PRIVACY IN MOBILE LEARNING APPLICATIONS: USER PRIVACY CONCERNS AND IMPLICATIONS OF APPLYING PRIVACY BY DESIGN APPROACH

by

Daria Ilkina,

BBA (Haaga-Helia University of Applied Sciences, Helsinki, 2011)

A thesis

presented to Ryerson University

in partial fulfilment of the

requirements for the degree of

Master of Management Science

in the Program of

Management of Technology and Innovation

Toronto, Ontario, Canada, 2015

Author's declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my thesis may be made electronically available to the public.

Daria Ilkina, Privacy in Mobile Learning Applications: User Privacy Concerns and Implications of Applying Privacy by Design Approach, Master of Management Science, 2015, Management of Technology and Innovation, Ryerson University

Abstract

This thesis investigates the privacy risks that m-learning app users face by identifying the personal information that m-learning apps collect from their users, and the privacy policies of these apps. It reveals that most of the m-learning applications have similar privacy policies, which seem to protect the interests of the providers rather than the users. The Privacy by Design framework is reviewed to determine whether it can help the developers address user privacy concerns. A survey is conducted to explore user concerns about m-learning apps' privacy practices. The results from the sample of 260 participants suggest that users are less concerned with the collection of personal information that is non-identifiable. The survey also revealed that the users are more concerned when an app shares their personal information with third parties for commercial purposes than when it is shared with the government.

Acknowledgements

I wish to thank for the support and guidance Dr. Catherine Middleton, Dr. Avner Levin, Dr. Ali Miri, Dr. Bettina West, Dr. Ann Cavoukian, Dr. Kathleen Greenaway, Dr. Deborah Fels, Dr. Ozgur Turetken, Mugino Saeki, Dr. Heather Driscoll, Dr. Ojelanki Ngwenyama, Dr. Lynn Lavallée, Toni Fletcher, Gloria Fernandes, Dr. Nataliia Kulikova, Dr. Alexander Ilkin, and Eric Hacke.

I would also like to extend a special gratitude to the committee chair and the committee members.

Dedication

I would like to dedicate this work to those who fight to protect privacy and do not accept the notion that “privacy is dead” in the Digital Age.

Table of Contents

Author's declaration ..... **ii**

Abstract ..... **iii**

Acknowledgements ..... **iv**

Dedication ..... **v**

List of Tables ..... **viii**

List of Figures ..... **ix**

Abbreviations, Symbols and nomenclature ..... **x**

List of Appendices ..... **xi**

Chapter 1 – Introduction and Research Overview **1**

1.1. Research Objectives and Research Questions 2

1.2. Mobile Learning Defined 5

1.3. Motivation for the Research 7

1.4. Structure of This Thesis 9

Chapter 2 – Mobile Learning Challenges, Privacy Concerns, & Privacy by Design 12

2.1. M-Learning Challenges and Main Research Areas 12

2.2. Privacy Considerations in M-Learning 17

2.2.1. Mobile Device-Related Vulnerabilities 17

2.2.2. Mobile Apps Permissions 20

2.2.3. M-Learning Apps-Related Privacy Issues, Threats and Concerns 22

2.3 Privacy by Design Framework 26

2.3.1. The Roots and Fundamentals of PbD 26

2.3.2. PbD Application Areas and Global Adoption 29

2.3.3. Criticism and Challenges of PbD 31

2.3.4. Applying PbD Principles to App-Based M-Learning 33

Chapter 3 – Methodology 36

3.1. Methodological Approach 36

3.2. Selection Criteria for the Apps for Privacy Policies Review 36

3.3. Quantitative Study 40

3.3.1. Target Population and Sample 40

3.3.2. Survey Design 42

3.3.3. Procedure 46

Chapter 4 – M-Learning Applications and Their Privacy Policies 48

Chapter 5 – Results of the Survey Study 70

5.1. Data Preparation Process 70

5.2. Sample Profile 72

5.3. The Sample's Familiarity With M-Learning Applications 76

5.4 Privacy Concerns and the Importance of Privacy Settings 82

5.4.1. ANOVA analysis results 91

Chapter 6 – Discussion 102

6.1. PbD Approach 102

6.2. Findings from the Privacy Policies Review 103

6.3. Survey Findings 104

6.4. Limitations 107

6.5. Implications and Further Research 108

Appendices 112

Reference List 148

Glossary 159

List of Tables

Table 2-1: The primary foci of the research on the m-learning challenges. 13

Table 2-2: Mobile learning security issues, threats and possible safeguards (adapted from Ugray, 2009) 24

Table 3-1: Inclusion and exclusion criteria for the m-learning apps for review 39

Table 5-1: Sample of M-learning Applications and What User Information They Collect and Share. 54

Table I-1: Settings that the users have customized in their m-learning apps..... 137

Table I-2: The features that the participants hope/expect to see in m-learning apps... 137

Table J-1: The importance of m-learning apps features or functionalities for the respondents, value range from 1 – Very Important to 7 – Not At All Important. 138

Table J-2: User attitude towards mobile learning apps collecting their information..... 138

Table J-3: Levels of users concerns when a mobile learning app shares their information with third parties. 139

Table J-4: Levels of users concerns about a mobile learning app's permissions..... 139

Table J-5: Users' feelings about m-learning apps' sharing their information with independent third parties for marketing purposes or with the government. 140

List of Figures

Figure 5-1: Age groups of the respondents....73
Figure 5-2: Gender of the respondents....74
Figure 5-3: The level of education of the survey respondents....75
Figure 5-4: The familiarity of the sample with m-learning apps....77
Figure 5-5: Frequency of use of m-learning application....77
Figure 5-6: Different genders' familiarity with m-learning apps....78
Figure 5-7: Age of the respondents and their use of m-learning apps....79
Figure 5-8: Frequency of use of the m-learning apps and the sample's age groups....79
Figures 5-9 and 5-10: The participants' education levels and their use of the m-learning apps....80
Figure 5-11: Frequency of use of m-learning application and the participants' education levels....81
Figure 5-12: Settings that the users have customized in their m-learning apps....83
Figure 5-13: The features that the participants hope/expect to see in m-learning apps 84
Figure 5-14: The importance of m-learning apps features or functionalities for the respondents, rated from 1 – very important to 7 – not at all important....85
Figure 5-15: User attitude towards mobile learning apps collecting their information..87
Figure 5-16: Levels of users concerns when a mobile learning app shares their information with third parties....88
Figure 5-17: Levels of users concerns about a mobile learning app's permissions....88
Figure 5-18: Levels of user concerns about an m-learning application sharing their PII or Non-PII with third parties for commercial purposes or with the government....89

Abbreviations, Symbols and nomenclature

App – software application

E-learning – electronic learning

GPEN – Global Privacy Enforcement Network

GPS – Global Positioning System

ICTs – Information and Communication Technologies

IP – An Internet Protocol address

IPR – Intellectual Property Rights

LMS – Learning Management System

M-learning – Mobile learning

MOOC – Massive Open Online Course

Non-PII – Non-personally identifiable information

OS – Operating System

PbD – Privacy by Design

PDA – Personal Digital Assistant

PII – Personally identifiable information

REB – The Research Ethics Board

TAM – Technology Acceptance Model

ToS – Terms of Service or Terms of Use

TPB – Theory of Planned Behaviour

List of Appendices

Appendix A – The 7 Foundation Principles of Privacy by Design 112

Appendix B – The Tips for Communicating Privacy Practices to The Apps' Users..... 113

Appendix C – Research Ethics Board Approval..... 115

Appendix D – Recruitment Scripts for Posts on Social Media..... 116

Appendix E – Consent Form for the Participation in the Study 120

Appendix F – Survey Questions..... 123

Appendix G – Study factors and items/variables for the survey 133

Appendix H – Demographic Information of the Sample..... 136

Appendix I – Important Features and Settings in M-Learning Apps for the Users..... 137

Appendix J – Tables of Means 138

Appendix K – ANOVA Tests..... 141

Chapter 1 – Introduction and Research Overview

In our age of rapid technological development, personal data generated by user behaviour has gained a new meaning and a new value. This personal information has become an economic asset for many businesses and organizations. (Cavoukian & Reed, 2013.) Unfortunately, the increase in the value of personal information may lead to larger privacy risks and greater challenges for personal data protection.

This thesis is focused on the user-related privacy concerns in mobile learning or m-learning. According to Ugray (2009), there are three m-learning user groups that can be affected by the m-learning security issues and threats: the managers, the instructors, and the learners. The instructors and the managers are the m-learning developers, implementers, and content providers. For the purposes of this study they are not considered to be end-users as they do not have to register or subscribe to the learning material, or enrol into classes. They are faced with fewer privacy issues, because they don't have to provide as much personal information as learners who are using m-learning applications. This research is mainly focused on the learners, because ultimately they are the end-users; and as such, they bear the greatest privacy risk.

