

THE PUBLIC INDIVIDUAL

Surveillance of Ladue High School students creates questions around safety, student rights and the role of private corporations within schools

* Indicates a false name to protect the identity of an anonymous student

BY ISAAC ZELINSKE
in-depth editor

BY EMERY MAO
staff

PHOTOGRAPHY BY VINCENT HSIAO
photo editor-in-chief

the Domestic Security Alliance Council leverage national security to collect the information of 35 million Americans via 650 private companies. This deal gives them full freedom to comb through everything someone does, from a purchase at Bass Pro Shop to posts on an extremist forum. Companies like Palantir are being used by the United States government to create large-scale databases of the American people in order to find potential domestic threats. This is done by monitoring everything from an individual's social media activity to their daily schedule to their movement. No matter who you are, your privacy no longer exists.

This hardly stops at the adult population. For the student, everything you do with your school issued laptop is monitored by the school. Every email you send, question you search, website you visit, file you save, word you type on a Google doc. Everything you do with your school issued laptop can be monitored. Well, that's another misconception. You aren't just monitored digitally on your school laptop — you are physically monitored everywhere within the school.

With updates in technology, school surveillance no longer stops at a teacher's glance and hall monitors. The student is now monitored by CCTV cameras, decibel detectors in bathrooms and metal detectors at all the entrances. School issued devices are now monitored by an online surveillance program, constantly updating a student profile which is built off your searches, app usage, emails and anything else you do on your school-issued devices. For the student, your privacy no longer exists.

PROTECT

What does surveillance look like at Ladue? Technology Coordinator Adam Stirrat explains the two key ways students are monitored online. The first of these ways is through the Google hemisphere. Ladue uses a Google Enterprise account as its main platform for emailing, document creation and learning management systems. These accounts allow the school to better manage student activity on docs, drive, slides, classroom or any other Google product. Ensuring that students are using these products and services properly.

"That's really just a Gmail account that has a licensed fee that we pay for every year with Google," Stirrat said. "They kind of latch on [the school district], calling [the school] a Google Enterprise facility. So you are indirectly being monitored through Google because when you sign up to be a Google Enterprise institution, everything that you do is saved by Google. Even when students graduate [and] move on, their work never gets deleted. It just gets kind of suspended. So everything is backed up, everything is saved."

The second way is usually the one most people picture in their heads when they hear the word surveillance: the network hemisphere. Through multiple companies, the district is able to watch what websites students go on with their school laptop and monitor the student's searches. Securly is the main service the school uses for search monitoring and Arctic Wolf helps with this.

"We use a company called Arctic Wolf, and we use a company called Securly, and they provide us opportunities to backtrack and keep and capture keystrokes," Stirrat said. "So in a nutshell, we are able to monitor their web traffic, meaning I can see what you did all day long, from minute to minute on every single website, as long as you were logged in onto our computer using our browsers."

The physical aspects of school surveillance, such as the cameras around the building, which are reactive tools, are managed by the safety and security team. It's important to note that this capability to monitor the students activities does not mean someone is always watching, and typically, no one is. The camera's are in place more as a tool for safety and review as opposed to a tool to monitor the student population.

"Day-to-day monitoring, that's really not happening," School Resource Officer Richard Ramirez said. "Obviously, we have a lot of cameras, but those are reactive tools that we use if something happens. We could use that as a reference. But there's not somebody, per se, watching those constantly. We would only go to the cameras if we had to react to something that's already happened."

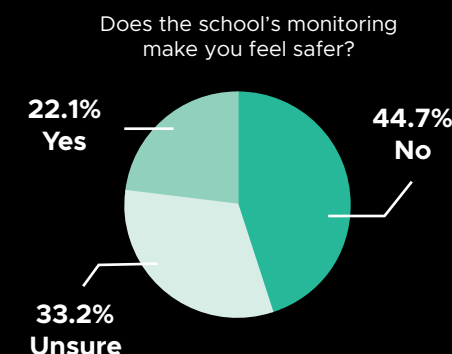
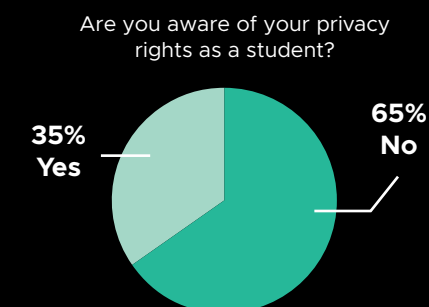
Junior Assistant Principal Andrew Ross agrees; it's important to have a real connection with students, the kind you can't get by watching them through a camera and their search history. Surveillance through the school isn't an end-all be-all, but rather a safety net in case an emergency takes place.

