La Salle University
La Salle University Digital Commons

Mathematics and Computer Science Capstones

Mathematics and Computer Science, Department of

Spring 5-18-2018

Security Management for Mobile Devices of Higher Education

Kala Battle
La Salle University, battlek1@student.lasalle.edu

Recommended Citation

Battle, Kala, "Security Management for Mobile Devices of Higher Education" (2018). *Mathematics and Computer Science Capstones*. 37.
https://digitalcommons.lasalle.edu/mathcompcapstones/37

Security Management for Mobile Devices of Higher Education

Kala P. Battle

LaSalle University

Table of Contents

Abstract

Mobile learning has made a major impact on the security of Learning Management Systems (LMS) in higher education. The advancements in mobile technology have made mobile learning one of the top trending topics regarding education and technology. Students appreciate the convenience and flexibility that mobile learning offers. However, there is an added concern with the security in mobile learning. Instructors and students have little say in what software will be used in mobile learning. This paper will address the issues surrounding security management in LMS platforms, the basics of the Family Educational Rights and Privacy Act (FERPA), and the best practices to improve security management in mobile communications of higher education.

Security Management for Mobile Devices of Higher Education

The Impact of Mobile Learning

Mobile learning is equated with any module of e-learning that is accessed on a mobile device. It provides students and teachers the ability to utilize portable computing devices while connected to local and wireless networks. Teaching and learning is extended to spaces beyond the traditional classroom with the utilization of mobile learning ("Mobile Learning", 2016). Learners and instructors have increased flexibility and opportunities for greater interaction ("Mobile Learning", 2016). Mobile learning offers students a convenient method to advance a new way of learning through mobile devices because content can be accessed whenever and wherever they want. ("Background of Mobile Learning or mLearning", 2014).

Over the past two decades, mobile learning has grown to become a great advantage to students in higher education. Dating back as far as the 1970s, mobile learning became a part of a very significant decade. Hardware and software were developed beginning with the pioneering work done by Xerox, by setting up a group named Dynabook. Dynabook was a device that served as a "personal dynamic medium" and was the size and shape of a one regular book (Berge, Muilenburg, & Crompton, 2013). Handheld devices, like PDAs, became more flexible, smaller and personalized and could be used in schools to help teachers to create tests and teach lesson plans. It was not until the early 2000s that the concept of mobile learning expanded with the introduction of tablets, which evolved into compact devices that served as mobile computers for students and teachers. "By the year 2005, more than 50% of public schools included laptops for students in their technology budget, and 90% of schools had access to the internet" ("Trusted ICT Support for schools & IT solutions for the education sector.", 2017). The creation of smartphones, tablets and laptops has provided a major opportunity for new experiences for students in education. Mobile learning has given students a another line of communication between each other and the teachers.

With mobile learning and portable devices being accessible to users at any time and any place, it is easier for learners to remain on track, and this can result in less college dropouts (Laskaris, 2015). It is estimated that the usage of mobile devices and applications by college students are greater than the usage in non-students, and that is about 79% of the students (Poll, 2014). According to Poll, 2014, only 83% of students regularly use a smartphone or tablet, and 51% use tablets daily which is an increase from 52% in the previous year. Educators make up about 74% of the support for students using technology, and this is due to teachers choosing to use mobile technology in their classes ("Trusted ICT Support for schools & IT solutions for the education sector.", 2017). "In fact, the "Alliance for Childhood" discusses how advancements in technology are progressing faster than adults can understand the ethical ramifications of its use" (Mattison, 2017). However, according to Wagner, 2016, of the 97% of schools having access to internet, about 95% of all incidents relating to security breaches in mobile learning are because of human error.

Security Breaches

Security Breaches, caused by vulnerabilities in the network, are also known security violations that can result in an unauthorized access to data, applications, networks, desktop and mobile devices or system services (Technopedia, 2017). Security breaches occur when an individual bypasses an underlying security mechanism and enters an unauthorized perimeter of IT (Technopedia, 2017). The user plays a critical component in the cybersecurity of mobile devices, whether it is intentional or accidental. According to IBM and the Cyber Security

Intelligence Index report, human error accounts for 52% of security breaches because they cannot be controlled or relied upon (Pham, 2014). As of 2017, about 24% of security breaches were caused by users carelessly sharing their computer login credentials, or not logging out of their computers at all (Ford, 2017). Not using password protection on mobile devices and computers can result in users becoming the victims of cyber theft – like remote exploitation.

The intent of remote exploitation is to cause damage to a user's computer or mobile device by putting malware on the device or network to steal personal information. In remote exploitation, the hacker sends the device content such as an email or text message, and this will then send a flaw such as a buffer overflow. The remote attack will not affect the attacker's device, but it will find points of vulnerability in the device or network. The points of vulnerability can provide the hacker with full control of the mobile device or computer, and this can be a security concern for many students. If a hacker gains full control of a student's mobile device or computer, all personal information can be sent to the hacker's computer. Remote Exploitation is not the only option for cyber-attackers to gain access to student information.

Even the most sophisticated computer systems are not impenetrable, and recent cyber-attacks have proven that higher education institutions are not an exception. (Harrie & Hammargren 2016). Mobile devices and software have made security breaches and identity theft a common occurrence; especially amongst the larger colleges and universities ("A University Security Audit for 2015", 2015). According to Ford (2017), 63% of breaches can be attributed to the use of weak or stolen passwords. In a 2015 university security audit, it was found that about 80,000 students were affected by a security breach or identity theft at state colleges in California, and 48 colleges were found with more than 1,000 public-facing IP addresses ("A University Security Audit for 2015", 2015). The convenience of students having the visibility to see other students' personal information has become a major concern because mobile devices have become more accessible to features including internet capabilities and applications. This can cause the cost of cyber security controls to be expensive.

Breaches in the network can be detrimental to sensitive data in many computer systems and mobile devices. According to the 2015 "*Cost of Data Breach Study: Global Overview*", most of the contributing factors for a high cost per stolen record in the U.S. are because of high regulation and time. "Malicious attacks can take an average of 256 days to identify while data breaches caused by human error take an average of 158 days to identify" ("2015 Cost of Data Breach Study: Global Overview", 2015). Therefore, if a security breach is detected in less than 100 days, the cost of the security control remains at a manageable dollar amount. However, if the detection is greater than 100 days, then the average cost rises. While there is an understanding in the value of cost and protection against human error in mobile security, security breaches can also occur in Learning Management Systems (LMS).

