

School Districts & Educational Apps in Classrooms.

By Kayleigh M. Stack

Writer, Blogger, Ethnographic Researcher

<http://kmswritings.pressfolios.com>

Everyday teachers and schools are being bombarded by an influx of education technology apps for free use. Marketed to all forms of educators, “freemiums” are initially pitched to individual users, a genius advertisement tactic to encourage potential customers affiliated with a target demographic to bite the bait - for free - in the hopes to eventually tap into district usage, where the “freemium” model would no longer be available and advanced features come at an extra cost. This is no real surprise since, like most services we enjoy or believe in, eventually comes with a price. However, what is not often expected, that has been happening with the surge of educational apps used in many school districts, is students who have been using such apps at their schools - often considered to be a secure environment - have had their private information, including test scores, school district, age, gender, ethnicity, etc, made publicly available on the internet, without their, or the district's, consent.

This has caused educators in district-wide schools to go into a frenzy. Generally, most teachers have to abide by a set curriculum from their district, with some creative license. The lesson plans the teacher designs need to be vetted by the school or district at which they work. However, the grey area of the vetting process lies in the tools they choose to assist in carrying out their plans. This is where education technology apps slip under the radar in the general assessment. It is not so much about approvable gadgets, since whether or not they get approved for their lesson plan makes little impact in terms of security concerns. The danger doesn't lie in how the the apps use the information gathered from their users.

Let us scale back for a moment before we get ahead of ourselves; falling down the conspiracy rabbit hole can be fatal on many levels. Educational Apps are meant to be exactly what it sounds like – educational. There is no furtive attempt to be malicious, in fact it is the exact opposite. Most learning products are adaptive, meaning they are scalable in the sense that as a person uses the application, it learns more about that user, personalizing the lesson plans to give them challenges in their weakest areas. Hence, the umbrella term for such products – smart devices. The issues lie in the machine learning itself. When technology is adaptive, it is learning about it's users through storing data to analyze it. This information often times is then collected and resold to many different markets – including but not limited to PR agencies, advertising companies, researchers or other educational platforms. User's information is raw data that can be recycled, reused or sold to tailor advertisements for specific target demographics or to help with other educational developments, in this case.

Therefore, it is not the app itself, rather, it is the security and privacy are where the pitfalls lie in the use of such tools in schools. The question for most school districts now is - how do they safeguard their students from personal information being leaked from the apps when schools

are generally in the dark about who is doing the collecting, how the data is being used and where that information is being stored.

How to solve such an issue that is likely to grow over the years as we become more and more inundated by these types of apps? Since most teachers are sovereign entities when it comes to being able to sign-up for external technologies for their students, resulting little-to-no reporting to the district about their in-school use. Therefore, perhaps this is where one begins. Schools can make it mandatory for teachers to report the apps used with students to districts, following a compulsory review from an in-house, or remote, technology director to make sure the app is secure and no student information will be shared to third parties.

Educational Institutes are generally a bit slower on modernizing due to their size and all the tiers of approval that are required, making their more advanced competitors (i.e. educational apps) desirable for teachers to use in classrooms. With all the red tape, antiquated mentalities (at times) and dozens of hoops to go through for district approval, it can be difficult to see dramatic changes fast. However, academic institutes, specifically with a focus on preK - High School, need to perhaps move with a bit more speed when it comes to the current tech culture and the reality in which education is heading. Technology isn't going away, and banning educational apps will eventually become a nearly impossible task. Therefore, setting up the necessary protocol for vetting such devices should become a mandate.

Sources:

<http://mashable.com/2010/11/22/technology-in-education/>

<http://www.nytimes.com/roomfordebate/2012/12/11/privacy-and-the-apps-you-download>