US schools intensify student surveillance in the COVID-19 era

Kylie Rose
5 November 2020

Millions of students participating in online learning are gravely concerned about how schools are monitoring their activity on and off campus and using their data. As technology continues to advance by leaps and bounds, critical issues of privacy, data use and basic democratic rights are being brought to the fore.

Just last month, the University of Miami was caught using facial recognition technology to track down students who attended a protest opposing the university's reckless reopening plans.

The university emailed nine students who went to the protest to tell them the dean of students wanted to discuss the "incident" which they had participated in, referring to the small protest. When the students questioned the university dean, Ryan Holmes, as to how the university knew the identity of those involved in the peaceful demonstration, he told them the University of Miami Police Department (UMPD) had helped identify the students via surveillance footage.

After a slew of bad press, the university released a short statement denying it uses facial recognition technology. While the university itself may not use the technology, it is evident that the campus police do. In the sheriff's résumé, he states the school utilizes an advanced camera system with sophisticated algorithms for "motion detection, facial recognition, object detection and much more."

This chilling incident raises serious questions regarding the basic democratic rights of students everywhere.

The incident in Miami is not an isolated event. Rather, it is part of a broad trend at K-12 schools as well as university campuses throughout the country. In many cases, schools have used the transition to online learning, brought on in response to the COVID-19 pandemic, to intensify the surveillance of students.

How widespread is student surveillance?

For years, schools have been using surveillance technologies to monitor their students through social media, facial recognition cameras, device usage, location data and more. As the technology has advanced over the years, the scope and depth of the surveillance and data collection has vastly expanded, with very little oversight or regulation.

It is no exaggeration to say that millions of students are monitored daily by private corporations contracted by schools. Gaggle, a leading provider of school email and shared document monitoring, says its technology is currently used to monitor a staggering 4.5 million students across 1,400 school districts.

This trend intensified after the 2018 Parkland shooting. Schools across the United States have since invested a substantial amount of funds toward student surveillance methods. The "school security industry" rakes in nearly $3 billion a year in the United States.

The recent shift to online learning in the wake of the global COVID-19 pandemic has prompted another wave of increased student surveillance. Over the last school year alone, school systems in more than 100 cities have started partnerships with Gaggle.

Businesses like Gaggle, Bark and GoGuardian are often hired to implement 24/7 monitoring of students on the premise that it "protects students' safety." There is, however, no factual basis to support the claim that these surveillance methods keep students safe.

Surveillance companies are able to monitor everything from professional emails to personal chat messages, without permission from the students themselves.

Bark for Schools, for instances, has a frighteningly long list of all things they are able to monitor online. Through Google Suite and Office 365 they are able to monitor videos, pictures, documents, emails, Google Chat messages and more. They also provide a monitoring extension on Chromebook that allows them to collect data on students' web searches, visited URLs and page titles.

In 2017, GoGuardian, a web-filtering and monitoring company, upgraded its technology to scan through every page a student accesses on school devices.

There is virtually no end to the data being collected.

Bark's surveillance is also not limited to school-provided devices. If a student is on a personal computer or phone, surveillance still occurs through the student's Google Suite account. Schools are thus able to enact 24/7 surveillance of students' personal information through personal devices, with no acceptance by parents of students needed.

Under the rhetoric of "protective measures" schools and private businesses can see every single thing being said between students. There is no way of being assured that school administrators are not retrieving data about private information separate from school safety.

Furthermore, as the most recent exposure at the University of Miami demonstrates, there is immense potential for this data to be harnessed to politically intimidate and punish students for speaking out against campus policies or political issues.

The giant corporations behind student surveillance

The private corporations behind student surveillance have deep ties to some of the largest corporations on the planet.

Bark, like many other private surveillance companies, partners with large corporations to store and encrypt the vast sums of data collected.

Bark for Schools, one of the fastest growing student surveillance businesses, is an Amazon Web Services (AWS) EdStart member and uses Amazon DynamoDB, a key-value and document database by Amazon, to organize and store students' data. Bark states that Amazon is a "trusted

partner in the cybersecurity industry, and they handle all of our database encryption needs." It is unclear exactly if and how Amazon uses the data collected. However, since businesses like Bark offer surveillance technologies to schools free of cost, one can safely assume that corporate giant Amazon is getting something in return for this partnership.

AWS EdStart works with many other educational technology startups like Bark. Amazon states they work as a "mentor" for these businesses and offers benefits like promotional credit, access to Amazon Cloud Drive, help with campus management and more. Amazon is offering these services to businesses across the world, making it easier for the billion-dollar corporation to have access to student data.