The thesis explores privacy challenges in the app-based mobile learning environment. Different types of the m-learning applications and their privacy policies were reviewed for this study to find out what information is collected from the users and how this information is used. This research also explores how the Privacy by Design framework can be applied to address privacy concerns in the m-learning apps and to provide

guidelines on embedding privacy in the development process of m-learning solutions. Quantitative data were collected and analysed for this study in order to examine the importance of privacy for the m-learning app users and to investigate whether privacy concerns have any impact on their usage patterns.

1.1. Research Objectives and Research Questions

Whether privacy has to be sacrificed for the sake of the innovation and/or business development is the subject of debate. There is a belief that privacy cannot exist in our modern digital world. However, as pointed out by Cavoukian (2012), this is a misleading and flawed "zero-sum model" that has to be shifted towards a "positive-sum paradigm" that should be inclusive and allow for the simultaneous growth of privacy and other functionalities. Following this idea, I adopt a viewpoint that privacy should be embedded in the designs of mobile learning solutions, because it is the responsible thing for the developers to do and is beneficial for them and their users.

The primary objectives of this study are to identify the privacy concerns in m-learning applications, to investigate whether users are concerned with the privacy risks at all, and to determine if those concerns somehow affect their use of the m-learning applications. The secondary purpose of this study is to explore how and if Privacy by Design (PbD) can address user privacy concerns and help developers of m-learning applications create more privacy-conscious solutions while being more transparent with their users. Privacy by Design is a framework developed in the 1990s by the former Information and Privacy Commissioner of Ontario, Ann Cavoukian. The main idea behind this approach is that privacy should be embedded in the design principles,

the core processes, and the daily operations of any organization. According to PbD, user privacy should be a primary design consideration so that organizations can be proactive rather than reactive when it comes to the privacy threats.

For the purposes of this thesis, PbD is not used as a theory to guide the research process; though I do attempt to apply the principles of PbD to demonstrate their potential in m-learning. The PbD approach is built upon 7 principles that allow organizations to embed privacy concerns in the architecture of their systems and processes. Together those principles (see Chapter 2) define a number of the responsibilities and requirements that could be considered a strategy or a guideline for the successful implementation of the best privacy practices in business and product development.

The research is guided by the following research question:

- *What are the user privacy concerns regarding m-learning applications and what effect these concerns have, if any, on the use of m-learning applications?*

The following sub-questions are explored to support the main research question:

- How do m-learning applications communicate privacy information to the users? Do they have privacy policies? And how transparent are they about their use of personal information?
- How user privacy concerns can be addressed to embed best privacy practices in the app-based m-learning environment?

- How concerned are users (experienced, novice and/or potential) of the m-learning apps about user information collection? Does it matter to the users what type of personal information is collected from them?
- How do the learners feel about m-learning applications' developers sharing their user information with the third parties?
- Does it matter to the users what kind of user information their m-learning apps share with third parties, for what purposes, or with which parties?
- Can Privacy by Design approach help developers create m-learning applications that protect user privacy? If so, how?

The review of Privacy by Design framework helped direct this research and focus more on particular issues of communicating privacy information to the users of m-learning apps. Privacy by Design framework helped to guide the review of the privacy policies of the mobile learning applications. The review of the privacy policies was necessary to design a comprehensive survey that would address the main research question. Privacy by Design framework also helped to focus my attention to the following issues while reviewing m-learning applications:

- Are users informed about what data is collected from them and how it is used?
- Can users of m-learning apps opt-out from sharing their privacy information?
- Who can access user information, is it shared with third parties and for what purposes?

1.2. Mobile Learning Defined

According to Verma et al. (2012), m-learning is a perfect ecosystem for learning to occur, because learning as an activity is dynamic and mobile with regards to space, time, and topic areas: "learning occurs at different places (e.g., learning institutes, workplaces, homes, and even places of leisure), at different times (e.g., working days, weekends, or holidays), and between different topic areas of life (e.g. education, work, self-improvement, or leisure)". Verma et al. (2012) generalized that there are three types of the m-learning systems: push-based, application-based, and browser-based. This research is focused on the application-based m-learning (i.e., apps that have to be downloaded and installed on mobile devices, and not web browser-based tools). Push-based tools differ from the others in that information delivery is initiated by the provider of the m-learning tool and not by the user, i.e. they don't provide on-demand service. Mobile learning applications (app-based tools) require more personal involvement and control from users than push-based solutions, which is why the user privacy concerns are potentially higher in app-based solutions.

Li Shiliang and Sun Hongtao (2013) define m-learning as "any learning or training (i.e. knowledge construction, skill development training, and performance support) which learners engage in across various locations and contexts at the time of their choosing". Dye et al. (2003, as cited in Chong et al, 2011) expand this definition by stating that m-learning is any learning or training that occurs on a device that can provide content and wireless communication between a course instructor and a learner, meaning that m-learning requires interactivity. In this thesis, I adopt the aforementioned views, adding

that m-learning has to be performed using a handheld mobile device such as a tablet, a personal digital assistant (PDA), a smartphone, or a mobile phone.

Even though different researchers propose different definitions for the mobile learning, all of those definitions can be roughly classified into two categories:

1) *a techno-centric perspective on m-learning*, through which the m-learning is defined by the technology: m-learning is any learning or training that is delivered and received by the means of the mobile devices such as phones, PDAs, digital audio players, and even digital cameras, voice recorders, pen scanners, etc.;
2) *a learner-centred perspective*, when m-learning is defined as "any sort of learning that happens when the learner is not at a fixed, predetermined location, or [as] learning opportunities offered by mobile technologies" (Keskin & Metcalf, 2011).

To properly understand the uniqueness of the mobile learning ecosystem and its challenges, we should consider both the technological and the learner (user) centred perspectives of m-learning, which is why this research takes into account the specifics on m-learning delivery via applications on mobile devices, as well as the views and concerns of the current and potential users of such apps.

There are many mobile learning applications available and many are in development. Hao and Dennen (in Miller & Doering, 2014) categorise the variety of m-learning applications according to their paradigms and functions. They identify four types:

1) **M-learning app as a "Tutor":** the main function is direct instruction and assessment (e.g., Flash cards, quiz games apps);

2) **M-learning app as an "Information source":** the main function is to present information (e.g., eBooks, animations);
3) **"Simulator":** an m-learning app that presents an environment (e.g., role-play games or virtual worlds);
4) **"Collaboration enabler":** an app that connects people and helps them work together (e.g., discussion forums, Web 2.0).

Considering the definition of m-learning adopted in this thesis, the applications that provide learning content but do not require users to interact with a course instructor and/or between each other are not considered mobile learning applications. The methodology part of this thesis (Chapter 3) discusses in more detail what type of m-learning apps were included in this research and why.

1.3. Motivation for the Research

Mobile learning (m-learning, also sometimes spelled mLearning) has been around for about two decades. It used to be considered a part of e-learning or a transition from it, and some researchers still share this view (Kadirire, 2009; Park et al., 2012; Ayoma and Oboka, 2013). However, a growing number of researchers (Haag, 2011; Cheon et al., 2012; Kambourakis, 2013; Garg, 2013) agree that m-learning is a completely separate practice from e-learning, with its own rules and philosophy. According to Kambourakis (2013), compared to e-learning, m-learning "imposes an entirely different path to be followed towards information presentation, instructional design, graphic and user experience design". Mobile devices are becoming more ubiquitous than personal computers due to their affordability and portability. Because of that, users in many

countries bypass e-learning technologies in favour of adopting m-learning. (Towards Maturity, 2013.) In many developed countries, including Canada, being mobile and digital is more of a necessity rather than a luxury in recent years. People increasingly use mobile devices in their everyday lives for socialising and communication, shopping, business, entertainment, planning out their tasks and schedules, accessing news, and more (Nielsen, 2014). As mobile devices become more affordable and accessible, mobile learning technologies become more widespread and relevant. The latest advances in the mobile devices not only help increase the popularity of the mobile learning, but also create new possibilities for the development of the mobile learning applications. Due to these technological developments, the "paradigms of teaching and learning are being transformed from a traditional, situated, and lecture-based format to an on-demand, online environment, where learning is collaborative and socially constructed" (Schroeder, 2013).

The researchers and scholars who explored m-learning in the early 1990s expected a rapid revolution in education with the emergence of m-learning technologies. Despite these high expectations, no dramatic change in the education or workplace training was achieved at that time, and we still have a long way to go until we embrace the full potential of the mobile devices and the mobile learning technologies in schools and in the workplace (Cheon et al., 2012). This raises questions about the possible challenges and obstacles for m-learning development and motivated me to explore user-related concerns in the m-learning ecosystem.

