BYOD: Mobile Learning and Copyright Issues

By Brendan McMahon and Fritz Dolak

Wireless technology is quickly becoming commonplace and even ubiquitous. This is true especially in the world of education. According to a study done by Cisco\(^1\), 95.2% of educators are using their smart phones for work purposes, more than any other industry. Teachers, media specialists, administrators, librarians and students alike are all bringing their own smart phones, tablets, laptops, and other mobile devices to connect to Wi-Fi networks. This new trend of BYOD (Bring Your Own Device) potentially creates a multitude of issues including personal information security, device security, and copyright sensitive information security.

All educational resources such as hardcopy textbooks, images, videos, and their electronic counterparts are protected by The Copyright Law, and qualify as vulnerable data. Something as simple as losing an end-node device (such as a mobile device, tablet, or laptop) might very well possibly result in illegal copying or redistribution of that copyrighted data. In universities, it has never been easier for students to bring mobile devices to campus for research and classroom assignments and potentially share that information, regardless of whether or not they have permission to do so. Internet-connected devices aren’t under the protection of the network once they leave the network, and unless precautionary steps are taken, schools might not have any control over what happens to the data once it does leave.

The growth of mobile devices in K-12 school settings\(^2\) is the result of the massive availability of the products for personal use as well as the capacity to use smartphones, tablets, and laptops for educational purposes including flipped classrooms, blended learning, and other customized educational tools to allow students to learn at their own, individualized pace. Many school districts across America are distributing laptops and tablets to students and teachers in order to enhance learning. By providing access to
online resources, copyrighted materials that might otherwise be difficult to duplicate and distribute are now readily accessible to students anywhere they are able to access the Internet.

The opportunity to utilize these BYOD resources is invaluable. We live in a time and place where information is available on demand 24/7. The research process has changed drastically since the advent of online databases such as JSTOR, EBSCO’s Academic Search Premier, and many other e-resources which, for example, offer copyrighted e-books, articles, graphics, audio, and video resources to students and researchers for a licensing fee or free of charge for legitimate educational uses. The response of those involved in copyright compliance should keep the benefits of these services in mind and aim to be proactive about potential infringing activities rather than being reactive to a DMCA takedown notice or potential lawsuit. Setting instructions and guidelines for teachers, media specialists, administrators, and librarians seems to be a sound, best practices approach. School officials and administrators should offer education on these issues and explain potential copyright infringing activities that might occur when mobile devices are lost or misused.

To assist in alleviating these potential copyright infringements, a valid option would be to create tiered or divided structures of access to materials. For K-12 schools, this might mean different levels for different classes. The same could be applied for teachers, media specialists, administrators, and librarians, including higher-education students. There already exist different hierarchies that could easily be utilized. For example in academia, a caste system of privileged access could consist of graduate assistants, adjunct faculty, full professors, department heads, and so on. Jeff McMahon, Chief Information Officer of Decatur Township, describes a system that is utilized in which different wireless networks allow different levels of authorization, from students, to teachers, to administrative faculty. This system uses special software to monitor logins and what kinds of information users are allowed to view. Each level would be afforded increasing access to and educational rights to copyrighted materials. Another model might consist of different colleges within a university not having access to this same copyrighted information or by placing copyrighted materials on a course management system like Blackboard allowing access to copyrighted materials only to those students who are enrolled in that specific course.

Perhaps the most realistic, but expensive option in terms of securing copyrighted materials and protecting privacy is the inverse-BYOD, where an institution administers
devices and retains ownership, but allows the personal, educational use of those devices. Many school districts, such as Indianapolis Public Schools have already adopted this concept by distributing laptops and tablets for students to use in both at school and at home. The school, however, still has control of the device and how it is used, even when students access the internet outside of the network. By doing this, an administrator could restrict access to certain types of data or block ports typically used for file-sharing without invading someone’s privacy, as would be the case if the administrator tried to set restrictions on a laptop a student has bought. In the event that copyright laws were being potentially infringed, the school has the ability to restrict Internet access, access to the device itself, or completely retract the device.

BYOD is a growing phenomenon. Consequently, academic institutions and K-12 districts need to embrace the change, but also address the very real potential of copyright infringement due to a lack of potential security issues in order to be compliant with the U.S. Copyright Law and avoid any potential infringing activities.

While BYOD has allowed educators and students to find new and better ways to teach and learn, educational institutions of all levels need to be aware of the potential inherent threats. A lack of planning and security could lead to copyright infringement or violating educational licenses but armed with the knowledge and a strategy, BYOD can simultaneously provide productive educational benefits as well as complying with the Copyright Law.

4. Jeff McMahon was the Director of Instructional Technology at Indianapolis Public Schools from 1986 to 2013 and has been the Chief Information Officer at Decatur Public Schools since June of 2013.