The nature of these businesses and their deep ties to corporations have immense implications for students. The data being retrieved from student surveillance is not only in the hands of the school. It is also in the hands of the big businesses that have these schools as clients, their partners, and perhaps, behind the scenes, even more dubious actors.

In fact, most of the companies offering spying services to schools hold or have previously held contracts with police departments. Many have direct ties to the Pentagon and intelligence agencies. In 2016, the American Civil Liberties Union (ACLU) exposed one of the companies, Media Sonar, for recommending that police officers follow hashtags like #BlackLivesMatter, #DontShoot, and #ImUnarmed during the 2014 protests against the police murder of Michael Brown in Ferguson, Missouri. In late 2015, Media Sonar also worked with the Ferguson-Florissant School District, which asked for alerts on the terms "protest" and "walkout."

These companies are often contracted without notifying students or parents.

Funding surveillance while defunding basic elements of education

The amount of money being spent by school districts on surveillance is staggering.

According to a report from New York's Lockport City School District, the district has used $3.8 million in public funds to buy facial recognition security systems to identify individuals who "don't belong on campus."

This year, a Minneapolis school spent over $350,000 on a partnership with student surveillance company Gaggle, that uses artificial intelligence and moderators to scan students' private emails, messages and more. School districts in Texas, Illinois, California and Florida spent, from 2012-2018, a combined total of almost $1.5 million, allegedly to detect potential social media threats from well over a million students.

These high-tech surveillance methods are being prioritized over funding in other necessary sectors, like school infrastructure or hiring school social workers.

Just to give a sense of the scope of money spent: In New York, the average school social worker makes an annual salary of around $56,000. If the Lockport City School district shifted their funds from expensive student surveillance systems to employing social workers, they could hire 67 new workers trained in aiding students.

Over the last few decades there have been major slashes in public education funding. According to a report from the Department of Labor, employment in local, state and private education fell by a total of 350,000 this past September.

There has been an overall 20 percent decrease in state funding for higher education since 2008. Under conditions of a deepening pandemic, which is exacerbating the broader economic and social crisis for the working class and poor, the bipartisan gutting of school district budgets across the US is projected to reach an unprecedented scale.

According to a recent Economic Policy Institute (EPI) study, K-12 districts across the US are facing a $1 trillion shortfall by the end of 2021. Ohio Governor Mike DeWine announced a $355 million budget cut from K-12 schools, Georgia officials have begun discussing a $1.4 billion slash in K-12 spending and many other states are proposing massive education budget cuts.

What is driving student surveillance?

According to an article published by the Electronic Frontier Foundation: "There is no evidence that surveilling students will lead to better safety outcomes in general. In fact, the few studies that exist show that more cameras inside school buildings decrease students' perceptions of safety, equity, and support ."

The fact of the matter is that implementing high level monitoring is not being done for students' wellbeing.

Fundamental issues being faced by youth are being ignored, while millions are being spent on jeopardizing young people's privacy for profit. Issues of poverty, mental health and access to resources are being denied while great sums of money are being directed to private businesses to enact more surveillance of students, increasing the policing of schools.

The ruling class, Democrat and Republican alike, is terrified of the coming upheavals of the population. Recent years have seen nationwide protests and walkouts by hundreds of thousands of students motivated by the issues of police violence, school shootings and climate change. The surveillance of students is part of a broader campaign to prepare for mass demonstrations. They are preparing for massive repression.

The University of Miami's surveillance of student protests poses a serious threat to student security—this high level of monitoring is pressuring students to not attend protests or voice their political opinions. Self-censorship as a result of surveillance is being pushed on young people by their government, schools and campus police.

This effort to monitor all student activities is one aspect of a wider process of militarization taking place on campuses throughout the country. It poses immense dangers to the democratic rights of youth, students, and workers everywhere.

The intensification of state oppression, especially as it connects to police violence, is being heightened by this technology. The police are already utilizing these surveillance methods to intimidate students becoming politically active, as seen with the University of Miami's campus police. This oppression will only grow as more schools partner with these surveillance companies and escalate the monitoring of student activity.

The extraordinary social and political situation in the United States—raised to new heights by the coronavirus pandemic—is having a significant impact on the lives of millions of youth and students. The crisis confronting young people needs to be combated with the aim of improving the general wellbeing of students and providing them the best resources possible to meet their physical and mental health needs, which is impossible under capitalism.

Neither the Democrats nor Republicans will wage a struggle against student monitoring—workers and youth must fight this issue together. The fight for student privacy against surveillance companies must ultimately be tied to the fight for socialism.

wsws.org/contact