The literature review (see Chapter 2) revealed that there is a lack of research about the privacy threats in the m-learning environment. Current research about m-learning

revolves mostly around the economic challenges of m-learning delivery and acceptance (e.g., no access to mobile devices) and less so around the socio-technological problems within the m-learning ecosystem. Even though there is a growing body of research on the issues of the m-learning design (Uden, 2007; Maske et al., 2011), adoption (Liu et al., 2010; Crescente & Lee, 2010; Gong & Wallace, 2012), and acceptance (Liaw et al., 2010; Maske et al., 2011; Cheon et al., 2012; Mohammad & Job, 2013), there is a lack of studies on the issues of privacy in m-learning (Kambourakis, 2013; Ugray, 2009). The research that has been done in the area so far is mainly focused on the challenges from the developers' and designers' perspective, and on the privacy concerns of the educators who provide the content for the m-learning solutions. Unfortunately, little to no attention has been given to the actual users of the m-learning tools (i.e., the learners) with regard to what privacy threats they may encounter using m-learning applications, and how much they care about their privacy in their use of m-learning apps.

It is important to identify the m-learning privacy challenges in order to design the solutions that deal with those challenges effectively. Starting from the early stages of the product development, the designers have to consider that the m-learning applications they create can have potential privacy risks for the users of those applications.

1.4. Structure of This Thesis

The research process for this thesis included a literature review on the privacy concerns in the m-learning ecosystem, a review of the m-learning apps, and a survey of user privacy concerns in the use of m-learning applications.

Chapter 2 covers the literature and theory review. In this chapter, I present a relevant body of literature and current research in the field of m-learning in general, and the review of the literature on privacy issues in m-learning in particular. This chapter discusses the most common concerns in the mobile learning industry and identifies the gap in the research on m-learning privacy challenges. It starts from a general overview of the field of study and then proceeds to a more narrow inquiry into the specific privacy concerns in m-learning. In addition, this chapter focuses on the Privacy by Design approach and explores if it can be applied (and how) in the mobile learning apps research and development.

The literature review helped in defining the research problem and set the ground for the next stages in the research process. Apart from the literature review and the theoretical considerations, the research involved two major steps: the review of the privacy policies of m-learning applications, and the survey study.

Chapter 3 outlines the research design and discusses the methods used for this thesis project. Both secondary and primary data were collected for the purposes of this study. The secondary data included reviews of the academic publications, white papers, media articles and reports, and other publicly available materials. The Privacy Policies and the Terms of Service of different m-learning apps were reviewed for this research in order to identify potential user-related privacy risks and to explore what needs to be addressed in the survey research. Chapter 3 discusses different types of m-learning applications and the context of this study to explain the inclusion and exclusion criteria for the mobile learning apps for the review. It also presents the methodology for the survey study and the design of the survey instrument.

Chapter 4 presents a review of the Terms and Conditions, Terms of Use/Service and Privacy Policies of the popular m-learning apps to identify what user information is being collected by those apps and why.

Chapter 5 covers the results of the survey research. Data collected through an online survey tool have been coded, entered in SPSS, cleaned, and analysed. This chapter presents the results of that data analysis.

Chapter 6 presents the discussion about the thesis findings, interpretation of the results, and the implications and contributions of this research. This concluding chapter also acknowledges the limitations of the study and makes suggestions for further research.

Chapter 2 – Mobile Learning Challenges, Privacy Concerns, and Privacy by Design

2.1. M-Learning Challenges and Main Research Areas

M-learning has been viewed either as a part, or as an extension, of e-learning since the 1990s, but lately more researchers consider it a discipline in its own right (Ugray, 2009; Crescente & Lee, 2010). According to Crompton (2013), m-learning became a recognized term only in 2005. M-learning has the potential of making learning more widely accessible, because it decreases the limitation of the learning location with the mobility of the general portable devices (Ayoma & Oboko, 2013). It is a growing industry in many regions in the world, especially in the United States and China (Liu et al., 2010).

There are many issues to consider in the m-learning ecosystem. M-learning used to be considered a disruptive innovation and was expected to substantially change the learning and training practices and become ubiquitous over two decades ago. This *revolution* occurred neither in education nor in business environment. For mobile learning to move "from project status to the mainstream", Paliwal and Sharma (2009) suggested the following:

- Convince the universities to accept m-learning;
- Produce m-learning development kits for the universities and colleges worldwide;
- Produce course guides and develop literature on m-learning;

- Produce course modules for mobile devices. (Paliwal & Sharma, 2009).

However, before taking the aforementioned steps, there is still a need to understand the specific problems and concerns in the m-learning environment. Knowing what challenges have to be addressed in m-learning can potentially boost its development and implementation, and also improve m-learning adoption, perceptions and acceptance toward it. Common m-learning challenges can be identified from reviewing relevant literature.

According to McConatha and Praul (2007), the first published studies focusing specifically on m-learning date back to the early 2000s. Within those studies the question of the mobile learning challenges has been raised repeatedly, yet there is some controversy about it among the researchers and educators (McConatha & Praul, 2007). Consequently, there are different perspectives on how those challenges should be addressed and resolved. Table 2-1 below summarizes various problems, challenges and concerns in the m-learning environment identified and discussed in the literature.

Table 2-1: The primary foci of the research on the m-learning challenges.

Topic/concern	What questions were raised; what problems were explored	Notable publications
Adoption of m-learning	• Empirical analysis of factors affecting the adoption of m-learning in Malaysia based on the extended technology acceptance model (TAM) and the theory of planned behaviour (TPB). • Literature reviews of m-learning adoption processes worldwide.	Liu et al., 2010; Chong et al., 2011; Crescente & Lee, 2011; Gong & Wallace, 2012.
User readiness or market	• Exploration of older workers' attitudes toward m-learning in	Song & Erdem, 2011; Cheon et al., 2012;

readiness; Perceptions and attitudes toward m-learning	hospitality (case study); • Investigating college students' perception and readiness toward m-learning applying the TPB.	Marwan et al., 2013.
Acceptance of m-learning	• Applying the Activity Theory (AT) in the research on acceptance toward m-learning. • Using the TAM and the TPB to evaluate students' acceptance of m-learning. • The TAM model evaluation of the drivers of user acceptance and willingness to pay for m-learning.	Liaw et al., 2010; Maske et al., 2011; Park et al., 2012.
Teacher perception of m-learning	• What are teachers' perceptions to m-learning and do they differ depending on the discipline/branches? (Developing Mobile Learning Perception Scale for analysis)	Uzunboylu & Ozdamli, 2011.
Drivers of m-learning business development	Descriptive research to classify m-learning actors and its environmental factors (technology, market condition and regulations identified as main drivers of m-learning business).	Nasiri & Deng, 2009.
M-learning implementation	• What are the criteria for the inclusion of m-learning in education and training; • What teachers should know to organise/create a course for m-learning; • How to develop and implement m-learning strategy in a large enterprise; • The importance of continuous learning support in m-learning environment.	Paliwal & Sharma, 2009; Schroeder, 2013; Garg, 2013; Elias, 2013.
Content delivery	• Exploring mobile learning with micro-content delivery for mobile devices (case studies); • How to create instructional content;	Bruck et al., 2012; Elias, 2013.
Evaluating effectiveness of m-learning	• How to effectively measure learning in the mobile environment? • How to evaluate the effectiveness of m-learning?	Sharples, 2006; Vavoula & Sharples, 2009; Saccol et al., 2010;

	• M-learning as a support service to increase effectiveness of e-learning and increase learner retention rate.	Traxler, 2013; Ayoma & Oboko, 2013.
MOOCs in the m-learning context	Evaluating the MOOC format as a possible pedagogical approach for m-learning (case study and empirical analysis)	De Waard et al., 2011; De Waard, 2013.
M-learning and the cloud	Descriptions and explanations of cloud computing and suggestions on using it to resolve data storage challenges in m-learning.	Mallikharjuna Rao et al., 2010; Verma at al., 2012; Elias, 2013; Kambourakis, 2013.
M-learning design	Investigating what are the design challenges in m-learning. Suggested points for considerations from the various articles: • Small screen sizes; • Mobile device memory size; the issues of data storage; • Device variability; • Context of use; • Mode of access; • Internet access and internet download speeds. Offline or online access; • Design scale; • Multimedia content creation; • Accessibility of the m-learning apps.	Sharples, 2006; Crescente & Lee, 2011; Maske et al., 2011; Tan & El-Bendary, 2013; Elias, 2013; Miller & Doering, 2014.
Security and privacy concerns in m-learning	Literature reviews and overview of the developments in the m-learning technologies, conducted to classify possible (potential) security and privacy challenges.	Ugray, 2009; Kambourakis, 2013; Garg, 2013.

W.-H. Wu et al. (2012) conducted a meta-analysis to review and synthesize relevant to m-learning literature, and came to the conclusion that all current research in this area can be divided into two broad categories or "research directions": 1) "evaluating the effectiveness of mobile learning," and 2) "designing mobile learning systems." (Wu et al., 2012, p. 818.)

The literature review conducted for this thesis revealed that the problems of m-learning adoption and acceptance are the most explored subjects in research on m-learning. The most commonly used theories in the studies on those issues are the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM). In addition, the Activity Theory developed by Engeström is becoming increasingly popular in m-learning research. For a detailed review of theoretical approaches used in m-learning research, see Keskin & Metcalf (2011). After technology adoption and acceptance, the most popular research subject in m-learning is m-learning design. The variety of mobile devices makes it difficult to create common m-learning standards and to design m-learning solutions that cater to different platforms (Educause, 2010); both of which can explain why challenges of m-learning design is a popular research topic.

