Samantha Schlesser

Math 350

Debate Rough Draft

4 October 2019

Schools Should Be Banned from Accessing Laptop Webcams

Computers have been infused into a large portion of society and culture, and access to computers has become increasingly important to people in their day-to-day lives. According to the United States Census Bureau, 8 percent of households reported owning a computer in 1984. However, by 2015, this percentage increased to 79 percent (Ryan 1). Because of their massive impact on daily life, educators have implemented computers in most schools in the country. While this approach has multiple benefits such as developing students’ engagement and instant access to knowledge, there is a setback. School districts that distribute laptops to their students should be banned from remotely accessing and viewing images from the laptops’ webcams due to potential invasion of privacy, possible concerns regarding school policies and the dangers of data collection and use.

A well-known class action case has surrounded this issue: Robbins v. Lower Merion School District. In 2010, The Lower Merion School District in Pennsylvania issued Apple laptops to 1800 students as a part of the “one-to-one” initiative (Page 1). A student, Blake Robbins, was accused by his high school administration of “improper behavior in his home” and was shown a picture that his laptop had taken. The Robbins claimed that they were unaware that student laptops could be remotely activated, and they did not receive any documentation, see any material on the school’s website informing them about it, or sign any forms giving the school permission. It was discovered that the MacBook was activated over 400 times in 15 days and thousands of pictures were taken. The school accused Blake of taking pills, but the snapshot taken by the laptop showed him eating candy (1). This case is a large reason as to why schools should be banned from accessing webcams. While the case did not reveal the reason as to why the school activated the webcam so many times, it probably was not to make sure the laptop was being stolen. If schools are not banned from being able to access the webcams, concerns will arise from parents about the school’s privacy precautions and the technology provider’s policies and agreements with the school. If the school has not informed the parents like in Robbins v. Lower Merion School District, and even if neither the school nor the technology provider has malicious intent, then this could lead to unwanted legal issues. In order to avoid this and students being watched without their permission again, schools should be banned from being able to activate their webcams altogether. To avoid theft, one alternative option would be that schools should be able to track when the student logged on to the laptop instead.

Some schools issue laptops to their students to take home, seeking to give them more tools to succeed, including 21st century technology skills preparation. The transition to a largely digitized world has reduced the amount of personal control over personal data and has opened up more possibilities for unwanted access, and this now is an issue in schools. The Lower Merion School District case is an example of why school districts should not be permitted to access the pictures or webcams of their computers; it was a complete invasion of privacy and a violation of the Fourth Amendment. The ECPA was passed in 1986 as an amendment to the federal Wiretap Act, and generally “forbids the interception of electronic communications without the consent of a party to that communication” (“EPIC - Electronic Communications Privacy Act (ECPA)” 1). Therefore, it is illegal for a school to access the webcams of a student’s laptop without their knowledge. There are alternative ways to make sure prevent theft such as installing a tracking software that the school can only access with the permission of the student and their parents.

Although some schools access the webcams to avoid theft, they could collect far more information on students than is necessary. Not only can a school’s access to student’s laptop cameras invade the privacy of the student, but it endangers everyone and everything in front of the lens, including their family members. The school could use the webcams to collect information about the student or their families that they keep private or for more malicious purposes like stalking or taking inappropriate pictures of the student or family member. The information could be shared without consent or used as commodity. In 2005, a complaint was filed in a U.S. District Court in Nashville, Tennessee after a middle school girl noticed a webcam in a locker room, according to a New York Times article by Patrick Di Justo (Di Justo 1). After the school claimed that the webcam was not positioned to observe dressing and undressing, an official reviewed the video and stated that it showed the girls changing their clothes. It was later found that the video images were available over the internet and were accessed by multiple unknown people (2).

Although this case does not involve school-issued laptops, it supports the argument that school cannot be trusted to have access to explicit or sensitive footage. If the webcam had been on a student’s laptop, and the video was available on the internet, then the student would have been put in a much more dangerous situation; the unknown people watching the video would have gathered information about the student’s residency and/or family without the student’s knowledge. Thus, if schools are not allowed to have webcams in locker rooms for privacy’s sake, they should not be allowed to have access to their student’s laptops for the same reason.

Due to potential invasion of privacy, possible concerns regarding school policies and the dangers of data collection and use, school districts that distribute laptops to their students should be banned from remotely accessing and viewing images from the laptops’ webcams. With new technologies and the growing digital world, protection of the Fourth Amendment is becoming a bigger and bigger concern. Forbidding school districts from potential invasion of privacy is important step forward to fixing this concern.

**Sources/Works Cited**

Di Justo, Patrick. “On the Net, Unseen Eyes.” *New York Times*, 2 Feb. 2005.

“EPIC - Electronic Communications Privacy Act (ECPA).” Electronic Privacy Information

Center. *Electronic Privacy Information Center*, epic.org/privacy/ecpa/.

Page, Andrew. “Watch It! (Cover Story).” Tech & Learning, vol. 31, no. 2, Sept. 2010, pp. 44–52. EBSCOhost,

search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=53833498&site=ehost-

live&scope=site.

Ryan, Camille, “Computer and Internet Use in the United States: 2016,” *American Community*

*Survey Reports*, U.S. Census Bureau, Washington, DC, 2017. s