Key Challenges Associated with Bringing Personal Mobile Devices to the Higher Education Classroom

Ieda M. Santos, Ph.D
Emirates College for Advanced education
P.O. Box 126662 Abu Dhabi, UAE
isantos@ecae.ac.ae

ABSTRACT
The use of students’ personal mobile devices in education seems an attractive option to higher education institutions as these devices may help reduce costs as well as support teaching and learning. However, the concept of “bring your own device” or BYOD, presents challenges to institutions used to control which technology students and faculty would adopt in teaching and learning practices. This paper aims to review key challenges associated with the BYOD initiative often discussed in the relevant literature. These challenges include network infrastructure, network security, IT support, equity issues, and BYOD disruptions. The paper also reviews a case study recently conducted at a higher education institution in the United Arab Emirates to illustrate in practice how these key challenges may affect the adoption of personal mobile devices in the classroom. Based on the review, this paper proposes potential strategies to help minimize these challenges.

Keywords
Personal mobile devices, BYOD, classroom, institutional challenges

INTRODUCTION
More and more students are arriving at universities with personal mobile devices, such as smart phones, iPads and notebooks. These devices are students’ everyday tools, and are becoming their first choice for accessing the Internet, as well as for communication services and media and software applications (Lundin, Lymer, Holmquist, Brown & Rost, 2010; Melton & Kendall, 2012). It is predicted that the number of students’ personal mobile devices will increase in university contexts (Fang, 2009) and will be increasingly used to complement learning activities.

Traxler (2005) suggested that forms of mobile learning should explore the use of personal mobile technology. Recently, widespread ownership of mobile devices among students in higher education has been seen as providing an unprecedented opportunity for harnessing these devices for teaching and learning (Vanwelsenaers, 2012; UNESCO, 2013). Contrary to traditional policies that rely on universities providing students with technology (Hlodan, 2010), the ubiquitous mobile devices allow educational institutions to adopt BYOD programs (Kobus, Rietveld, & van Ommeren, 2013). More specifically, students’ mobile devices are used to support teaching activities in and outside the classroom.

Some universities are already embracing the BYOD program (Abram, 2012; Cisco, 2012). This trend is predicted to continue to grow for the foreseeable future (Dahlstrom & diFilipo, 2013). The BYOD program seems an attractive option for educational institutions because of reduced costs as it takes advantage of the already available technology that students own (Traxler, 2005; UNESCO, 2013). In addition, these devices can potentially enhance classroom learning, for instance, anywhere and anytime access to learning resources, and can promote collaboration, interaction, and support-differentiated instruction (Violino, 2012; Johnson, 2012; Santos, 2013). However, integrating students’ personal devices in the classroom presents major challenges to higher education institutions. Traxler (2010b) noted that:

Student devices present a major challenge to many of the institutional practices and procedures associated with ICT and “conventional” desktop e-learning. It is easy to say that education should embrace student devices but not easy to say how. This is part of the paradox. (p.156)

The challenges often discussed in the literature are associated with network infrastructure, network security, technical support, equity issues and classroom disruptions. The purpose of this paper is to present a review around these key challenges. This is followed by a review of a case study recently implemented at a higher education institution within the United Arab Emirates to illustrate how these challenges occur in practice when adopting personal devices in the classroom. Based on the review and the practical example provided, the paper expects to discuss potential strategies to help minimize the challenges.

BRING YOUR OWN DEVICE
Students’ use of personal technology in higher education began with the adoption of laptops in the late 1980s (diFilipo, 2013). However, what is different now is the way in which mobile devices can be utilized, allowing access to information and communication tools anytime, anywhere (Cherwell Software, 2012). When educational institutions decide to embark on a BYOD program, it means that they would be explicitly implementing a policy on relying on students’ personal devices.
technology (Hockly, 2012). The basic idea behind the BYOD model is that students will use their personal devices to support teaching and learning. This idea contrasts with institutions providing students with mobile technology. For example, Abilene Christian University issued iPhones and iPods to a group of students and faculty to carry out learning activities (Perkins & Saltsman, 2010). Lin and Rivera-Sánchez (2012), on the other hand, discussed the implementation of a mandatory SMS student response system in a Singaporean University where students used their personal mobile phones to participate in weekly and graded classroom quizzes. In this case, the authors suggested that all students owned a mobile device, making it feasible to implement the BYOD initiative.