M-learning providers and developers face pedagogical, technical, administrative, and even legal challenges when designing their m-learning products and services. It is important to recognise that those challenges also include security and privacy concerns (Kambourakis, 2013). For instance, one of the most recent books on mobile learning, "The New Landscape of Mobile Learning", edited by Charles Miller and Aaron Doering (2014), combined a number of articles with the latest research on the design challenges in the app-based m-learning, yet privacy concerns were completely overlooked in all of the studies selected for this publication. Generally speaking, the research gathered in this book was mostly conducted from the designers' perspective or the teachers' and content developers' perspectives, but not from the users' perspective. This sort of ignorance of the user-related privacy concerns seems to be a common problem in m-learning research. The researchers express concerns with the protection of the course

materials from the course developer's perspective, i.e. copyright issues (Kambourakis, 2013), but there is no discussion about protecting the users and the information they provide to m-learning applications.

There is a need to identify possible insecurities that are specific to the m-learning environment, because an understanding of the user privacy concerns is a prerequisite for the development of the user-centered design. This thesis aims to begin an inquiry into user-related privacy concerns in app-based m-learning ecosystem.

2.2. Privacy Considerations in M-Learning

2.2.1. Mobile Device-Related Vulnerabilities

As m-learning gains more acceptance, the developers face more challenges in the m-learning implementation and design. Some of these challenges are directly related to the reliance on the mobile and wireless technology (Ugray, 2009). It may be harder to manage security concerns in application-based mobile learning than in the web-based mobile learning because the applications are downloaded directly onto the users' devices. Mobile and wireless devices are inherently vulnerable to the privacy risks, security breaches and cyber threats because of the broadcast nature of wireless communication (Ugray, 2009; Garg, 2013). Hence, the developers have to think about the privacy and security concerns of both the apps and the devices (Kam, 2012; Garg, 2013). Mobile devices used for system-to-system data transfers or to enable interaction (e.g., in m-learning context) may trigger privacy risks such as unwanted data collection or leakage, user's location tracking, improper redirection to an unknown website,

initiation of an unknown service, receipt of unwanted content, and also identifying users when they want to stay anonymous (Cavoukian, 2011).

According to Kam (2012), the devices and the apps follow a standard lifecycle of technological development, in which a security is not a concern until a technology is adopted and becomes a part of consumers' everyday life. Rapid adoption is encouraged to get this lifecycle going and to boost innovation and development. Such "backwards approach" to security may be justified by the vendors' uncertainty about the adoption of the new technology, but it creates a problem defined as a "lifecycle of insecurity" (Kam, 2012): developers often address security issues at the point when a device or an app is already adopted and is already popular with the users. This order of things doesn't make the job of the developers easier. Ignoring security aspects to release an app or a device as soon as possible doesn't necessarily have a positive impact on the business development as well. It would be more reasonable to "reverse the cycle" and embed privacy and security in the design rather than coming up with the solutions after the security threats become a major problem. (Kam, 2012.)

Users cannot rely on applications and wi-fi hotspots for security if they need safe Internet connection to use an app; and mobile devices do not necessarily have built-in protections like anti-virus software, firewalls, or VPN. Users can download applications to protect their data, but it should not be only the users' responsibility to protect the data on their devices from privacy and security threats, as many users may not be aware of all the risks that come with downloading an app. There is also a concern that mobile users do not take the necessary measures to protect themselves from the privacy risks and the possible vulnerabilities. According to Symantec's Norton Report

2013, 57 percent of adults were unaware about the existence of the security solutions that can protect their mobile devices in 2013; yet, in 2012 this number was at 44 percent. If this trend is correct, it can be explained by rapidly growing numbers of the users of the mobile devices (Symantec, 2014). As mobile devices become more ubiquitous and users come from increasingly diverse backgrounds, increasing numbers of users may not see the value of personal information protection until they experience a breach of their data security. Furthermore, privacy protection cannot be left to the users alone as most users may not know how to protect their data, or may not have the tools or resources to do so.

Contrary to popular belief, password protection is insufficient to secure personally identifiable information (PII) on a mobile device. Access to PII on a mobile device has to be both password-protected and encrypted to secure the device from the breaches of PII (Cavoukian, 2013b). Fortunately, iPhones and Android phones are now encrypted by default, not relying on user skills or even awareness to provide this security. However, Garg (2013) claims that the data encryption and the login-protected access are not enough; he suggests that m-learning app users need to implement more rigorous security measures such as Mobile Device Management (MDM) and Mobile Application Management (MAM).

Apart from the breaches and cyber threats, there are other more common risks that users might not be aware of. For instance, mobile applications often collect highly accurate sensor data (such as location) without users' knowledge, without a clear explanation of why they need to collect these data, and without explicitly declaring who has access to this information after it is collected.

The above-mentioned data protection measures may seem extreme for m-learning apps' users; but student or learner information may be very sensitive. M-learning applications collect not only personal information such as birth date, personal contact information, and credit card information, but they also collect and store their users' educational history (e.g., courses/classes taken or enrolled in), grades, test scores, learning progress, etc. It should be considered that sharing this information with commercial organizations, government, or any unknown third parties might be damaging or unpleasant for some users.

2.2.2. Mobile Apps Permissions

Most apps require their users to grant various permissions to enable even the basic features of the apps. An application's permission means an access to the information on a user's mobile device that this application requires in order to operate or to unlock special features for the user. Every application has some baseline permissions that are granted automatically when the app is installed (e.g., access to the Internet). In addition, an app could ask for many extra permissions such as access to contacts, access to calendar, GPS/location tracking, access to a camera or a microphone, etc.

More than 1,200 mobile apps were examined in the Global Privacy Enforcement Network (GPEN) Sweep in May 2014 (Cohen, 2014). In the course of this sweep, 26 privacy enforcement authorities from different countries reviewed the privacy policies of 1,211 mobile applications and found that more than 30% of those apps ask users to grant permissions beyond the functionalities of the apps or do not provide an explanation why they need an access to some of the user personal data (Cohen, 2014).

For example, it is understandable that Instagram (a photo-sharing app) requires a permission to access a camera so that users can take pictures using the app; and it asks for an access to its users' photos for users to be able to upload their pictures to their Instagram feeds. As another example, it is unclear why a flashlight application would ask to access users' location, and contacts. The sweep revealed that most of the apps track users location, but in many cases it is unclear why. (Cohen, 2014.) According to Sweatt et al. (2014), sharing user location "with the public or specific third parties might be risking robbery, identity theft, etc." (Sweatt et al., 2014, p.27). Considering how sensitive such information could be, it is important to find out how applications use this information and whether they share it with any third parties.

Depending on the app or on the device, users may grant all app's permissions by default. For instance, due to Android's design, mobile applications "must grant all access regardless of the permission type or need" (Liccardi et al., 2014). In other words, an Android user can either choose to allow all permissions at install time or opt-out from using some apps altogether. Apple users manage their permissions differently. An iOS app's permissions system does not grant any special permissions for the apps when a user installs an application, allowing for only basic permissions. When an iOS application needs to use additional permissions, a pop-up window occurs asking the user to grant the access, and the user then has a choice of refusing to provide it. An iOS user can also manage the permissions in the Settings after the app is already installed. Android users used to have a similar option with an even better functionality via the AppOps built-in application permission manager, but it is no longer available for

Android 4.4.2. Some advanced users can root[1] their Android devices to allow them to individually manage permissions; but this is a complicated process and most users would not have the technical skills, nor the wish to void their device's warranty.

It is worth mentioning, however, that not everything that may be perceived as privacy breach or developers neglecting privacy is intentional. According to Fekete (2012), without proper monitoring programs installed, the developers may not know that their apps handle personal information exactly as it is described in their apps' privacy policies. Fekete (2012) also suggests that some apps may collect personal information "simply because it may be useful in the future", and he cautions to avoid following this practice.

Generally, users can opt-out from sharing certain data with the mobile apps only if they are aware of the permissions and the privacy policies of the apps they use. However, many applications are ambiguous about what information is collected on their users and for what purposes. To investigate how m-learning applications use personal information, I profiled 31 m-learning apps. The results of this examination are presented in the Chapter 4.

2.2.3. M-Learning Apps-Related Privacy Issues, Threats and Concerns

The literature review suggests that there are many issues in m-learning directly related to the mobile devices and the insecurities of the wireless networks; however, there is a lack of research exploring the m-learning-specific privacy threats. The mobile apps

[1] Rooting means running a process that grants the user a root access (control) to the operating system of the Android device.

developers and designers share many common security and user privacy protection challenges, but every type of application might have specific concerns related to its functionalities. Specific challenges for the developers of m-learning apps should be explored.

