Edtech: The Ultimate Apt
Michelle Wolfe

This paper aims to explain the main security and privacy issues with edtech platforms. It is not a technical deep dive but an explanation of the key issues faced by schools and privacy advocates. The pandemic has rendered this situation particularly critical. We have a creeping tide of surveillance dressed as child protection. The very sad thing about edtech right now is that technology should render education more accessible. Technology is wonderful, it enhances our lives. Yet with education,it comes at an increasing personal cost even when the platform is free. The ultimate modern trojan horse: surveillance as "for the children".

Schools are and always have been catalysts for inequality. There are deep societal issues that 2020 has brought to global attention. Schools are a large part of our lives and impact the future success of an individual. We need to understand that data is like plasma: there is a constantly renewable source to plunder for third parties and profiling.

So how might this profiling work and how would one know the risks? It is often hard for an individual parent, student or educator to assess risk. When people ask questions, and even as a privacy professional this happens to me, you often get called paranoid or difficult. So to challenge or even enquire about biometrics or the third party data sharing of a platform risks your social capital. It may even risk your child's place in a school or group.

Schools are places where we should operate with trust and respect. Parents leave their children with us in loco parentis. Educators work with accountability and transparency. When parents are presented with an app to use to manage homework, or when educators are told they need to use a proctoring platform, they may assume it has been tested. Trust is inbuilt into the fabric of schools. We demand it from students and parents.Yet do we demand as much accountability from edtech we use?

The implications are serious.Let us examine one scenario. A student enters school at age three.Phonics and numeracy tests define their class level,their behaviour is recorded onto school databases that are shared with a parental app. This app manages school communications. The child struggles with spelling and the parents work long hours and have patchy internet in their part of town. (let us remember that schools across the road from and sponsored by Facebook often don't have wifi). The information on this family might suggest low attainment or lack of engagement. Their

socio-economic profile is often added to data shared with third parties. This ends up creating a larger picture of the local area they live in. Even of the state or region. It might affect what infrastructure investment happens. For example leisure centers or summer schools or tutoring for “better” colleges. Long term it ends up being an area that maybe gets low investment on roads or buildings or healthcare.

This might seem incredible and impossible, yet it happens. In the UK, the government will give third parties detailed data including free school meals and SEND status of ALL the families in a local education area. A recent study of US based education and parenting apps showed that nearly 20% shared data with third parties. Which is not at all compatible with COPPA.

I have worked with non profits and organisations in the USA who managed to install hardware in schools and work for years with the students or parents without the principals of the schools being aware. If the superintendent's office or another school recommends something, people often assume that compliance has been done.

If we return to the issue of internet or device access, we must look at what Chris Gilliard calls “digital redlining”. This is the suppression of groups or communities by restricting access to opportunity: in this case, the internet. In the USA the right to have internet access as a public utility is blocked in around 25 states. If we layer this on top of existing poverty or device access- you begin to see the issues. Schools and edtech assume a level of digital resilience and device/internet access that significant numbers of families do not have. Therefore to extrapolate engagement or attainment metrics based on use of certain platforms is exclusionary.

The most urgent issue however is biometrics and AI. Neither have a legitimate or proportional place in educational settings. Similar to employment consent- it is doubtful that families can actively and willingly consent when they do not have a choice.

Furthermore, it is dangerous and marginalising for young people and their families to have their biometrics, which cannot be changed, entered into a system that may share that data. Let us not forget that in the USA, DHS set up fake schools so that undocumented families would register. They then deported them.

Surveillance in schools is as Audrey Watters says,is police surveillance dressed up as care. It does not belong and we must at all costs, fight it. The

security issues alone around storing biometric data on-site or in vendor clouds, should keep most of you awake at night.

AI and biometrics are used in various ways- from cashless meal payments to exam proctoring and anti-plagiarism software. None of this belongs in a modern education system that cares for equality.

Cashless systems can be done via ID card- as they are in most Silicon Valley tech companies. In addition, the right to access food should never come with a condition. Especially when so many children live in poverty.

Proctoring and anti-plagiarism tech assumes ill-intent. It puts the onus on the student to prove their honesty. This is simply unjust, and places a privileged white Los Gatos living life model on platforms used unfairly in Bangladesh or Costa Rica. So for example: a student with means and regular access to a quiet room with a high speed internet is better able to pass AI checks for "abnormal behaviour" than someone with a noisy street and patchy internet. Pearson will take up to five days for some exams to "check" if a candidate cheated. If the AI says you cheated, how do you fight? Do you then miss out on the job/visa/internship? And you need to re-book a quiet room, maybe pay again for the internet.

Again: education here is a catalyst for inequality and injustice. Remote access to exams and course material SHOULD be the way to balance and inclusion. Yet it is not. Quite the opposite in fact.

So what are the solutions?

Firstly, to collaborate with educators and families. Not influencers or politicians. Ask the people who will use it what they need. Especially marginalised groups. Even "nicer" apps such as mental health apps do not reflect the lived realities of Black students. They need to speak about microaggressions and such which rarely feature in white led design.

Secondly, digital resilience.Inform, empower. Teach everyone how to use the tech- how to use keyboard shortcuts, how to move between tabs, how to type, how to stay safe online. The list is endless. We assume that everyone has used a laptop or email..reader, they have not.

Finally, no is a complete sentence. Especially when it comes to biometrics and AI. We can say no. We can give parents, guardians and students the power to say no and not be the "difficult"one. This also goes for use of SMN

such as Facebook. By all means have a landing page but redirect families to an intranet or portal. Schools should not be chasing clicks and likes and demanding students create accounts to access information.

This talk was inspired by my experience working in schools, as a parent myself and as a privacy advocate. It can feel very isolating being told you are paranoid. CS and IT departments are not privacy or security minded. This is not a criticism but it is important that we do not adopt every bit of shiny tech proffered, for fear of being left behind.