Security in Learning Management Systems

Vulnerabilities in LMS platforms can have extreme consequences that can affect an educational institution and its reputation. Accessibility is a prime example of a major vulnerability for LMS platforms because there is a lack of security in the privacy of student information. Since some of the mobile learning platforms are available to the public, there is a chance that anyone can access private student information (Bourgeois & Bourgeois, 2014). Mobile learning platforms are more likely to be susceptible to a cyber-attack. This could be a reason why many Universities have stopped using Massive Open Online Courses (MOOCs).

Massive Open Online Courses (MOOCs) are a cloud-based education technology that can be accessed on the internet (Young, 2015). A MOOC is a virtual classroom that performs the same functions as the ones used in traditional education systems, and it is an inexpensive platform for students. The discussion of privacy regarding students using MOOCs has been a debatable topic due to students often submitting personal information like birth dates in discussion boards, and this information is not protected. Because the data stored in MOOCs is not protected, providers have an easy and open access to that information. This can raise a security concern for many students because MOOCs have the function to collect large amounts of data including student records and performance (Young, 2015).

Big Data is data content that stores massive amounts of information to be kept for analysis regarding trends. Big Data raises a privacy concern because it is “shorthand for the ability to store so much information that even trivial details can be kept and analyzed for trends in areas such as consumer preferences, economic development, and crime mapping” (Young, 2015). The most common issue of Big Data is the exploitation of Personally Identifiable Information (PII). Big Data can excel at revealing the correlations of someone’s identity, potentially creating a new “fact” about the individual without confirmation (Young, 2015).

The data in MOOCs is not always protected by the Family Educational Rights and Privacy Act (FERPA). This is due to MOOCs not being funded under federal student aid. Big Data is also not covered under FERPA because the statute of the law can break down and cause a breach in the system when confronted with technology that can collect and use this type of data (Young, 2015). This would mean that students are unable to knowingly consent to the terms of what personal information would be collected for a service because the future of the information used is not detailed at the time of the collection (Young, 2015). Therefore, if there is a breach in the system, this can cause private information collections to be linked and analyzed. “MOOCs managed to defy categorization under FERPA and provided a bigger picture of the disadvantages that arise when existing privacy legislation attempts to regulate a technology that does not clearly fit into the statute's domain" (Young, 2015).

Blackboard is a platform used by professors and students to obtain and post work assignments. According to Pauli, 2011, Blackboard Learn was discovered to have several "zero-day security vulnerabilities". This means programmers have zero days to address an attack before it is exploited after learning about it. According to Schultz 2012, staff and students who worked at the University of Texas Brownsville admitted to using admin access to steal exams through the university Blackboard system in 2008. It was also reported that a student compromised the personal data of over 500 students and staff members by causing a breach in the Blackboard system at Baylor University (Schultz 2012). Although Blackboard is rated number five on the top 10 favorite technologies used in 2017 (Kelly, 2017), many universities – like La Salle University and Community College of Philadelphia – have transitioned from using Blackboard to using Canvas

Canvas is a leading LMS platform that has made teaching and learning more efficient and easy. Canvas provides notifications on student coursework, and provides instructors the option to choose which Canvas tools they would like to use during the duration of the courses. Although Canvas is a cloud-based platform, it is difficult to hack the system because it is easy to deploy security fixes almost immediately. In November 2014, Instructure paid Bugcrowd $10,000 to find security flaws in their system. In the vulnerability assessment, Canvas by Instructure yielded 59 validated bugs (Locke, 2015). Out of the 59 unique bugs found, about 33 of them were ranked with a severity of a 2 or lower (Locke, 2015). This would have caused an exploitation in student information and privilege escalation. Researchers from Bugcrowd informed the engineering team about the bugs, and Instructure immediately addressed the security flaws. Then, in 2015, the same vulnerability assessment was conducted again, and only 10 validated bugs were found, none of which were deemed critical because they had all been resolved within 24 hours (Locke, 2015). Because of Instructure's success, Canvas has been replaced by Blackboard in more than 1600 educational institutions, ("Global Study from Canvas Ranks Teachers' Concerns and Attitudes on Technology in the Classroom", 2016). Unlike MOOCs, Canvas is covered under FERPA, but there is still a growing concern from students about the privacy of their personal information.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a privacy law that was enacted by Congress to protect the privacy of students and parents (Easterly, 2015). FERPA was created to ensure educational records could be accessed by students. The FERPA law applies to any state or agency, higher educational institutions, universities and schools ranging from preschool to 12th grade ("Parents' Guide to the Family Educational Rights and Privacy Act: Rights Regarding Children's Education Records", 2007). According to Easterly (2015), federally funded institutions that are administered by the U.S. Department of Education – like universities and colleges – must comply with certain procedures regarding disclosing and maintain educational records. FERPA was provisioned to provide students with ownership of their own educational records and personal data because schools were only mere custodians of that information.

In colleges and universities, the privacy rights of FERPA are assigned to students who are 18 years of age or older. Therefore, if the students were not attending school, they would be a part of the working class (Ramirez, 2009). FERPA includes the protection of student report cards, grades, transcripts, disciplinary records, contact and family information as well as class schedules (“Protecting the Privacy of Student Education Records”, 1997). The FERPA law does not cover medical records, but it allows parents the right to view their children’s educational records. Schools are required to send parents and eligible students notifications annually regarding their rights under FERPA, and students or parents can request to have changes implemented based on a limited number of circumstances. When a student turns 18, schools are not obligated to provide student information to the parent unless (“FERPA for Parents”, 2015):