"I find it more humanistic and important to be physically present students in the hallways, saying hi to people in the cafeterias and being in classrooms [rather] than sitting, watching cameras," Ross said.

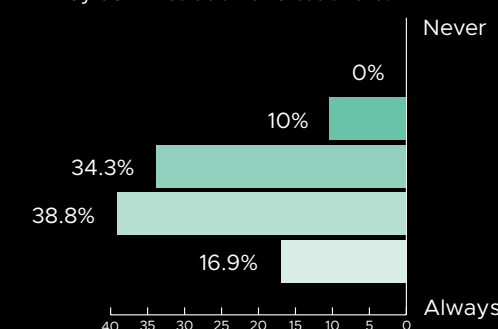
TRACKED BY THE NUMBERS

Ladue students share their views on surveillance in and out of school

Panorama surveyed
202 students March 30



To what degree do you feel monitored by administration and teachers?



Do you have an instance where you felt surveyed by the school?

“I remember looking up something about medication on my phone after school only to have my query blocked because it contained “drug” in it. It made me realize how the school was still watching me even after hours on my personal device.”

E

EVERYTHING YOU DO ONLINE

can be monitored. Every text you send, question you search, website you visit, picture you like, word you type on a Google doc. Everything you do online can and will be monitored. Well, that's what most think, but you aren't just surveyed online — you are surveyed everywhere. Where you drive, what you eat, who you're friends with, daily spending habits, your routine — everything you do can and will be monitored.

This sounds impossible, like conspiracy or something out of Orwellian fiction, but it's our reality. Federal programs like

WHO'S THERE?

Other than school, students are monitored in other ways outside of school

IN-DEPTH

WORKPLACE

Having security cameras is legal, but the workplaces need a legitimate business reason to install them. Employers are also required to disclose the presence of security to their employees.

SOCIAL MEDIA

Apps in general gather data for business purposes. However, social media specifically, focuses on keywords, monitors emotional reactions, and alerts the user on big trends.

TRACKING APPS

Apps like Life360 are used for live tracking. These apps need permission from both sides to work.

SOURCE:

rhombus & sprinklr

The balance between privacy and safety is difficult to define and is subjective from person to person. By allowing students access to school-provided digital devices that can be taken home and used at all times of the day, the Ladue District must also be held to certain standards of technological safety.

“Sometimes we have to do things for the 10% of the time when something bad could happen,” Stirrat said. “90% of the time, students are safely using and behaving on their computers. 10% of the time they’re not, so it’s really hard to kind of just capture the 10%. We’ve got to kind of offer that universal approach of safety and monitoring so you can ensure safety.”

But the school isn’t always able to oversee students online, no matter how many safeguards are in place. Many students use servers called proxies, allowing them to circumvent the school’s internet rules and access blocked websites. For Mordechai Montgomery* (12), whose name has been changed to protect his identity, VPNs and proxies allow him to browse the web without school supervision.

“I’ve used [proxies] ever since I was a freshman here,” Montgomery said. “I started using them because

I was bored in school and I wanted to free myself.”

Montgomery* is not only an avid user of proxies and VPNs, but also a supplier. Many of his friends have been able to access the unblocked internet with his help. However, this usage hasn’t gone without its consequences. Earlier this year, an upsurge in proxy users caused the technology department to step in, leading many to get caught.

“There was a crazy surge of people installing an app called BlueStacks, which is basically an emulator that allows you to run Android apps,” Montgomery* said. “It also circumvented the school network, but because of that surge, the tech office found out [and] they ran a check on everybody’s laptops.”

Even though the blocks the school district puts into place can be inconvenient, Montgomery* still agrees that they’re for the best — even if he doesn’t always follow the school’s rules that are in place.

“It might feel bad to students, even myself, that you can’t access certain websites or something that you want to [do] during your free time, but at the same [time], I can understand why the school went on to do it because there might be a risk of some viruses or you might



LEFT: On a CCTV camera, Ladue students are seen sitting around a table in the cafeteria. These cameras are used to monitor students for safety and security. “We use the cameras to investigate who is doing certain unsafe things,” School Resource Officer Richard Ramirez said. “Nobody’s sitting behind the cameras watching. It’s only when things are brought to our attention.”