As noted by Traxler (2010b), educational institutions cannot afford to ignore the use of students’ personal mobile devices in education. These are students’ everyday tools that can be used to enhance their learning in and outside the classroom. Cisco (2012) added:

Students can use their mobile devices to respond to multiple-choice questions, allowing professors to collect active feedback within minutes. Users can also access online applications such as MATLAB and Blackboard for anytime, anywhere learning using their preferred devices...This capability, combined with the fact that wireless access is available in more far-flung areas of the campus, is improving convenience and promoting a richer learning experience. (p.3)

While the BYOD program offers opportunities for higher education institutions ranging from teaching and learning opportunities to reduced technology costs (e.g. Traxler, 2005; Manuguerre & Petocz, 2011), it also presents challenges (Dahlstrom & diFillipo, 2013; Traxler, 2010a). In the following sections, the paper discusses key challenges associated with integrating students’ personal mobile devices in the classroom.

NETWORK INFRASTRUCTURE
It has been argued that if higher education institutions plan to embrace and benefit from a BYOD program, they would need a robust infrastructure that supports a wide range of wireless enabled mobile devices (Dede & Bjered, 2010; Cherwell Software, 2012). According to Dahlstrom and diFillipo (2013, p. 3), the challenge is “Maintaining and upgrading infrastructure to accommodate more devices and technologies that cross paths with IT domains, predicting what the next technology will be in order to proactively be ready to accommodate it.”

Studies have suggested that lack or poor Internet connectivity can cause disruption to mobile learning activities. For example, Nykvist’s (2012) case study on the use of BYOD in teaching reported that the institution network was not initially built to handle an extreme load of wireless mobile device users. According to the author, when multiple classes were running at the same location, saturation could quickly be reached and students found it hard to obtain IP addresses, or encountered an extremely slow transfer of data. Similarly, Stav, Nielson, Hansen-Nygard, and Thorseth (2010) found that students had difficulties in completing learning activities due to technical problems associated with reduced network capacity. The study recommended the institution to provide sufficient capacity in the wireless network and proper location of access points.

Mobile computing requires connectivity and needs to be delivered wirelessly (Campbell et al., 2013). According to Dede and Bjered, (2010), most institutional technology infrastructures are built on the assumption that student Internet access occurs within computer labs for a period of time. The same infrastructure supporting those computer labs is used for administrative purposes. Therefore, to accommodate a BYOD program, many institutions will need to upgrade their network capacity by increasing bandwidth, adding wireless access points, and boosting their network management capabilities (CDW-G, 2012; Fritschi & Wolf, 2012). Improvements in the network infrastructure, however, imply that universities must support the financial costs of maintaining and sustaining wireless access (Melhuish & Falloon, 2010). Campbell et al. (2013, para. 23) stated that “…we have much still to do to enable an infrastructure that is scaled sufficiently and flexible enough for BYOD but that is just another example of the things on which we higher education information technology should spend our dollars.”

NETWORK SECURITY
A further implication for higher education institutions is related to network security. In other words, allowing students to connect their personal mobile devices to the institutional network can expose sensitive information (diFilipo, 2013). Higher education institutions have been dealing with BYOD since they started issuing laptops to students. However, the number of mobile devices that students currently bring to university campuses has strained the existing security (diFilipo, 2013). A BYOD program represents a dramatic shift for many institutional IT departments accustomed to controlling which technology students and faculty could use. Such an approach enables IT personnel to manage network and information access privileges to maintain the level of data security (Emery, 2012). Markeelj and Bernik (2012, p.103) noted that “The usage of mobile devices can’t be restricted just because they represent an information security risk, but we should use this technology wisely.”

Several security risks related to BYOD have been discussed in the literature. For example, the loss of a mobile device that is unprotected could mean exposure to personal or corporate data that users might have stored in that device. A further risk is that mobile devices can communicate with various networks concurrently, regardless of firewalls. If a mobile device is connected to an institution’s network as well as a public network, an unprotected path to the institution’s
central information system can potentially be opened, creating a security issue. A mobile device can become a gateway to an institution’s private information (Markeel & Bernik, 2012). Markeel and Bernik (2012) observed that there is no available system to enable institutions to monitor the performance of their information system in regard to accessing and transferring data via mobile devices. However, institutions can educate students and faculty about security practices and network polices as well as remind them about responsibilities as users (CDW-G, 2012). The literature has suggested several strategies that institutions can implement to secure corporate data as well as other sensitive information (Violino, 2012; Markeel & Bernik, 2012; Poe & Garfinkel, 2009). A widely discussed strategy is to require students and faculty to register their personal devices with the IT department (referred to as Mac address registration). The network will only provide access to the registered devices. Many universities use this strategy to protect their wireless network/s. For example, as part of its security system, the University of South Florida1 in the United States requires students to register their devices with the IT department. When students register their devices, it enables the IT personnel to track or monitor a wireless user through its Mac address. A further strategy includes implementing private segregated networks for mobile device users which prevent them from accessing corporate data (CDW-G, 2012).