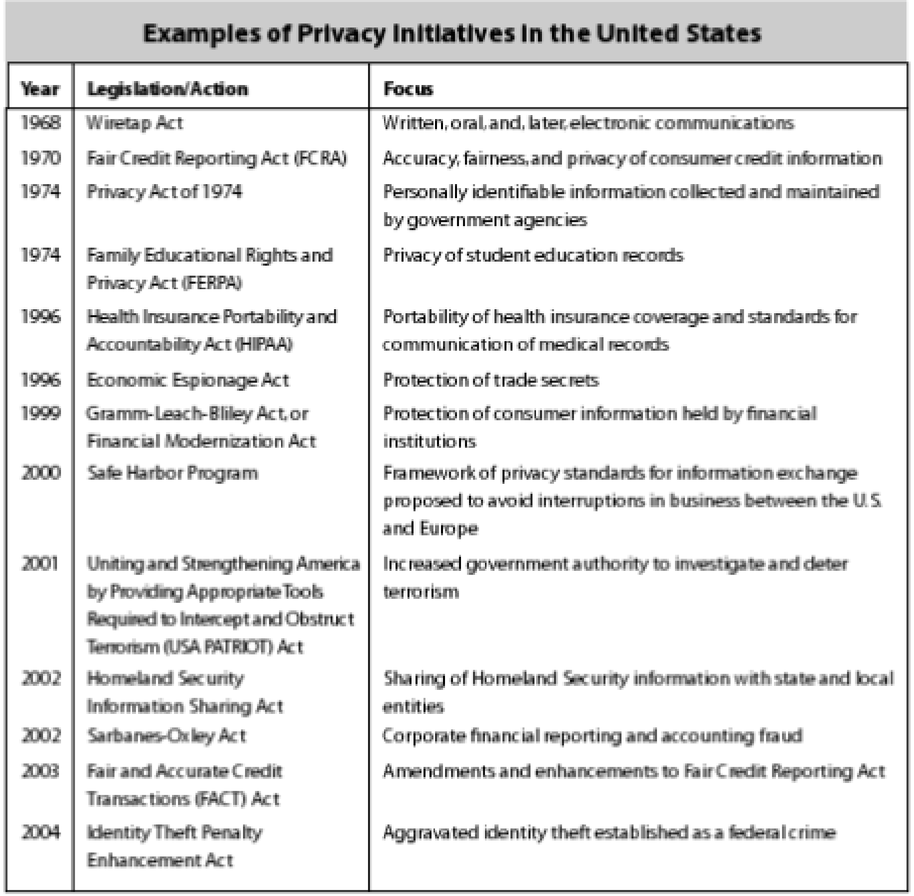
- The student is claimed as a dependent for tax reasons (i.e, the student is in school/college). Only then can schools provide student educational records to the parents.
- If there is a health emergency, schools can provide the parent with educational records of the student.
- If the student is under the age of 21 and he or she has violated any policy or law.

FERPA allows teachers and federal officials the permission to utilize student information to gain an understanding of the achievements of the student, but they are not allowed to use that information in making decisions (“FERPA for Parents”, 2015). According to the U.S. Department of Education, 2015, schools are required to retrieve written permission from the parent or students, who are over the age of 18, if they need to release any information from the student’s educational record. In addition, schools must inform parents and students about directory information, (i.e., student’s name, address, telephone or date of birth) that has been disclosed. Schools must provide the parents and students adequate time to request the student’s information not be released (“FERPA for Parents”, 2015).

Under FERPA, there are many educational institutions that use protected online systems to give students and parents the access to class materials or educational records. This includes school websites that require password and user IDs (“Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices”, 2014). About 95% of school districts send student records to companies like Google and Microsoft to help control the management of their school services (Nava, 2015). Out of that percentage, 7% of the school districts signed contracts that will prevent the selling of student data, but this does not include Metadata (Nava, 2015).

While FERPA provides protection for the confidentiality of a student's educational record, it is the responsibility of the Family Policy Compliance Office (FPCO) to enforce the law. FPCO works with educational institutions, parents, students and other local departments of education. All communication between the office and schools should include basic information such as, name and contact information, name of the school and location of school because it affects the response from the FPCO ("Parents' Guide to the Family Educational Rights and Privacy Act: Rights Regarding Children's Education Records", 2007). FPCO has the responsibility to maintain any information regarding the FERPA law received on the website for the Department of Education. This includes proper communication provided to parents and students in a timely manner. It is under the authority of the FPCO to respond to any complaints filed by the parents or students regarding violations under the FERPA law and mediate those complaints with a response that will assure parents of the compliance with FERPA ("FERPA for Parents", 2015).

Since the implementation of FERPA, there have been Amendments to the law over the years following the practices in educational applications (Ramirez, 2009). Refer to list of examples regarding Privacy Initiatives in the United States Below.



Examples of Privacy Initiatives in the United States

Year	Legislation/Action	Focus
1968	Wiretap Act	Written, oral, and, later, electronic communications
1970	Fair Credit Reporting Act (FCRA)	Accuracy, fairness, and privacy of consumer credit information
1974	Privacy Act of 1974	Personally identifiable information collected and maintained by government agencies
1974	Family Educational Rights and Privacy Act (FERPA)	Privacy of student education records
1996	Health Insurance Portability and Accountability Act (HIPAA)	Portability of health insurance coverage and standards for communication of medical records
1996	Economic Espionage Act	Protection of trade secrets
1999	Gramm-Leach-Bliley Act, or Financial Modernization Act	Protection of consumer information held by financial institutions
2000	Safe Harbor Program	Framework of privacy standards for information exchange proposed to avoid interruptions in business between the U.S. and Europe
2001	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act	Increased government authority to investigate and deter terrorism
2002	Homeland Security Information Sharing Act	Sharing of Homeland Security information with state and local entities
2002	Sarbanes-Oxley Act	Corporate financial reporting and accounting fraud
2003	Fair and Accurate Credit Transactions (FACT) Act	Amendments and enhancements to Fair Credit Reporting Act
2004	Identity Theft Penalty Enhancement Act	Aggravated identity theft established as a federal crime

Recent research studies have made mention that the practices in educational applications in relation to laws and disclosures for privacy show a lack of transparency. The lack of transparency is due to the privacy policies of applications. In a 2016 interview survey, it was found that schools issued devices to students without the knowledge and consent of the parents (Gebhart, 2017). This keeps parents in the dark about what data is being collected by the schools. There is a lack of usability for students, and as a result, online learning systems do not provide the necessary rights of control to enable protection on mobile devices (Bourgeois &Bourgeois, 2014). “Since 2015, the Electronic Frontier Foundation (EFF) has been taking a closer look at whether and how educational technology (or “ed tech”) companies are protecting students’ privacy and their data” (Gebhart, 2015). That lack of transparency in privacy policies can cause providers of online learning to make mistakes in offering students the protection they need most. However, the implementation of legislative measures – like FERPA – are not enough to suppress the security and privacy concerns.