BELOW: Safety and security manager Dan Lottmann demonstrates how Ladue High School’s security cameras operate. Lottmann works as part of the safety and security team, which helps monitor the high school’s campus and keeps students safe. “Safety is at the foundational element of any school,” Junior Assistant Principal Andrew Ross said. “If we don’t feel safe, then it makes it really hard to learn, have a positive experience and interact comfortably with others.”



get distracted from learning if you were playing a normally blocked game on your computer,” Montgomery* said.

Safety has, and will always, be the greatest priority for the school. Not only is it a major priority of the administration, it’s their part of their state assigned duties.

“We are responsible for student safety, and we are responsible for knowing at all times,” Ross said. “Following [the regulations] is really important because, God forbid, we actually have a safety incident in a building.”

OBSERVE

There exists an ever present line between the security of an institution and the individual rights and privacy of those within it. Where this line should be drawn is a topic of constant and vigorous debate. For those in favor, there is no duty more dire than that of protection for as many people within the institution as physically possi-

ble. On the other end, opposers bring up arguments of how far that line really needs to be drawn in order to properly balance the rights of each person as an individual and the complete safety of all its members.

“From an educational perspective, I am very taken by the philosophy that you don’t learn when you are not authentic,” social studies teacher Jeff Miller said. “If all I’m thinking about is ‘I’m being monitored,’ there’s no learning. There’s no critical thought happening there.”

Student monitoring extends beyond the physical world and into the digital space. The latter has become extremely commonplace as schools become in-

creasingly reliant on technology for day-to-day education and tasks. Each student and their guardian is required to sign and agree to the terms of the Limitless Learning Parent & Student Technology Agreement in order to access and use their school-issued

devices. This agreement allows administration to monitor safety and ensure proper student use of their school-issued devices.

“When you sign that waiver and that statement, you are signing off that you are using digital devices that are being issued from the school,” Stirrat said. “So, you should assume that everything that you are doing on your school computer is ours to see and watch. That is part of that small fine print.”

The school relies on Securly, one of the many digital software companies for web monitoring. A research study done by the University of California San Diego found that 83% of online surveillance companies used by schools monitor student devices 24 hours a day, seven days a week. Securly is one of these companies, allowing Ladue to observe and manage student activity no matter the location or time.

“I’ve known many people who play a prank on their friend by searching [something] inappropriate on their computer,” Montgomery* said. “Then, that [friend] has been called to the tech office because [of] that thing that was searched on their computer.”

The software itself is in place on the basis of protecting the student body.

M

“My job is to keep you guys safe and out of trouble, not to find ways to get you in trouble.”

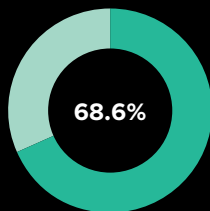
Rick Ramirez,
school resource officer

A DIGITAL TRAIL

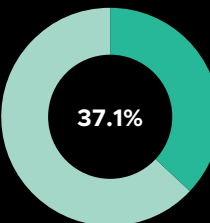
App involvement in data collection and tracking

How much personal data is shared with third parties?

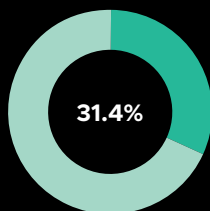
FACEBOOK & INSTAGRAM



LINKEDIN



YOUTUBE



Third parties may include marketers, law enforcement, political parties and government agencies.

How do apps collect data?

Cookies: When a website is visited, cookies are stored to track activity.

GPS: Apps request access to location to provide location-based services.

User Accounts: Creation on user accounts allows activity to be tracked across many devices and platforms.

Permissions: Apps request specific permissions to access features, but they can also be used for tracking.

Accept

Deny

Why do apps collect data?

Apps use tracking mainly for business purposes and in some cases to sell information to third parties. The data collected is used to improve user experience and personalize it to the user's needs. This may include the amount of time spent on looking at something in the app and advertisements that may be interesting or hated. However, some tracking is necessary for the app to function.

Don't Allow

OK

SOURCE:
PAC mag & NYU

However, some critics argue this level of safety could be achieved with a far lesser degree of school surveillance.

"In a liberal democracy, you have to be extremely careful when and how you use those things," Miller said. "History would tell us that it's very easy to slip from like, 'Well, I'm just using it for the right reasons' to 'Wait, now I'm using it kind of all the time.'"

The majority of these services rely on AI models to assist in their data collection. The same UCSD study noted 71% of companies used AI for automatic keyword flagging, and only 43% had a list of human-reviewed words. These key words define what is surveyed, making them extremely important to how these services function.