**IT SUPPORT**

According to Traxler (2005), mobile learning creates a demand for support structures and its development is dependent on the institutional capacity to provide such support. A study by Smith, Salaway and Caruso (2009), for example, suggested that if the number of mobile device users increased, then the institution’s IT department would be overwhelmed with demands for technical support for those devices. However, supporting multiple mobile devices with different models and operating systems can be more complicated than supporting a range of identical devices purchased and maintained by IT staff (Sangani, 2013). Traxler (2005) noted that:

> …the perception amongst IT support staff that the whole area of handheld computers, their platforms and their applications is too personal, fluid and diverse to... support at an institutional level in the way that PC provision is supported...This kind of attitude will inhibit experimentation and progress... (p. 184)

Quinn (2012; p.101) observed that a “top issue is whether to support learner-owned devices...” Campbell et al. (2013) pointed out that if higher education institutions expect students to use their own devices in the classroom, it creates an obligation to provide support for those devices. However, others have indicated that students should be responsible for repairing their faulty/damaged mobile devices (CDW-G, 2012; Hockly, 2012). According to CDW-G (2012), IT support should assist users accessing the network, although this can become a challenge due to the variety of operating systems and platforms. The University of British Columbia, Faculty of Medicine2, which embraced the BYOD model, clearly states in their guidelines that students are responsible for repairing their own devices.

Researchers such as Alden (2013) believe that students are quite comfortable with using their devices, and can learn informally how to work them (Kukulska-Hulme, 2010). Alden (2013) feels, however, that students may occasionally need technical support to perform certain tasks such as downloading or using applications. A study by Ramsden (2005) on the use of Personal Digital Assistant (PDA) did raise concerns regarding IT support for students and faculty within the current supporting structure. The author suggests a supporting structure with an emphasis on a student-to-student network type.

**EQUITY**

The BYOD program may widen the digital divide. It has been argued that if students’ personal mobile devices become an institutional requirement in teaching and learning, then all students must have access to a device and a wireless network (Dede & Bjered, 2010; Traxler, 2010a). Beckmann and Martin (2013), for example, indicated that during the implementation of learning activities, the instructor unintentionally disadvantaged students who did own a mobile device. Therefore, institutions must ensure that not a single student is disadvantaged due to a lack of available technology (Cherwell Software, 2012). In this respect, Kinash, Brand and Mathew’s (2012) study indicated that in order to ensure all students could access a mobile technology, each was assigned to a loan scheme whereby an iPad was available for both university and home use. A further strategy to avoid equity issues is forwarded by LaMaster and Stager (2012):

> Those without phones teamed up with their neighbors. By the end of the period, all 27 students were working on their assignments collaboratively on personal devices. And they have done exactly what we educators always dream of: They assessed their learning needs and found the right tools to satisfy those needs without adult intervention. (p. 6)

Although mobile device ownership among students is widespread, not all can afford the latest technology, or devices may be less powerful compared to others’. As such, learning activities must be compatible with all mobile devices (Curtis, 2012). Schepman, Rodway, Beattie and Lambert (2012), for example, described a multi-platform solution as a necessary

---

1 [http://www.usf.edu/it/class-prep/wireless.aspx](http://www.usf.edu/it/class-prep/wireless.aspx)
2 [http://med.ubc.ca/files/2012/02/FoM-BYOD-Student-Guidelines.pdf](http://med.ubc.ca/files/2012/02/FoM-BYOD-Student-Guidelines.pdf)
condition for mobile learning. The authors noted that it is advantageous to use technology which enables mobile learning on hardware that students already own and which utilizes relatively generic software which can be tailored to different tasks. Johnson (2012), while referring to equity issues at school level, added:

When selecting library e-books, online databases, learning management systems, and e-textbooks, part of the criteria must be how accessible these materials are on a wide a range of operating systems. In a BYOD scenario, students might be bringing smartphones or tablets running Apple’s iOS or Android, netbooks running Windows or Linux… (p. 85)

Moreover, when planning outside class activities, instructors must be aware of any limitations that may raise inequity issues, such as students who do not have an available or sufficient data plan for their mobile devices (Nykvist, 2012).