The future of information security in mobile learning

Best Practices in mobile learning, security and mobile devices

The need to provide proper security for mobile learning and mobile devices should never be underestimated. Mobile devices are often thought of as not being the most secure means of storing personal data. This has been the primary concern for IT departments because of the malicious software that can specifically target mobile devices and tablets. The average number for app downloads completed by a user can be over 100, but once a smartphone app is infected with malware or a virus, it is easy for personal information to be stolen by a hacker (Ivec, 2015). Therefore, it is important for students and teachers to educate themselves on the importance of using the best practices to properly protect mobile content.

Bring Your Own Device (BYOD) policies are becoming increasingly popular for many educational institutions, and they are striving to remove the dividing line between work and play. BYOD allows students and teachers to use their mobile devices for educational use, which gives them instant access to a variety of educational apps (Campbell, 2017). BYOD is a mere effort to better utilize resources and cut costs for many educational institutions because the devices are already owned by the students and teachers (Siddiqui, 2014). BYOD allows educational institutions to spend more money on improving their network infrastructure and security systems to better accommodate students' and teachers' mobile devices (Keengwe, 2015). BYOD is supposed to improve student experience by using the internet, and students expect schools to be more supportive of BYOD programs since mobile technologies are already used for work and play.

Colleges and universities need to implement BYOD policies that will address support for mobile devices and offer provisions for institutional liability (DiFilipo, 2013). Many Universities and colleges – like the University of Georgia – have put a BYOD policy in place that details the expectations and the need for security precautions with the user who may be signing in or taking a quiz on an LMS platform. Universities and colleges should be formalizing BYOD by implementing policies – like acceptable use, security requirements for data and devices, employee privacy and liability of devices or services – to prevent private information from being exposed. According to Negrea (2015), without rules for BYOD, mobile devices can be brought on campus undetected. For some policies, it is required for students to register their mobile devices with the school. Other BYOD policies will only allow university-issued devices access to private student information (Negrea, 2015). According to Rayome (2017), collegiate IT staff need to understand where key data is located and ensure protections are in place – like two-factor authentication – for those who use the data.

Running LMS platforms can be risky for educational institutions because they usually carry a lot of users on one network. A great way to mitigate and reduce the risks of a user compromise is through 2-factor authentication. 2-factor authentication is a two-step verification method that requires a username, password and an extra piece of information that only the user knows – like a physical token or a 4 to 6-digit code (“What Is 2FA?”, 2018). In 2011, Google introduced the use of 2-factor authentication for their users, and shortly after, MSN and Yahoo followed behind with their introduction of 2-factor authentication (“What Is 2FA?, 2018). Educational institutions should be encouraging teachers and students to enable 2-factor authentication on their mobile devices because it can reduce the chances of a hacker accessing their personal information. One of the downsides to 2-factor authentication is that new hardware tokens need to be ordered and issued, which can cause delayed problems for the user because the tokens can easily be lost (“What Is 2FA?, 2018). However, this security process can help lower the number of incidents regarding identity thefts on the network.

Mobile Device Management (MDM) tools are another great way that can help educational institutions cut the risks of cyber-attacks in mobile learning. MDM is a type of software system that is used for mobile security to monitor, manage and secure a user’s mobile device (“Everything You Need to know about MDM, 2018). MDM is available for multiple providers and operating systems – like DaVita, INC. and Apple. One of the biggest downfalls in protecting personal information and mobile devices is the user. Mobile device users put a high value on personal data stored on their phones, but do not think about the risks behind information being accessed by someone other than themselves. MDM tools can be used to either protect data or wipe content from mobile devices if it has been lost or stolen – like PIN/password protection or control app distribution. For instance, DaVita, Inc. uses a tool called AirWatch, a MDM tool that lets users activate their mobile devices and tablets in a single step without needing an iTunes account or other generic software. Teammates at DaVita are required to submit an access request through our Teammate Self-Service tool to gain access to use AirWatch. Once the teammate is enrolled into AirWatch, the company can make changes to the environment. IT departments can maintain compliance and monitor the device through the admin console application for AirWatch. If the mobile device is stolen or lost, automated responses can be sent to administrators. The device can be locked down so that no one is able to utilize any of the device features or access any personal information. Some other functionalities of AirWatch include (Hein, 2012):

- The ability to update each device configuration profiles. This can be for the entire group or the enterprise.

- Send a request for information to the device, lock the device or wipe off all data remotely, if needed.
- If the device is being retired, a user can un-enroll the device by using the Admin console or deleting the MDM profile through their settings app depending on the type of device.
- Finally, queries can be created and customized, and those queries can be used to report device information to users or administrators.

Mobile devices can be found on most college campuses today. Some universities – like St. Edward's University – use MDM to help protect the information stored on mobile devices (Wong, 2014). Depending on the type of information students and teachers are putting on mobile devices, other Universities may want to consider MDM as an option. According to Wong (2014), MDM enables central configuration, monitoring and security as well as efficient management of sensitive data. MDM enables collegiate IT departments to enforce password policies, sync users to email, and configure devices to connect to the WIFI (Wong, 2014). Collegiate IT staff can effectively manage mobile devices regardless of the operating system or type of device (Mourning, 2015). This makes the learning experience better for students because they will feel safe using their personal devices on college campuses. MDM tools can help organizations – like universities and colleges – decrease the exposure to vulnerabilities that can compromise private information. Without the use of MDM tools, confidential data can be at risk for a cyber- attack, and the ease of achievement for data breaches can greatly increase.

With the evolution of mobile technologies, mobile devices have managed to transform the way students process information and access the internet. However, there is an ever-growing shift in the nature of security threats. The number of ways to enhance the convenience of mobility and security within mobile devices are increasing. Lawmakers are enforcing stricter security measures through regulation, and advanced security software are being pushed out to users to respond to the number of security threats ("What is the Future of Mobile Security", 2018). There is a belief that the next generation of mobile security will consist of characteristics that can contribute to the upgrade in security. These characteristics include (Goode, 2016):

Focus on user- The user should be at the center of the design for mobile security. This ensures that the user's experience is consistent with any mobile device used. Security applications should be easily accessible, and ease-of-use should be implemented to lessen the burden on the user's experience.

Agile Multi-Factor Authentication – Authentication methods should be used and implemented in the design process. The idea of a strong multi-factor authentication has become widely expected by users and organizations due to the "result of industry regulation and vulnerable legacy authentication mechanisms such as passwords" (Goode, 2016). Apple has already managed to implement fingerprint scanning into the iPhone. Apple has since changed the home button to only use fingerprint scanning as well as facial recognition for the iPhone X.