"I've seen some sort of things around how Palantir, Oracle and other software companies will use AI for data gathering and surveillance, whether that be through ads or through observation," Rony Kaul (11) said. "Then [that data] can be used so that they can get a better grasp of their population."

Kaul has spent a lot of time researching the way AI is being used by these companies. What he's found is that the ultimate goal for a majority of these companies is to create a profile for the people they monitor, predicting when they may want to buy something, when they may do something or when they may commit a crime. Securly functions in a similar way, developing a profile of a student with an added 'at risk' identifier. Based on a student's activity, Securly assigns if the student is all-clear, concerning, at risk or critical. By developing this profile, the school can get a better sense of their student population. However, when schools rely on any form of private, for-profit, corporation, it can potentially bring with it a plethora of complications.

"In order to drive their profit margin as far as they possibly can, these [companies] are going to be as unregulated as they possibly can for as long as they possibly can," Miller said. "You're going to do an analysis of, 'Am I going to do something that could be abusive for a while that makes us a lot of money?' And then five years later, somebody sues them because they've gone too far. Even if they lose that lawsuit, they still win at the end of the day."

With an extremely complicated and nuanced issue like school surveillance, this strict reliance on private corporations could threaten the information and privacy

safety of the school's students. Corporations historically tend to have a less nuanced approach towards this.

"School and at home are two things that have very different moral implications," Miller said. "'What am I doing at school versus what am I doing at home? And to what extent should a school be able to reach what you are doing at home?' Those are the types of questions that private corporations are not as into. They don't like having those conversations unless it really helps their bottom line."

School safety will always be a point of concern for the administration. But, as most things are, this question is not as easy as pushing the scale entirely towards safety and away from the students' rights as individuals. On the other end, it's irresponsible to allow complete and total individualism and freedom on technology while disregarding the safety of the entire student body. However, no matter what side of the spectrum, disclosure is important.

"It definitely feels immoral to keep [the monitoring] under closed curtains from the students," Kaul said. "[Students] wouldn't know any of this. I don't even know any of this. It just feels very wrong."

If the goal of the school is to make the students feel safe, monitoring being outsourced to the services of a private company can complicate student trust in the school.

"Corporations are being driven by profit," Miller said. "It's just that capitalist mindset of: you have to follow profit. You have to grow and grow and grow. And if you have to do those things, you are going to leave morality at the door."

The topic of school surveillance, like national surveillance, has no correct answer. The line between individual rights and the safety of the population will continue to be drawn time and time again. Each of these factors need to be taken into account when it comes to the use of a mass monitoring system within any institution. Ladue administration wants to keep students safe, students want complete freedom and the corporations just want to make money. [P]

'WHAT THE HELL IS A PALANTIR?'

OPINION: Palantir is a dangerous, unchecked company with too much power

BY ISAAC ZELINSKE
in-depth editor

The end of World War II cemented the United States as a global superpower. Following the devastation caused by the atomic bomb, a message of fear was sent to all who opposed the U.S. Since that war, the U.S. has been stingy with such blatant acts of intimidation, but in the modern era, the U.S. is feared beyond their destructive power. Now, war is fought through information. By partnering with Palantir, the U.S. government has been given the digital equivalent of an atomic bomb.

Palantir CEO Alex Karp is often bombarded with questions about what his company exactly is. He has responded with "a software" or "an AI company," but he struggles to say exactly what Palantir is — a surveillance company. Palantir is a company with the express purpose of allowing their clients to collect, manage and observe extremely large sets of data. This seemingly innocent appearance allows the company to dodge the eyes of those that are less observant.

The danger of Palantir is not not in their operations. The U.S. government signed a \$10 billion contract with the military to use their services. According to Palantir, all they do is collect and manage data. However, this data is not just numbers, it's people. Palantir has given the U.S. an all-encompassing view of any population on Earth, including their own. This same technology has been utilized by Immigration and Customs Enforcement, which recently signed a \$30 million contract to assist in the mass deportation of immigrants.

Not only does this seem oddly Orwellian, but it gives Palantir an unbelievable amount of access. Even if you do hold trust with the U.S. government, Palantir is an external, private corporation whose interests do not include the average U.S. citizen. Palantir is dangerous; there has been report after report of the ways Palantir could abuse their unlimited access. They are not an innocent software company designed to protect us all. It is an unregulated surveillance company designed to make profit — not protect the U.S. [P]