The Pipe Dream of Sensible School Internet Policy
Adam Kercheval

The American public school system has always had a strange relationship with students' technological autonomy. When I was growing up in the 2000s, technology in school was viewed with caution and resistance more than anything else: Kid Pix and TypeToLearn were the only applications readily and independently usable by students on school computers, and getting online without a teacher in the room was an uphill battle at best. For better or worse, as I aged, this challenge only excited me and my peers, and the thrill of getting past a district firewall created an urge in me to poke holes in security systems that still motivates me to this day.

Now that I work as an elementary school's IT specialist and can once again stick my fingers into the inner workings of public school district technology and security policy, I feel I must report back some concerning news: while technology, access to the internet, and availability of hardware have grown and changed dramatically in schools over the years, the district-wide playbook for cybersecurity is almost entirely unchanged. Still to this day it appears as though district cybersecurity departments spend most of their energy trying to keep students off of individual websites and platforms that they deem dangerous, instead of prioritizing the security of the district and network as a whole. In other words, inside the great firewalled garden that is a school district's network, security measures are typically put in place to police the students (and faculty) inside the garden, instead of making sure that the garden is safe from outsiders to begin with.

At a recent call I attended with other IT workers from my district, we discussed a multitude of security concerns, but predictably the main one held among many was the rise in popularity of TikTok, and the necessity (according to them) of blocking access to it on the district's network. Aside from the very valid concern of phishing, there was practically no discussion of possible security issues that could arise from sources outside of the school's network. There was no mention of our students' unbelievably easy to guess default account passwords, no mention of the increased reliance on Google for account information and personal data storage, and no mention of the school-specific Wordpress sites which are frighteningly out-of-date (when I started working at my school in 2019, our site had not been updated since 2013). TikTok was truly the main concern.

TikTok, is, of course, a place where students can conceivably come across "bad" content, but to spend time and energy attempting to prevent students from getting there in the first place seems not only impossible but also tremendously misguided. District IT departments can obviously block any request going in or out of the network with "tiktok" in the header, but they would be ignorant to think that that would prevent students from accessing the app. Proxies and firewall-circumventing websites are as old as time, and still work darn well. This is not even to mention the glaring hole ripped open in school wifi networks by cellular data. Even the least tech-savvy student can turn off wifi in school and use data to open apps and websites a lot worse than TikTok, and they can even create a hotspot to let their friends on, too!

But no, TikTok is a main concern. Funnily enough, YouTube receives none of the caution that is given to TikTok, perhaps because it is more established in the school system?

More familiar to teachers? Owned by American Google, innocuous and patriotic, unlike subversive and mysterious Chinese TikTok? Whatever the reason, YouTube is deemed educational, and TikTok is deemed evil, despite the reality that TikTok is at worst a classroom distraction, and YouTube is at worst an incubator for school shooters, but I digress.

To be clear, TikTok is indeed a risky place to be online. Only time will tell what information gets shared and to whom by way of TikTok, but it's hardly more concerning in that sense than any other social media platform. Singling it out as Public Enemy No. 1 on district networks won't fix that, and doing so will only divert energy away from preparing for the inevitable break-in that will happen to a district that from the outside is laughably insecure. And of course, my school district is neither the only district to have vulnerabilities like this nor the only district to so blatantly ignore them, and frankly I'm very worried for the day the you-know-what hits the fan, especially if it happens right now during remote learning, when the integrity and accessibility of a school district's network is more important than ever.

Students respond best when they are told the truth, and when they are given independence and responsibility. We would be much better off educating them sincerely about the risks that come with online activity, and allowing them a degree of online autonomy in a space where they don't fear judgment or repercussion for accessing sites that have been deemed non-educational. We can still make sure students are being safe online (I am not arguing for the unblocking of pornography on school networks) while also communicating to them that we trust them and that they are worthy of trust. And to top it all off, we won't have to constantly keep tabs on which new social media sites to block, and can instead spend energy making sure the sensitive data we have access to is kept safe!

Realistically, I understand that this might be a pipe dream, and that large-scale shifts in perception like the one I'm advocating for don't usually happen without an impetus. All I can say is I hope we come out of that impetus in one piece. Until then, I don't have too many problems with pesky school firewalls breeding more hackers.