetooth signals.

None of these features can be a replacement for supporting public health workers, access to testing, and preventative measures such as PPE. Even in scenarios where these technologies may prove to be an effective aid, individual users are in the best position to weigh these benefits against the privacy risks for themselves. Also, it is up to the university to make it clear how data will be used and protected.

## Potential Impacts

New technologies for tracking COVID have been developed very rapidly, and have not received the extensive security testing that would happen in a normal development process. The resulting bugs from these rush jobs have the potential to undermine any planned data collection and security protocols. If community members at a university are compelled to use these programs, despite the personal and technical risks, universities risk disproportionately harming the most vulnerable individuals among them.

Putting students and workers in an adversarial position with school officials will only undermine the efficacy of these required apps and devices. For example, if a student is worried about their location being tracked when attending a protest, they may opt to simply turn off their device or leave it at home. Without trust and transparency, officials risk creating less reliable data and potentially chilling free speech on campus.

## Call on University Leadership

We can't let the current crisis set a precedent for universities to intrude on our right to privacy, and foster mistrust with not just the institution but public health workers more broadly. That is why we are calling on university officials to commit to the following:

- Drop any existing mandate for these new apps or devices, and vow to keep similar initiatives entirely voluntary in the future.
- Reveal the contracts universities make with the external vendors of these applications or devices.
- Disclose what kind of information is collected about the users, for what purposes, and specifically which technologies are utilized in this collection.
- Outline how this information is handled, and what specific steps are taken to ensure this data is secure.
- Make it clear which entities, internal or external to the university itself, handle or have access to this data.
- Disclose whether or not the university or external vendors grant access to collected data available to federal, state or local law enforcement.
- Keep up to date information about issues and vulnerabilities in technologies employed, with these updates being as detailed as possible without exacerbating risk.

We need you to join our call on university leadership across the country to commit to our University App Mandate Pledge (UAMP). Good public health outcomes require trust in public health officials, and the opportunity to consent to (or withhold consent from) any surveillance measures put in place. This pledge is a chance for school officials to publicly commit to respecting the privacy, security, and consent of everyone they ask to return to campus.