There are many privacy risks to consider in m-learning. One of the main concerns remains the fact that users have little to no ability to manage their privacy settings in mobile applications. As was mentioned earlier in this chapter, users may share personally identifiable information with the apps, including but not limited to the information about their courses, their progress and grades, their academic and professional or even personal interests. Information about what course a user wants to take or takes for personal or professional development may be sensitive, a user may not want to share this information with third parties. Information about the progress of the m-learning users and their grades may be another piece of information that they would not want to share with anyone. Increasing numbers of m-learning applications also incorporate connections to social networking sites (Ugray, 2009), meaning that those applications have access to the users' profiles on social networks and vice versa. This creates additional privacy challenges, because learning-related information may be too sensitive to share it with others (Ugray, 2009).

In recent years, many m-learning solutions have been integrated with cloud computing due to the limited storage and computational power available on mobile devices. With the help of cloud technologies it is now easier for educators and learners to share large files via m-learning platforms (Kambourakis, 2013). However, the cloud computing paradigm presents new security challenges for the educational environment. Verma et

al. (2012) identify three mobile cloud-related security threats in m-learning: malware, privacy concerns, and authenticating access. They suggest dealing with those threats by "putting in-host based security just as we do for PCs" (Verma et al., 2012).

An interesting approach specifically tailored to m-learning security and data protection can be observed in the US army. The developers of the mobile learning tools for the US army pursue solutions which ensure that their smartphones can access learning and training data but not store it, thereby limiting the exposure of sensitive data if a device is captured or hacked by hostile forces. (Gould & Biron, 2012.)

Table 2-2 sums up the general security threats and problems and their possible safeguards in the m-learning ecosystem.

Table 2-2: Mobile learning security issues, threats and possible safeguards (adapted from Ugray, 2009)

M-learning issues and phenomena	Type of threat or problem	Safeguards
Novel technologies, devices and apps	Errors, malfunctioning	User training
Lack of uniform viewing platform	General access issues	Developing for broadest possible base; limiting supported device types
Limitation of battery power, memory and computing capacity available for devices	Device usage limitations	Developing 'slim' apps; developing computationally low intensity security algorithms and protocols; using cloud technology
Small device size	Physical threat (i.e., the device can be stolen)	Physical protection of devices
Cloud education	Availability, privacy, malware	Putting in-host based security
Business continuity	Availability	Disaster recovery; crisis and risk

		management
Broadcasted data	Confidentiality, privacy	Encryption; digital signature; authentication and access protocols and policies
Learning content creation, protection, and access	Integrity, availability, confidentiality, privacy	Encryption; digital signature; authentication and access protocols and policies
Emerging learning hubs on social networks	Privacy	Limiting openly accessible data

In addition to the aforementioned issues, Kambourakis (2013) suggests that there are problems of "content filtering", and the protection of copyright and intellectual property rights (IPR). He describes the need for content filtering as the need to block some inappropriate content from children (Kambourakis, 2013). In the case of app-based m-learning, providing appropriate content for learning is the responsibility of the course instructors and content developers, with app developers responsible for preventing any inappropriate third party advertising. As for the copyright, while protection of the learning materials in m-learning apps may be a valid concern, the focus on this topic within a discussion on privacy challenges in m-learning provides another example of the research where attention is given to addressing the problems of content developers and system designers rather than to the exploration of the learners' personal data protection. Admittedly, Kambourakis (2013) makes a point that there should be a fair trade-off between the users and developers: the users have to share some data so that developers can provide their assistance, enable assessment and support collaboration. However, it should also be said that often users have to provide more information than an app requires to function, and often users have no possibility to opt-out from sharing this information with the app.

To sum up, the literature review identified the following gaps that this thesis aims to address:

- There is little research on privacy issues in m-learning, and in this research only developers' and providers' privacy challenges are considered. No attention has been given to the privacy concerns from the perspective of m-learning users (learners).
- The privacy concerns that have been mentioned in the literature on m-learning are very general and can be applied to anything that is done on mobile devices, and not specific to m-learning activities.

2.3 Privacy by Design Framework

2.3.1. The Roots and Fundamentals of PbD

Privacy by Design (PbD) is a framework created in the 1990s by the former Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian. PbD advocates for embedding best privacy practices in an organization's default mode of operation rather than trying to assure user privacy only by complying with regulatory frameworks and privacy legislation. This approach states that privacy risks should be addressed when a technology is being developed and not when it has been already adopted (Cavoukian, 2012), which is why PbD could be an appropriate approach for breaking the "lifecycle of insecurity" in the modern technologies.

PbD is composed of the seven principles that are designed to serve as a guide for embedding best privacy practices across the business ecosystem. Each principle

encompasses a set of actions that are needed for successful systematic execution and fulfillment of those principles. The PbD framework was developed to anticipate and prevent privacy-invasive events rather than wait for privacy risks to turn into breaches (Cavoukian, 2013a); thus the first principle of PbD is called *"Proactive not Reactive; Preventive not Remedial"*. It dictates a number of actions that focus on the roles played by organizational senior management in the development and execution of an effective privacy policy (Cavoukian, 2012).

The second principle of PbD is *"Privacy as the Default Setting"*. It was set to protect users' privacy even when they don't protect themselves. As was discussed earlier in this thesis, users are not always aware of the privacy risks associated with the use of mobile devices or m-learning applications. Moreover, even if a user knows about the threats, they may not know how to address them. For that reason, the PbD approach encourages the developers and managers to ensure that personal data are automatically protected by IT solutions and business practices. This principle dictates that ensuring the security of personal data should not be the responsibility of a user alone. The providers, designers, and developers should be responsible for creating safe and secure systems that would have user privacy protection as a default setting.

The next principle – *"Privacy Embedded into Design"* – urges organisations to incorporate best privacy practices in the core of their business practices, IT solutions, and system development lifecycles instead of making privacy an "add-on" feature after the systems have been already developed. According to PbD, user privacy should be an essential design component rather than a secondary feature (Cavoukian, 2013a).

PbD advocates the philosophy that if some design features are not feasible from the privacy perspective, than the developers should let go of those features at the design stage or find a technological solution that would allow adding the desired features without jeopardising user privacy. It is unethical of the designers to add features to their products that cannot be built to respect user privacy.

One of the most challenging dimensions of the PbD is its fourth principle, called *"Full Functionality – Positive-Sum, not Zero-Sum"* (Cavoukian, 2012). The PbD approach doesn't tolerate zero-sum solutions that require making trade-offs to the disadvantage of the user privacy protection. This principle aims to provide a set of requirements and activities for organizations to accommodate their development without sacrificing privacy, emphasising that innovation and legitimate business interest can coexist with best privacy practices and solutions.

The principle *"End-to-End Security – Full Lifecycle Protection"* states that the PbD approach has to be embedded into the systems from the beginning and then extend data protection from the period when first elements of information are collected throughout the full lifecycle of that data involved from start to finish, until the time when the retained data is "securely destroyed at the end of the process, in a timely fashion" (Cavoukian, 2013a).

Next, the sixth principle is *"Visibility and Transparency – Keep it Open "*: it states that visibility and transparency are essential for the strong privacy program. An organization's approach to privacy should be visible and clear to its customers to generate trust in an organization and its operations.

Finally, the last principle of the framework is *"Respect for User Privacy – Keep it User-Centric"*: the PbD approach protects the interests of the end-user above all, and the compliance with the PbD requires organizations to make their systems user-friendly. From the PbD perspective, user-centricity means "anticipating users' interests and capabilities, making it easy for them to interact with a given system, to understand the essential privacy-related processes, their applicability and relevance and to make effective use of available options to express [user] privacy preferences and customize [user] online experience" (Cavoukian & Weiss, 2012). Furthermore, creating a user-friendly and user-centric design means taking into account or anticipating, whenever possible, who the end-user will be, and developing tools and solutions with that particular user in mind. For instance, if a product or a system is intended for children's use, it might be appropriate to make the privacy settings more restrictive (Cavoukian & Weiss, 2012).

2.3.2. PbD Application Areas and Global Adoption

Over the last almost 20 years, PbD gained a widespread acceptance within the public and private sectors. The PbD framework has been endorsed by the International Association of Data Protection Authorities and Privacy Commissioners, the European Union, the U.S. Federal Trade Commission, and many individual privacy professionals (Cavoukian, 2012).

In 2010 PbD was unanimously approved as an international standard by the International Assembly of Privacy and Data Protection Authorities at their annual conference in October 2010 in Jerusalem, Israel (Cavoukian & Jutla, 2014). At this

conference PbD has been declared an essential component of fundamental privacy protection in the Resolution, which was co-sponsored by Canadian Privacy Commissioner Jennifer Stoddart and Commissioners from Germany, New Zealand, the Czech Republic, and Estonia (Cavoukian, 2013a).

Since then, the PbD has been organized in nine application areas and translated into 37 different languages (Privacy by Design, 2014). According to Cavoukian (2012), the key application areas in which the PbD research is currently directed are:

1) CCTV/Surveillance Cameras in Mass Transit Systems;
2) Biometrics Used in Casinos and Gaming Facilities;
3) Smart Meters and the Smart Grid;
4) Mobile Devices and Communications;
5) Near Field Communications (NFC);
6) RFIDs and Sensor Technologies;
7) Redesigning IP Geolocation Data;
8) Remote Home Health Care; and
9) Big Data and Data Analytics.