Campbell et al. (2013) noted a further equity issue that may arise:

…if BYOD does not become established within higher education…Learners’ experiences of a sophisticated, agile, and personally responsive computing ecosystem reflecting their own growing powers of judgment and creativity, powers linked to their own developing identities, will be destructively absent from their experience of school…thus depriving both learners and teachers of the experiences they need in order to thrive in a truly complex world. (Para. 9)

BYOD AS DISRUPTION

Mobile devices are seen as offering opportunities to support teaching and learning but they can also disrupt lectures (Sharples, 2002; Fang, 2009). Research has shown that students’ mobile devices are often perceived as a source for distraction, cheating and inappropriate use of the technology (e.g. Tatar, Roschelle, Vahey, & Fenue, 2003; Sharples, 2002; Mueller, Wood, De Pasquale, & Criukshank, 2012; Geist, 2011). For example, Geist (2011) reported that many instructors considered mobile devices as a distraction during lectures, as students would not pay attention because they were often browsing the Internet or accessing social media. Burns and Lohenry (2010) further indicated that most of the faculty and students agreed that mobile phones in the classroom were a source of distraction. Mobile phones, in particular, are considered distracting because of problems with ringing, texting messaging, and/or multitasking (Fang, 2009).

While Scornavacca, Huff and Marshall (2009) found that students occasionally accessed social network during learning activities, the overall experience of using personal mobile devices in the class was positive. The study concluded that positive results can be achieved by encouraging students to bring their personal devices to class. In order to minimize disruptions, Sharples (2002) proposed that instructors could either attempt to prohibit the use of mobile technology in class or, alternatively, welcome those devices but in full knowledge that there will be disruptions which need to be managed.

Several authors have discussed strategies to alleviate distractions caused by mobile technology, ranging from implementing policies to etiquette (e.g. Burns & Lohenry, 2010). Bugeja (2007), for example, showed that some universities are relying on educational campaigns to make students more aware of classroom etiquette. Fang (2009) added that rather than seeing distraction as a challenge, instructors should see it as an opportunity to reflect upon and modify their instructional approach. Many instructors, however, may not know how to integrate these tools into their teaching. To make good use of mobile devices in the classroom, instructors need to understand their educational value (Naismith & Corlett, 2006) and how to integrate these tools into classroom teaching (Mueller, et al., 2012). In addition, institutions need to provide training to instructors on how to guide students in the proper use of mobile technology (Sangani, 2013). Fong (2009) went further to argue that both students and instructors should be provided with training on acceptable technology use. Burns and Lohenry (2010) concluded that educating students on mobile technology use in the classroom is paramount for its successful implementation.

CASE ILLUSTRATION

This section reviews a case study conducted by Santos (2013) at a higher education institution in the United Arab Emirates to illustrate the challenges discussed in the above sections. The study investigated the implementation of classroom quizzes supported by students’ personal mobile devices, as well as explored the implications of bringing those devices to the institution. The study participants consisted of 19 Emirati female undergraduate students enrolled in a 15-week educational technology course within the Bachelor of Education program. A staff member of the IT department also took part in the study. Multiple methods of data collection were adopted, and a commercial web browser response system (SMART response) was adopted and is compatible with multiple mobile devices to deliver quizzes.

Network infrastructure and security – results by Santos (2013) indicated that institutional network infrastructure could only support the number of students currently participating in the study. To effectively promote a BYOD program at the institution, the study concluded that there was a need to increase network capacity. This agrees with others who observed the need to update network infrastructure to accommodate a variety of mobile devices and to handle large amount of data transfer (Dede & Bjered, 2010; Cherwell Software, 2012). Santos (2013) also showed that to increase the network capacity to allow a high number of personal mobile devices, money needed to be spent. This reflects what others have discussed about costs involved in improving network infrastructure to accommodate the BYOD initiative (e.g. Campbell
et al., 2013), Santos (2013) also revealed concerns over network security. For example, to secure the institutional network Santos used a guest account to protect the network in case students participating in the study abused or shared the password with anyone not in the study. This was a temporary solution proposed by the IT department. Similar to strategies discussed above (e.g. CDW-G, 2012), to improve security Santos suggested a segregated network where students are required to register their devices. However, to enable a segregated network, there was a need to increase the bandwidth capacity to accommodate the devices, which in turn required financial investment (Santos, 2013).