Mobile Single-Sign-On (SSO) – The support for Single Sign-On (SSO) is essential for modern institutions and enterprises because it is more convenient. Although this can be a downfall in mobile security due to a stolen or loss device being tampered with, most users believe it will allow them more time to complete what they need to without requiring authentication.

Simplified Unified Security – The next generation of mobile security needs to implement a more simplified approach to managing a variety of security features. Taking steps toward this type of approach means meeting the needs of convenience in mobile security, and it will avoid the major problems businesses and schools face. "Next generation mobile security solutions need to provide a simple, unified, solution to enable an enterprise to take control of both their BYOD and enterprise-owned mobile fleet" (Goode, 2016).

Mobile learning has grown to dominate the generation of traditional classrooms because of the advancements in wearable technology. Wearable technology – like the iWatch, has gained major popularity amongst users, and they are only a mere extension of the mobile phone. Smart watches have changed how students learn because they have the option to find expert advice through utilizing text messaging when they have a question either by phone or on a smartwatch (“What to Expect for the Future of Mobile Learning”, 2018). Smart watches have become more user friendly, and each time operating systems are updated, there is a new function available. According to recent research from CCS insights, it is projected that “wearable technology will be worth $25 billion by 2019, with smartwatches commanding a 60% share of the market” (“The Future of Wearable Technology”, 2018). Manufacturers are now wanting to design tether-free smartwatches. Tether-free smartwatches will have the capability to perform similar tasks that smartphones do without the need to pair them together (“The Future of Wearable Technology”, 2018). Smartwatches will enhance the communication between the student and the teacher, and it will help students to monitor their own learning experiences (Lynch, 2017). This could also include future advancements in LMS platforms.

LMS platforms of the future will become more hands-on, all-access tools for mobile learning (Lynch, 2018). Institutions will no longer have to purchase the same LMS products because they will be designed to meet the needs of each individual institution. According to Lynch (2018), LMS of the future will be designed for multiple uses – like homework help, purchasing, communication and more. LMS is expected to use more cloud-like functionalities so educators will be able to store information and access it for later use outside of the classroom

(Lynch 2018). Instead of communicating through general discussion boards, students will be able to communicate with each other and instructors through chat rooms and social media. In addition, LMS will be optimized for easy viewing and functionality (Lynch, 2018). For example, Blackboard and Canvas recently introduced Ally, an accessibility tracker that provides instructors guidance on how to check and correct common accessibility issues in class materials to make them more accessible ("Blackboard Ally Helps Make Course Content More Accessible for Students", 2017). The future of LMS will no longer be limited to desktops, and the advancements in LMS platforms will continue to provide a better learning experience for students.

Conclusion

Mobile learning offers the chance to provide an engagement of creative learning experiences for the student as well as the teacher. Mobile learning allows more insight on the idea of how students learn in the classroom and the mobile world. However, there is a need to promote security awareness in mobile learning especially amongst learners in higher education. Students and teachers should be aware of the security risks in mobile learning, and should be using their best efforts to protect their personal information. Using simple prevention measures – like pin/password protection, Mobile Device Management (MDM) and 2-factor authentication – can help improve mobile learning and create a better learning experience for the student. Privacy laws like – The Family Educational Rights and Privacy Act (FERPA) – can be complex, but it was created with a purpose to protect the rights of students in education. Educational institutions should be putting forth their best efforts to protect the rights provided to eligible students under FERPA and to avoid any possible breach of privacy in student information. Ignoring the misuse in mobile security and privacy may not result in the best opportunities for students, but approaching them head on can prevent a collapse in mobile learning for the future.

References

Alan Goode Managing Director, Goode Intelligence. (2016, August 02). Next generation enterprise mobile security needs to be simple. Retrieved November 18, 2017, from https://www.infosecurity-magazine.com/opinions/the-future-of-mobile-security/

Background of Mobile Learning or mLearning. (2014, July 15). Retrieved March 31, 2018, from https://sybrant.wordpress.com/2012/04/19/background-of-mobile-learning/

Berge, Z. L., Muilenburg, L. Y., & Crompton, H. (2013). *Handbook of mobile learning*. New York: Routledge**.**

Blackboard Ally Helps Make Course Content More Accessible for Students. (2017, May 18). Retrieved April 22, 2018, from http://press.blackboard.com/2017-05-18-Blackboard-Ally-Helps-Make-Course-Content-More-Accessible-for-Students

Bourgeois, D., & Bourgeois, D. T. (2014). *INFORMATION SYSTEMS FOR BUSINESS AND BEYOND*. S.l.: LULU. COM.

Campbell, A. (2017, March 22). To BYOD or not to BYOD... Retrieved April 14, 2018, from https://www.texthelp.com/en-us/company/education-blog/march-2017/to-byod-or-not-to-byod/

Cohn, C. (2016, July 9). How-and Why-We Can Improve the Future of Mobile Learning - EdSurge News. Retrieved April 09, 2018, from https://www.edsurge.com/news/2016-07-09-how-and-why-we-can-improve-the-future-of-mobile-learning

DiFilipo, Stephen. “The Policy of BYOD: Considerations for Higher Education.” *EDUCAUSE Review*, er.educause.edu/articles/2013/4/the-policy-of-byod-considerations-for-higher-education.

Easterly, E. J. (2015, April 1). FERPA Primer: The Basics and Beyond. Retrieved April 22, 2018, from http://www.naceweb.org/public-policy-and-legal/legal-issues/ferpa-primer-the-basics-and-beyond/

EDUCAUSE. (n.d.). Retrieved March 31, 2018, from https://library.educause.edu/topics/teaching-and-learning/mobile-learning.

Everything You Need to Know about Mobile Device Management (MDM). (n.d.). Retrieved April 08, 2018, from https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm

FERPA for Parents. (2015, June 26). Retrieved April 08, 2018, from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html

Ford, N. (2016, September 27). 63% of data breaches involve weak, default or stolen passwords. Retrieved March 31, 2018, from https://www.itgovernance.co.uk/blog/63-of-data-breaches-involve-weak-default-or-stolen-passwords/

Gebhart, G. (2017, April 13). Spying on Students: School-Issued Devices and Student Privacy. Retrieved April 08, 2018, from https://www.eff.org/wp/school-issued-devices-and-student-privacy

Global Study from Canvas Ranks Teachers' Concerns and Attitudes on Technology in the Classroom. (2016, January 26). Retrieved April 06, 2018, from https://www.canvaslms.com/news/pr/global-study-from-canvas-ranks-teachers-concerns-and-attitudes-on-technology-in-the-classroom&122586

Hein, R. (2012, July 11). 7 Reasons to Use AirWatch for Mobile Device Management. Retrieved April 14, 2018, from https://www.cio.com/article/2394249/mobile/7-reasons-to-use-airwatch-for-mobile-device-management.html

High Level Security Assessment of the Canvas and Moodle Learning Management Systems.