Previous PbD research, however, has not been focused on education. Some studies have been done with the focus on mobile communications technologies, but there was no specific focus on mobile learning. Those studies examined the design and architecture of Mobile Location Analytics (MLA) (Cavoukian, Bansal & Koudas, 2014), Near Field Communications (NFC) technologies in mobile devices (Cavoukian, 2011), and the privacy practices for mobile devices (Cavoukian & Prosch, 2010; Cavoukian & Weiss, 2012; Cavoukian, 2013b). The purpose of every paper published by Cavoukian in this

field was to produce guidelines or a set of practical steps that could be taken by all players in the industry (e.g., device manufacturers, operating system and platform developers, network providers, application developers, and users) to build-in privacy protections and make the design of mobile technologies safer and more user-centric.

2.3.3. Criticism and Challenges of PbD

PbD is not a theory that can be used in academic research to develop and test hypotheses. It is considered to be a guideline that can be used as a practical tool to establish ethical business practices with the user privacy in mind. Even though PbD is often referred to as a "conceptual framework", it is actually a set of seven principles that don't have relationships between each other or influence each other in any way. For this reason, PbD cannot be applied in constructing and testing theoretical models, i.e., it cannot be applied for making predictions in any industry or area of research.

Despite the theoretical shortcomings, PbD is still considered one of the most comprehensive guides for embedding and protecting user privacy across different areas in our Digital Age. The unique value of this approach is that it recognises the importance of embedding privacy in operations and technology to protect the users and not only the companies. However, PbD has flaws and limitations in the way it suggests to embed and protect privacy.

While the critics of the PbD do not say that the approach is bad or wrong in any way, they point out that PbD cannot be implemented because the framework lacks practical and feasible methodology of implementation. The most common criticism towards PbD in the literature is that the 7 Principles of the framework are too vague (Cürses et al.,

2011; Spiekermann, 2012) and don't elaborate on how privacy can be embedded into systems from an engineering perspective (Cürses et al., 2011; Birnhack et al., 2014). Previously cited in this thesis articles by Ann Cavoukian describing the methods of application of PbD in different areas of business and technology do not provide specific technical steps on how to implement PbD, and only suggest managerial initiatives. This is likely the reason why Birnhack (2013) calls PbD "a legal attempt to shape technology" (p.30), suggesting that there is a difference between understanding the technology from the regulatory and from the engineering perspectives; and that in order for PbD to be effective, the framework has to present a deeper understanding of the technical aspects.

Spiekermann (2012) asserts that PbD faces some challenges even if managers and engineers work together to provide more specific and technical guidelines of how PbD should be applied. She identifies three concerns:

1) Privacy is a poorly defined concept and is often confused with security; to protect privacy, all the actors have to know what exactly they are trying to protect.
2) There is no "agreed-upon methodology [that] supports the systematic engineering of privacy into systems".
3) There is a lack of information on what are the benefits and risks "associated with companies' privacy practices". (Spiekermann 2012, p.38.)

Mulligan and King agree that a tool that could help in "translation privacy into design" does not yet exist (2014, p. 982). They argue that before developing any methods of embedding privacy as a default setting, the regulators should ensure that their methods are economically sound and that companies would be able to afford developing

solutions with the desirable forms of privacy protection (Mulligan & King, 2014). From the review of the publications promoting PbD and from the 7 Principles of PbD it is unclear whether this framework considered the financial aspect at all when developing recommendations for companies.

It is important to note that none of the critics dismiss the PbD as a valuable framework completely, but they strongly establish that there are certain weak points in the PbD approach and it needs further development and improvement. There are new technological advances and tools being developed every day; it is hard for regulators to stay on top of the innovations and to provide methods for protecting privacy for the tools and products that go through their technological life cycles faster than their potential effect on privacy can be discovered. PbD is an example of policymakers recognising "the power of technology to not only implement, but also to settle policy through architecture, configuration, interfaces, and default settings" (Mulligan & King, 2014, p.992).

2.3.4. Applying PbD Principles to App-Based M-Learning

There are no recommendations available specifically for mobile learning applications, but Cavoukian & Prosch (2010) developed a set of requirements for all mobile application developers in general. These requirements or recommendations for implementing PbD include the following actions and tasks that mobile app developers should undertake (adapted from Cavoukian & Prosch, 2010):

- Inform users about how they use their data and provide timely notices about any changes.
- Employ informed consent if they gather any personal information from the users.

- Utilize appropriate security practices.
- Practice data minimization techniques: do not collect more information from the users than needed for the app to function and to provide good user experience. There should be "collection limitation" and it should be specified for what purposes personal information is collected.
- App developers should protect the personal data they collect throughout the entire lifecycle of the data – from data collection stage, to data use and storage, and until these data are no longer needed and should be destroyed.
- All the security practices implemented by the app developers should be clearly documented.

One of the objectives of this research was to examine if PbD can help the developers design m-learning apps that protect their users' privacy. As can be seen from the summary recommendations outlined above, PbD provides steps of *what* has to be done, but not *how* it should be done. This example supports the previously expressed concerns by some researchers (Cürses et al., 2011; Spiekermann, 2012; Birnhack, 2013; Birnhack et al., 2014) that PbD is currently not mature enough as a model to be successfully implemented because it doesn't provide any practical tools or methods to achieve Privacy by Design. PbD framework could work as an ethical guide for managers, but it needs to evolve methodologically to become useful and practical for engineers and software developers.

Nonetheless, based on PbD Principles at their current stage of maturity, I developed some guidelines for the review of m-learning applications in this research. Based on the

actions that PbD suggested for the app developers to take, I composed several questions that had to be answered during the review of the m-learning apps' privacy policies:

- Does the app have a privacy policy or make its privacy information available for the users in any way?
- Does the app ask for the consent to collect user information?
- Does the app notify the users about the changes in privacy policy or any changes in the use of personal information?
- Is it possible for the users to opt-out from sharing their information with the app?
- Is there enough transparency in communication privacy information to the users?
- Is there any explanation of how the personal data is used and for what purposes?
- Is it explained how the user data is protected? Who can access personal information that users share with the app?

These questions helped to identify *red flags* in the way some applications communicate privacy information to their users. Chapter 4 present the results of this examination of the m-learning apps' privacy communications. Further application of PbD in app-based m-learning will be explored in Discussion part of this thesis (see Chapter 6).

Chapter 3 – Methodology

3.1. Methodological Approach

Both secondary and primary data were collected for this research. A quantitative method was applied to collect primary data. These data were collected by administering an online questionnaire. The research was approved by the Ryerson University's Research Ethics Board (REB) (see Appendix C). The survey study involved minimal risks to the participants and was not experimental in nature. Section 3.3 presents the design and procedure for the survey instrument. The secondary data included reviews of the academic publications, white papers, media articles and reports, government policies and other publicly available materials. In addition, secondary data such as applications' privacy policies and terms of conditions were reviewed for the investigation on what mobile learning apps do with their users' information. This review helped in designing a survey for the collection of primary data. The next Section 3.2 explains the methodological considerations for collection and analysis of the secondary data.

3.2. Selection Criteria for the Apps for Privacy Policies Review

I selected the apps presented in this chapter without using any special software to find the relevant applications and information on them. As pointed out by Maske et al. (2011), no m-learning application dominates the market, because there is a lack of standards for m-learning app development. With more than 1,600 new apps being added to app stores on a daily basis (Article 29 Data Protection Working Party, 2013), it

was difficult to manually process all the apps that are self-described as m-learning or mobile learning applications and select those which are relevant to the scope of this study. A representative sample of various apps targeted at adult learners was selected. These apps were included in the review because of their diversity in subject matter, developers, target consumers, prices and platforms. Table 3-1 (at the end of this section of the thesis) provides a summary of the basic inclusion and exclusion criteria for the m-learning apps that were selected for analysis.

This research is focused primarily on the interactive m-learning applications. The "Information source" apps (see Chapter 1 for definition) are not covered in this study, because they are not interactive and hence do not fall under the category of m-learning applications as defined in this thesis. The referential tools and the info-libraries are not included in the review as well, because they can also be classified as the "information source" tools.

Arguably, apps that have only video content or present animations, or deliver materials in form of eBooks or any other downloadable content, can be considered mobile applications for the purpose of learning. However, there are too many of such systems currently available on the market and they often do not require their users to actively engage in the learning process. These applications also trigger fewer privacy concerns, because the users are not asked to upload their own files for assessment or to engage in online discussions with other learners or course instructors. Therefore, to make the research narrower and more specific, any m-learning apps that solely present information and do not facilitate collaborative learning were disregarded. Only m-

learning apps that offer users a possibility of self-assessment or checking their progress were reviewed.