Equity and IT support – study by Santos (2013) also reported concerns with equity issues. According to the results, although all students owned a mobile device, only a few had subscriptions to a local Internet service provider. In this study, students were provided with a wireless guest account to take part in mobile-based quizzes. It seems this action might have created two classes of users within the institution, in which one group had wireless access on mobile devices, while the other did not. In addition, the study suggested that only one group of students was benefiting from using advanced technologies to support learning. On a positive note, and in supporting others (Curtis, 2012) who indicated that learning activities must be cross-platform, Santos (2013) showed that a web browser response system enabled all students to access the quizzes. The only requirement was Internet access on students’ personal mobile devices.

The above review on IT support to personal mobile devices indicated mixed results with some arguing that IT support is needed while others believing students can support their own devices with little or no support. Santos (2013) revealed that students did not require IT support while taking part in quizzes. Only a few students had technical problems, mainly related to the password to access the wireless guest account. Agreeing with others (e.g. CDW-G, 2012), Santos (2013) suggests IT support for mobile devices can be complex due to the implementation of a variety of devices and operating systems. According to findings, IT support would be more related to provide Internet connectivity to students and distribution of applications to their mobile devices.

Disruption – Santos (2013) did not report disruptive issues caused by enabling students’ personal mobile devices in the classroom. As mentioned above, a few students had access to the Internet on their mobile devices. According to Santos, the guest account provided to the students required a password every time they wanted to access the wireless. Perhaps, the process of accessing the wireless that resembled a “hotel type experience” may have discouraged students to use their devices to access social media or other applications.

CONCLUDING REMARKS
This paper has discussed key challenges associated with bringing students’ personal mobile devices to the classroom. It is clear from the review that before embarking on a BYOD program, higher education institutions will need to consider carefully their network infrastructure and financial costs involved in accommodating a variety of personal mobile devices, which may consist of different models and operating systems. Without updating the network capacity, this may lead to equity issues in which not all students will have the same privilege of accessing or using mobile technology to support their learning within the classroom environment. In addition, lack of a robust network infrastructure may also interfere with implementation of learning activities as demonstrated by Nykvist (2012). This agrees with UNESCO’s (2013, p.35) observation that “Most mobile learning opportunities depend on reliable connectivity to the internet and other communication and data networks.” Institutional policy should also ensure that all students will have access to a device to be able to participate in organized learning activities. Activities should be compatible with all devices and measures, such as a loan system, to those students without access to a personal device.

Violino’s (2012, p. 41) recommendation to schools not to “… rush into a BYOD program without researching and addressing issues such as access controls, security and support” equally applies to higher education institutions. Pilot studies similar to Santos (2013) should be conducted to test the BYOD initiative and help advance understanding on how to deal with the challenges discussed in this paper and others that may emerge. Furthermore, pilot studies could include faculty that are more comfortable with using mobile devices in the classroom to experiment with the BYOD. Outcomes could be shared with other faculty, IT staff and others through workshops. The pilot may illustrate the development of strategies and written policies to deal with network security and disruptions caused by the use of personal devices in the classroom. However, developing policies may not be enough. Both faculty and students need to be educated with regard to network security practices. In addition, as observed by Geist (2011, p.806; 810), it is important to communicate policies regarding when and how to use personal devices in class. Geist found that “Students may be unaware that the use of cell phones affects teaching…Awareness fosters courtesy and professionalism necessary for optimal teaching and learning.”

The review suggested mixed results related to IT support for students’ personal mobile devices. Educational institutions should develop clear policies on how or whether they will provide support for personal mobile devices and make those policies available to students. Building on Ramsden’s (2005) ideas of creating a support structure based on students instead of relying on IT support, institutions could promote a student network supporting system based on mobile device models and operating systems. Alternatively, if practical, train and assign IT personnel to support major mobile device models or operating systems used at the institution. While Santos (2013) revealed that IT support was not required, more studies are needed to validate the results.
Outcomes of this review suggest potential strategies to help minimize the challenges associated with a BYOD model. More studies investigating these key challenges are recommended. Studies could, for example, include different groups of students, and focus on formal and informal learning.

REFERENCES