(n.d.). 1-4. Retrieved March 31, 2018, from https://it.umn.edu/sites/it.umn.edu/files/security_analysis_-_moodle_and_canvas_.pdf.

Ivec, S. (2015, March 04). Mobile Learning Lockdown: Is Your Data Secure? Retrieved April 08, 2018, from https://elearningindustry.com/mobile-learning-lockdown-data-secure

Keengwe, J. (2015). *Promoting active learning through the integration of mobile and ubiquitous technologies*. Hershey PA, USA: Information Science Reference, an imprint of IGI Global.

Kelly, R. (2017, October 16). 2017 Readers' Choice Awards. Retrieved April 14, 2018, from https://campustechnology.com/articles/2017/10/16/2017-readers-choice-awards.aspx

Laskaris, John, 7 Awesome Advantages of Mobile Learning. (2017, June 09). Retrieved March 31, 2018, from https://www.talentlms.com/blog/7-awesome-mlearning-benefits/

Locke, C. (2018, March 13). Hack This System! Instructure's Security Challenge to Hackers - EdSurge News. Retrieved April 06, 2018, from https://www.edsurge.com/news/2015-03-03-hack-this-system-instructure-s-security-challenge-to-hackers

Lynch, M. (2017, June 13). Five Ways to Leverage Wearable Technology in the Classroom. Retrieved April 8, 2018, from http://www.bing.com/cr?IG=10D9557FFE8D412F88E9FB5DD46FF253&CID=27748E7C62AC62B4333C85B763036318&rd=1&h=jfpoq4s_XKZvIXxOGcmaLDjS6O4wQ2Xv6VR7CMRNEF0&v=1&r=http://www.thetechedvocate.org/five-ways-leverage-wearable-technology-classroom/&p=DevEx,5072.1

Lynch, M. (2018, February 18). What Will the LMS of the Future Look Like? Retrieved April 22, 2018, from http://www.thetechedvocate.org/will-lms-future-look-like/

Mattison, L. (2017, January). Ethical Issues with Using Technology in the Classroom. Retrieved March 31, 2018, from https://study.com/blog/ethical-issues-with-using-technology-in-the-classroom.html

McQuiggan, S., Kosturko, L., McQuiggan, J., & Sabourin, J. (2015). *Mobile Learning: A Handbook for Developers, Educators, and Learners*. Hoboken, NJ: John Wiley & Sons.

Mourning, Jillian. "How MDM Can Improve Your Wi-Fi Efficiency and The Student Experience." *WiFi as a Service - Managed WiFi Subscriptions - SecurEdge Networks*, 28 Oct. 2015, www.securedgenetworks.com/blog/how-mdm-can-improve-your-wi-fi-efficiency-and-the-student-experience.

Nava, V. (2015, June 30). Protect Students from Corporate Data-Mining in the Classroom. Retrieved November 18, 2017, from http://www.nationalreview.com/article/420506/protect-students-corporate-data-mining-classroom-victor-nava

Negrea, Sherrie. "BYOD Boundaries on Campus." *University Business Magazine*, 26 Mar. 2015, www.universitybusiness.com/article/byod-boundaries-campus.

Parents' Guide to the Family Educational Rights and Privacy Act: Rights Regarding Children�s Education Records - FPCO. (2015, June 26). Retrieved April 08, 2018, from https://www2.ed.gov/policy/gen/guid/fpco/brochures/parents.html

Pham, T. (2014, June). Human Error Accounts for Over 95% of Security Incidents, Reports IBM. Retrieved March 31, 2018, from https://duo.com/blog/human-error-accountsforover95percent-of-security-incidents-reports-ibm

Protecting the Privacy of Student Education Records. (1997, March). Retrieved April 08, 2018, from https://nces.ed.gov/pubs97/web/97859.asp

Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. (2014, February). Retrieved April 8, 2018, from https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

Raj, Rishi. “BYOD- Bring Your Own Device- Advantages and Disadvantages in Education.” *MagicBox*, 23 Feb. 2018, www.getmagicbox.com/bring-your-own-devices-byod-pros-cons-schools-students/.

Ramirez, C. A. (2009). *Ferpa clear and simple: the college professional's guide to compliance*. Retrieved from http://dbproxy.lasalle.edu:6091

Rayome, Alison DeNisco. “Why Universities Must Adapt to Always-on Students and Support BYOD Policies.” *TechRepublic*, 11 Oct. 2017, www.techrepublic.com/article/why-universities-must-adapt-to-always-on-students-and-support-byod-policies/.

Schultz, C. (2012). Information security trends and issues in the moodle E-learning platform: An ethnographic content analysis. *Journal of Information Systems Education, 23*(4), 359.

Siddiqui, Rahat. (2014). Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS). 3. 233-236.

The 10 Best & Worst College & University Security Rankings. (n.d.). Retrieved March 31, 2018, from https://securityscorecard.com/blog/10-best-worst-university-security

Trusted ICT Support for schools & IT solutions for the education sector. (n.d.). Retrieved March 31, 2018, from http://www.ourict.co.uk/technology-education-history/

Wagner, M. (2017, September 21). 95% of All Security Incidents Involve Human Error - Insider Threat. Retrieved March 31, 2018, from https://edwps.com/cyber-the-insider-threat-by-mellisa-wagner/

What is a Security Breach? - Definition from Techopedia. (n.d.). Retrieved March 31, 2018, from https://www.techopedia.com/definition/29060/security-breach

What is the Future of Mobile Security? (n.d.). Retrieved April 08, 2018, from https://www.ecpi.edu/blog/what-is-the-future-of-mobile-security

What is 2FA? (n.d.). Retrieved April 08, 2018, from https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm

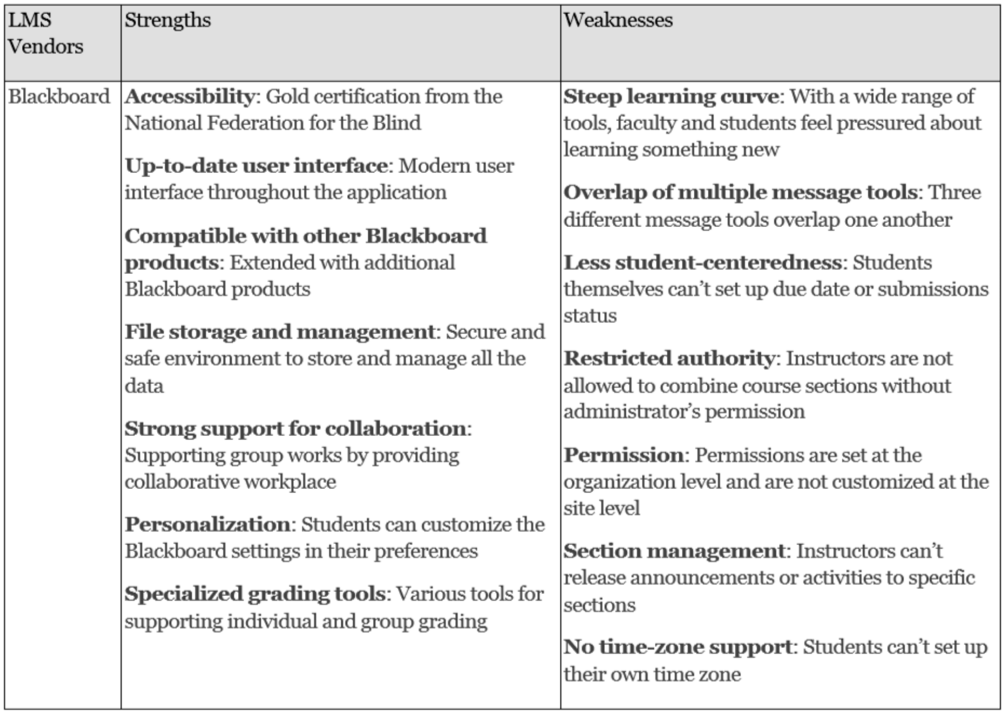
Wong, Wylie. “MDM: The Security Software That Lets Mobile Flourish on Campus.” *Technology Solutions That Drive Education*, 3 Feb. 2014, edtechmagazine.com/higher/article/2014/02/mdm-security-software-lets-mobile-flourish-campus.

Young, Elise (2015 March 03). "Educational privacy in the online classroom: FERPA, MOOCS, and the big data conundrum". *Harvard journal of law & technology* (0897-3393), 28 (2), p. 549.

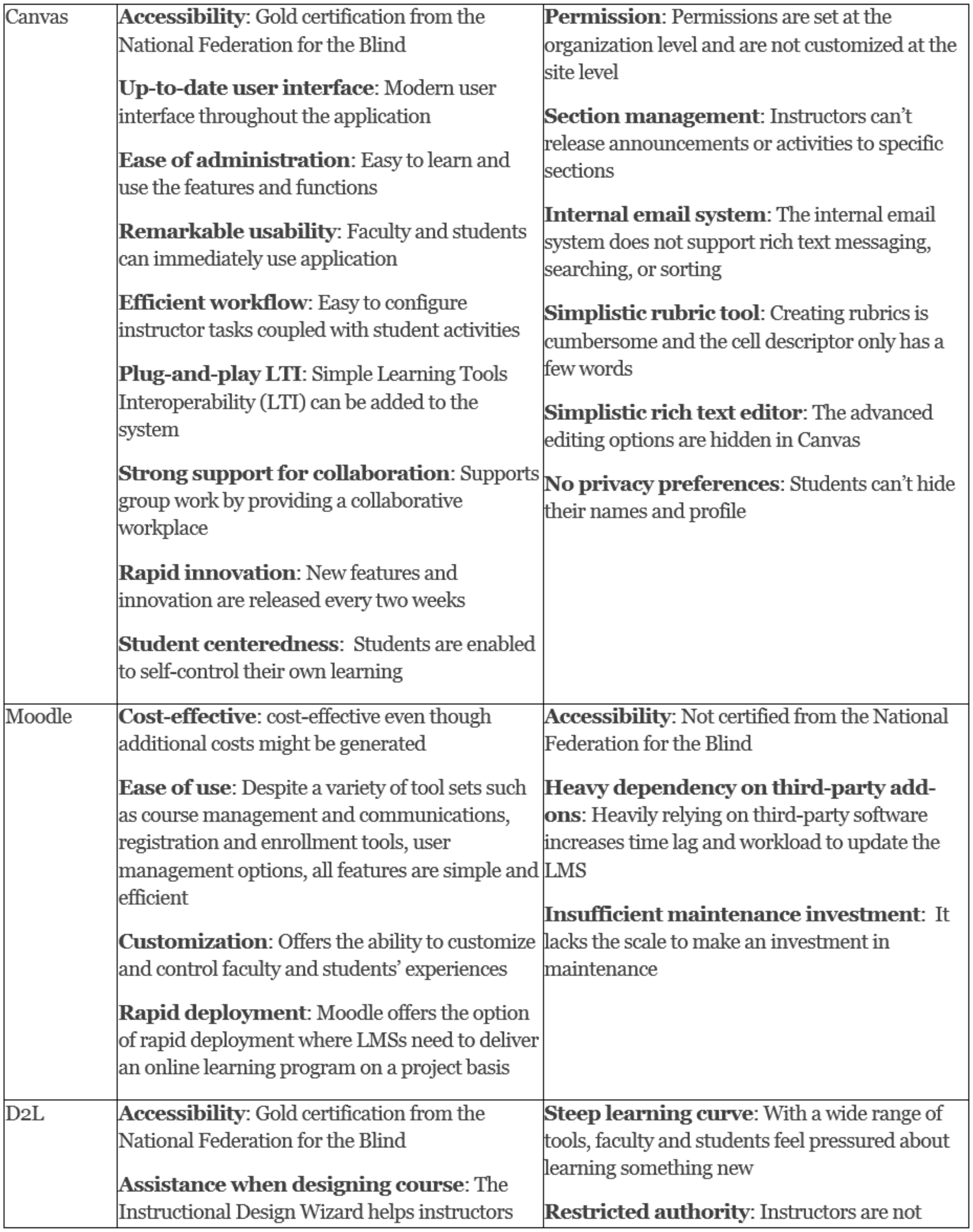
9 Ways You Should Be Repurposing Content to Grow Your Audience, Fast! (2018, February 07). Retrieved April 08, 2018, from https://www.kevcharlie.com/9-ways-repurpose-content-reach-larger-audience-less-time/