In addition, a few of the Learning Management Systems (LMS) available for mobile devices and app-based mobile learning platforms were included. A Learning Management System or LMS is a software application used for the delivery and management of the learning content and resources. An LMS usually allows for the learner registration, the delivery and tracking of the courses or training programs, and also for student testing. (Training Force, 2014.) Most Learning Management Systems (LMS) are designed for desktop computer or a laptop and often don't cater content for mobile devices such as smartphones, which is why only a small number of LMSs are included in this study.

The iTunes University app (iTunes U) was included in the list of LMS applications even though it is a *course management system* rather than a *learning management system*. The difference between such systems is that usually LMSs are more interactive and support collaborative learning and communication with course instructors. At the time when iTunes U was first launched in 2007 (Apple Press Info, May 30, 2007), it provided nothing more than some open-source course materials (e.g., videos, lecture transcripts, audio files, reading materials, etc.) from different universities. However, today the users of iTunes U can take self-assessment tests to check their progress and understanding of the material. Many courses now also provide various assignments (as homework) for the users to apply to a practical task what they learnt from lectures. For these reasons, it was decided not to exclude iTunes U app from the review.

Similarly to LMSs, most MOOCs are primarily web-based learning tools. The review includes only application-based solution. Some MOOCs such as Coursera have recently released apps for iOS and Android devices, but since those apps weren't initially designed as mobile learning solutions, they were not reviewed for this study. MOOC apps have yet to be developed and redesigned to cater for mobile users.

The selected sample originally included 56 apps, but was narrowed down to 28 due to similarities between some of the apps and because of the lack of interactive features or low popularity of the excluded apps. In October 2014, I was contacted by some representatives of the learning management systems that were competing for the contract with the Ryerson University to replace Blackboard that is currently implemented for the university. These companies had no impact on the study and just expressed their interest in the results of the survey research. After some consideration, I decided that some of the companies competing with Blackboard have to be included in the review, provided that they had a good application available for mobile devices. Thus, a total number of the apps included in the study was 31. 10 of those apps were LMSs.

Table 3-1: Inclusion and exclusion criteria for the m-learning apps for review

Inclusion Criteria	Exclusion Criteria
• App-based solution • Interactive • Provide an option of checking learner's progress / Has assessment feature • Apps that are available for download for free or should be purchased – both of these categories had to be included • Available for download in Canada	• Web-based mobile learning solutions (don't have an application) • Apps that are targeted only for little kids • Apps that just present information and have no interactive features, don't actively engage student participation in a course • Apps with very similar contents • Not available in English

The results of this stage of the research are presented in the Chapter 4 of this thesis.

3.3. Quantitative Study

3.3.1. Target Population and Sample

The target group for this study was adults over the age of 18. There were no specific exclusion criteria other than age. The population of interest included people of any gender, any educational background, and any occupation. As defined by the purposes of this study (see Chapter 1), both current users of the mobile learning applications and any potential or prospective users had to be included in the research, which broadened the potential participants to include any adult, anywhere in the world, with access to the survey. Though the research was not catered specifically for Canadians, more than 70% of the participants were residents of the province of Ontario.

The participation in this research was voluntary and anyone who had a link to the survey could participate, which is why it was hard to determine a specific sample. Non-probability or convenience sampling was used for this study. The participants were self-selected volunteers, which raised the possibility of undercoverage and voluntary response bias in this survey study. A pilot study was conducted to minimise the potential biases.

The participants were recruited via email and social media. I had access to the contact list of the Privacy and Cyber Crime Institute of the Ryerson University, which included about 6000 subscribers (although I don't know how many of those 6000 email

addresses were still active at the time of the research). The subscribers of the Privacy and Cyber Crime Institute were mostly students, faculty and staff of the Ryerson University, some technology journalists, and associates of the Institute. Considering that the subscribers of the Privacy and Cyber Crime Institute might be generally more apprehensive about privacy issues than other people, it was not specified that the focus of the study would be on privacy concerns. This was also done in order not to lead the participants and to counter response and sampling bias.

The survey was also distributed through Twitter, LinkedIn, Reddit, Google+, Facebook and Couchsurfing. In addition, I also asked my colleagues, peers and friends to share the link with their contacts, which is why it would be hard to estimate how many people in total saw the invitation to participate in the study.

The sample size was 260 participants. According to Alvin C. Burns and Ronald F. Bush (2014), I calculated the margin of error for this sample and confidence level 95% using the following formula:

Margin of sample error formula

$$\pm Marginof SampleError = 1.96\times\sqrt{\frac{p\times q}{n}}$$

In this formula "n" is our sample size, and both "p" and "q" stand for the variability in the responses to any given question of the survey.

The values of "p" and "q" should always sum to 100%. Burns and Bush (2014, p. 242) explain that "[a] 50/50 split in response signifies maximum variability (dissimilarity) in the population, whereas a 90/10 split signifies little variability." Since the target demographics include everyone above the age of 18, there is a possibility of significant differences in the responses. Hence, to calculate the maximum margin for sampling error, we should assume that both "p" and "q" stand for 50%. As a result, the margin of sample error in this survey research would be ±6.07%.

$$\pm Margin of Sample Error = 1.96 \times \sqrt{\frac{50 \times 50}{260}} = 1.96 \times \sqrt{\frac{2{,}500}{260}} = \pm 6.07$$

In conclusion, at a 95% confidence level, there is a margin of error of about ±6% in the sample results. This means, for instance, that if 45% of people sampled answered that they were familiar with m-learning applications and used them before, we can be confident that between 39% (=45% - 6%) and 51% (=45% +6%) people in general have tried using mobile learning applications (considering that the margin of error is plus or minus 6%).

3.3.2. Survey Design

The pilot questionnaire was composed of 28 questions and took approximately 20 minutes for the respondents to complete. Suggestions from other researchers and Ryerson University faculty also helped to compose questions to avoid leading the participants and reduce the researcher's bias. Administrating a pilot survey helped in determining whether the participants were able to follow instructions, whether the

questions were phrased clearly enough for the respondents to understand, and whether there are any errors previously unidentified by the researcher.

The results of the pilot questionnaire helped to determine which questions were more important than others for the purposes of the research. The respondents of the pilot questionnaire were able to leave comments in the text box answer options for some of the questions. The participants of the pilot study left comments regarding several questions, suggested additional answer choices and/or rephrasing. These comments provided a valuable feedback for improving the survey. The survey was redesigned to take 10 minutes instead of 20 minutes.

The final survey used to collect the data included 21 close-ended and partially structured questions: fixed response questions with a possibility for the respondents to add their own answer or opinion in the "Other" text-box reply options. 7-point Likert scale rating questions were used to find out how respondents feel about particular issues and to find out about their concerns regarding the use of mobile learning applications; whereas 5-point Likert scale questions were used to determine some of the usage patterns, such frequency of use of the m-learning apps, user familiarity with the apps, etc. Most of the 5-point Likert scale items were deleted from the final questionnaire, because the pilot survey revealed that those questions do not contribute to the research purposes and have no impact on other variables. After all the changes and improvements of the survey design were made, the average completion time for the survey became 10 minutes.

The online survey site was set up using FluidSurveys survey software tool[2], which is a multi-lingual survey tool that supports multiple different question types and has an option of custom formatting and editing. Using this survey instrument, I was able to create multiple-choice questions, closed-ended dropdown menu questions, open-ended text questions, checkbox questions (to allow respondents select multiple answers per question), and multiple choice grid questions (to present many variable in one question in a table).

There were no significant physical, psychological, social, economic, or legal harm that could result from the participation in this research. This was a simple minimal risk research protocol. The only minor risk associated with this study was the possibility that the participants could feel fatigued or inconvenienced as a result of taking the survey.

The questionnaire asked personal information such as age, gender, whether the respondents were residents of Ontario or any other area in or outside of Canada, and what were the occupations of the respondents. Despite those questions, no personally identifiable information (e.g., names, addresses, email addresses, etc.) was collected. Moreover, the respondents had a possibility to not provide the answers for those questions by choosing a response option "Prefer not to answer". The respondents' age, gender and level of education, and their use of m-learning applications (have or have not used before, frequency of use) were used as control variables in contingency tables with the other study factors.

[2] FluidSurveys website: http://fluidsurveys.com/

Apart from the questions that collected the basic demographic information about the participants, the survey included questions that were set to investigate user privacy concerns, attitudes toward m-learning applications' user data collection and third party sharing, and the usage patterns of m-learning apps. Those questions were divided into four categories and mixed in the questionnaire (presented to the participants in non-consecutive order) to avoid getting the participants focused on some particular concerns, avoid leading them or suggesting opinions, and to keep them from getting bored, fatigued or irritated with long questions. Each of the survey study factors included up to seven questions, because, according to Chong et al. (2011), having more than one question asked for each factor is important for reducing response bias.

Survey item selection was primarily based on the information collected from the review of the privacy policies of the m-learning applications. Some questions included more than one variable (see all of the survey questions with the answer choices in the Appendix F). For instance, questions 10-13 included up to 11 variables to explore the importance of different m-learning apps' properties or features for users and the levels of users' concerns about the apps' abilities to access different types of personal information. The purpose of these questions was to find out how users feel about sharing different types of information about themselves and their app usage with the app developers and any possible third parties. The full list of variables included in the survey research can be found in the Appendix G.