Table 1 – LMS Strengths & Weaknesses

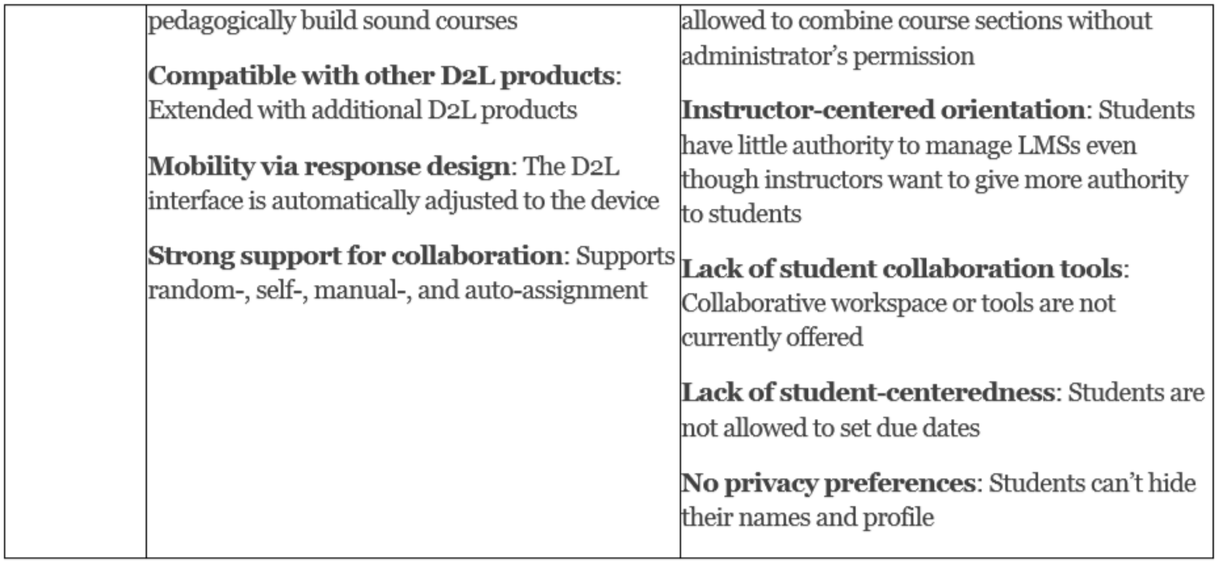
This chart displays the strengths and weaknesses of LMS platforms. The more common weaknesses displayed are permission, restriction and privacy.



LMS Vendors	Strengths	Weaknesses
Blackboard	**Accessibility**: Gold certification from the National Federation for the Blind **Up-to-date user interface**: Modern user interface throughout the application **Compatible with other Blackboard products**: Extended with additional Blackboard products **File storage and management**: Secure and safe environment to store and manage all the data **Strong support for collaboration**: Supporting group works by providing collaborative workplace **Personalization**: Students can customize the Blackboard settings in their preferences **Specialized grading tools**: Various tools for supporting individual and group grading	**Steep learning curve**: With a wide range of tools, faculty and students feel pressured about learning something new **Overlap of multiple message tools**: Three different message tools overlap one another **Less student-centeredness**: Students themselves can't set up due date or submissions status **Restricted authority**: Instructors are not allowed to combine course sections without administrator's permission **Permission**: Permissions are set at the organization level and are not customized at the site level **Section management**: Instructors can't release announcements or activities to specific sections **No time-zone support**: Students can't set up their own time zone



Canvas	**Accessibility**: Gold certification from the National Federation for the Blind **Up-to-date user interface**: Modern user interface throughout the application **Ease of administration**: Easy to learn and use the features and functions **Remarkable usability**: Faculty and students can immediately use application **Efficient workflow**: Easy to configure instructor tasks coupled with student activities **Plug-and-play LTI**: Simple Learning Tools Interoperability (LTI) can be added to the system **Strong support for collaboration**: Supports group work by providing a collaborative workplace **Rapid innovation**: New features and innovation are released every two weeks **Student centeredness**: Students are enabled to self-control their own learning	**Permission**: Permissions are set at the organization level and are not customized at the site level **Section management**: Instructors can't release announcements or activities to specific sections **Internal email system**: The internal email system does not support rich text messaging, searching, or sorting **Simplistic rubric tool**: Creating rubrics is cumbersome and the cell descriptor only has a few words **Simplistic rich text editor**: The advanced editing options are hidden in Canvas **No privacy preferences**: Students can't hide their names and profile
Moodle	**Cost-effective**: cost-effective even though additional costs might be generated **Ease of use**: Despite a variety of tool sets such as course management and communications, registration and enrollment tools, user management options, all features are simple and efficient **Customization**: Offers the ability to customize and control faculty and students' experiences **Rapid deployment**: Moodle offers the option of rapid deployment where LMSs need to deliver an online learning program on a project basis	**Accessibility**: Not certified from the National Federation for the Blind **Heavy dependency on third-party add-ons**: Heavily relying on third-party software increases time lag and workload to update the LMS **Insufficient maintenance investment**: It lacks the scale to make an investment in maintenance
D2L	**Accessibility**: Gold certification from the National Federation for the Blind **Assistance when designing course**: The Instructional Design Wizard helps instructors	**Steep learning curve**: With a wide range of tools, faculty and students feel pressured about learning something new **Restricted authority**: Instructors are not



	pedagogically build sound courses **Compatible with other D2L products**: Extended with additional D2L products **Mobility via response design**: The D2L interface is automatically adjusted to the device **Strong support for collaboration**: Supports random-, self-, manual-, and auto-assignment	allowed to combine course sections without administrator's permission **Instructor-centered orientation**: Students have little authority to manage LMSs even though instructors want to give more authority to students **Lack of student collaboration tools**: Collaborative workspace or tools are not currently offered **Lack of student-centeredness**: Students are not allowed to set due dates **No privacy preferences**: Students can't hide their names and profile

Table 2 - Privacy Initiatives in the United States Regarding FERPA.

This chart displays a list of examples of Privacy Initiatives in the United States.