3.3.3. Procedure

The participants were not identified or specifically selected for the study. There was no compensation or payment for the participation in this study. The participation was voluntary and anonymous.

The pilot survey was deployed on July 31st, 2014. The survey was live (i.e., open to collect responses) for 13 days from July 31st to August 12th, 2014, inclusive. 207 adults over 18 years old agreed to participate in the pilot study, but only 123 of them completed the questionnaire. The outcomes of the pilot study revealed the need to modify and shorten the survey. I reviewed the comments from the pilot study participants and made changes in the survey design. The full-scale survey was deployed on October 16th and collected responses until December 10, 2014. Clear instructions were provided for the participants of the study in the beginning of the survey.

Participants were asked to give their informed consent to participate in the study. The participants were not asked to provide any personally identifiable information. The intentions of the survey data collection were explained in the consent form provided prior to the survey questions, to ensure that the respondents understood the objectives of the study and what would be asked of them. The participants were able to withdraw their consent to participation at any stage of taking the survey by closing the browser tab with the survey link. All the recruitment materials and the Consent Form for the participation in the study were scripted to comply with the 2nd edition of Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans[3] (TCPS 2).

[3] Full text of the TCPS 2 policy is available here: http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/Default/. Last accessed on November 29, 2014.

The link to the survey was not unique for the email addresses in both the pilot and the actual survey: anyone could share the link to the questionnaire and the results could not be linked to any particular respondent in order to preserve anonymity and confidentiality of the participation in this study. The responses were submitted electronically through an online survey administrator and not through an email.

The raw data collected through the online survey software were exported from FluidSurveys to Excel on December 11th, 2014. Next, the data were entered into SPSS Statistics 22, coded and prepared for analysis (a cleaning process and close examination were performed). Thereafter, the results of the survey were analysed in SPSS to find any relationships or apparent trends that could lead to some conjectures, generalizations, or the development of testable hypotheses. The results of the survey study are presented in Chapter 5 of this thesis.

The collected data are securely stored on my personal laptop computer and will be retained for a year after the research completion. As was previously mentioned, the data cannot be linked to the individual participants of the study and no personally identifiable information was collected. Nonetheless, I encrypted the files with the collected responses to prevent unauthorised access.

Chapter 4 – M-Learning Applications and Their Privacy Policies

The privacy policies and Terms of Use/Service (ToS) of 31 m-learning applications were reviewed for this study. As was mentioned in the previous chapter, eleven of the reviewed applications were LMSs. Table 5-1 presents a list of mobile learning apps reviewed and the results of the review including the types of the data they collect, store and share about their users; as well as the applications' prices and user ratings. The user ratings can change between the different app versions and for different OS or devices (iOS and Android apps may have different ratings due to differences in the designs), which is why the average user ratings for all versions of the apps are presented.

Given that privacy legislation and related laws vary across the world, the developers home country was specifically noted. In some cases the data collected from the users is protected and shared according to the regulations of the countries of the apps' developers and not the location of the users.

While it would be logical to assume that m-learning apps from different countries may define personal information differently in their privacy communication to the users, a review of the privacy policies suggests that the language used in such documents is similar regardless of where an app was developed. Terms such as "personal information" and "aggregated non-personal data" were used in almost every privacy policy. American developers avoided using the popular (in the USA) abbreviations "PII"

and “Non-PII”, which may be explained by the developers’ intentions to target audience outside the USA and/or to make the language of the privacy policies easier to understand by not using specialized, industry-specific terms.

This and other information was gathered about the applications to create a comprehensive profile and to identify possible patterns or relationship. However, no apparent relationship between the apps’ sizes, prices, ratings, target markets, or subjects and the privacy policies of the apps have been observed. In general, most of the applications had quite similar policies that were obviously phrased to protect the interests of the developers and providers rather that the users. None of the policies specifically identified which third parties had access to user information, and the information gathered was defined quite vaguely and could potentially be much more broad than the users might suspect.

When this research was originally conducted in May 2014, 13 or 42% of the 31 applications included in the review did not have a privacy policy at all, which is an alarming number for such small sample. However, in January 2015 all of the applications were reviewed again for changes in their privacy policies and/or how they communicate privacy information to the users. By that time only 7 apps (or 22.5%) from the original list still did not provide a privacy policy to their users, a decrease of almost 50%.

Among those apps that had a privacy policy, most did not have it available within the mobile app, but required their users to find the website of the application provider or the developer to access this information. This creates unnecessary obstacles for the

customers who should not be forced to search for these documents on the internet or contact a company directly for this information. Documents such as privacy policies and terms of service should be easily and immediately accessible for all users.

Based on user-accessible privacy policies and terms of use, it was found that m-learning applications presented in the sample collect all or most of the following data from their users:

- **Registration data:** usually includes a user's name and email address, and occasionally other personal details such as mailing and billing addresses, phone number, business information, etc.
- **Shipping and billing information:** shipping and billing addresses, credit card number and expiration date.
- **Aggregate data:** aggregated non-personal data usually includes information about usage patterns such as the frequency of application use, nature of inquiries, etc. It is usually collected to find out how the app is being used and determine how it can be improved based on this information.
- **Transmission data:** the information regarding what content a user sends through the app and whom he/she sends it to.
- **Log data or the app and the site usage information, if some content is available via browser:** the information about a user's browser, domain name, IP address, the web pages he or she visits and how much time is spent on every webpage. This information is usually not linked to the users personally, but considering that the IP addresses are retained, we can argue that an individual can be identified via this information.

- **Device information and unique device identifiers:** *e.*g., operating system, IP address.
- **Permissions (default only for Android apps) that may include:** user contacts (may include the name and addresses of contacts external to the application, or only those contacted via the application itself); calendar; messages; photos, and so on.
- **Cookies** or other passive tracking mechanisms may be used if the application is accessed via a browser (there are no cookies within apps on mobile devices). Cookies cannot access personal information by themselves or access files on the user's device, so their privacy risk is limited. However, cookies are used in ad tracking and may store data entered by the user and data about user activities, which can be considered a form of personal information. (AllAboutCookies.org, 2014.) In this study, cookies were not regarded as a considerable privacy threat to the users of m-learning apps because most cookies are browser-based and this study focuses on native apps.

The review of the privacy policies revealed not only specific types of data collection and tools for doing the collection, but also outlined some instances of how data can be stored, managed, and resold. The most common aspect of data management relevant to a privacy-conscious user is a **business transfer**. According to the reviewed policies, the companies may sell, transfer, or otherwise share some or all of their assets in connection with a business transaction, merger, reorganization, or in the event of bankruptcy or selling their company to another entity. When this happens, the users' information is usually regarded as one of the assets transferred. Some applications take the responsibility for notifying their users in case of business transfers and consequent transfer of the user data to another company. However, some may transfer or sell user information without notice, in which case users would not be aware of the business

transfer. Only 4 out of the 31 companies included in the review mentioned in their privacy policies that they would notify their customers in case of business transactions when they have to provide some other party with all the users' PII and Non-PII (e.g. when a company enters bankruptcy, is acquired by a third party, or in case of a merger).

It was often specified in the reviewed privacy policies that an application may collect any personal or demographic information from their users if the users provide such information *voluntarily*. This is a misleading phrasing, because users of those apps have to provide personal information to register for these services, and they can't use the service without prior registration. Opting out from providing any personal information means you cannot use the application, which is not the same as making a choice between not providing any personal information to the app and voluntarily sharing some information while already being a user. A note on this is most explicitly written in the Privacy Policy of Qualcomm (provider of QLearn LMS), which has a special section "Opting out" with the following explanation on how users can opt out from providing their personal information to the app:

> *"You can stop all collection of information by the Apps by uninstalling the Apps."* (QLearn Privacy Policy, 2014).

In other words, if learners want to protect their privacy using m-learning apps, they have only one choice – not to use m-learning application at all. This is not a choice but rather an ultimatum from the service providers, as it forces users to provide whatever information is asked of them if they want to use the service/tool. Users are offered no granularity in the control of their own personal data. Knowing that some learners

cannot opt out from using the tool no matter what (e.g., some apps might be obligatory for university students or for some employees to use as part of their course program or professional training), the applications' providers can exploit their advantageous position and start collecting and sharing any of their users' personal information for any reason without notice. Currently, there is no penalty for such behaviour, and the providers can always say that the users could have protected their information by refusing to use an application.

In fact, we cannot know the extent to which the applications collect and share user data, because there is an obvious lack of transparency in every privacy policy. The third parties who are given access to the users' information are never explicitly named. Every privacy policy lists the circumstances and the reasons for sharing the user data with these third parties, but it is also clear that a "third party" could be basically anyone.

On a positive side, it was interesting to note that the reviewed m-learning applications do not directly monetize their users' information with third parties for unrelated marketing purposes. Although they do share user information with third parties to market their own products. This phrasing is somewhat controversial and tricky.

Table 5-1: Sample of M-learning Applications and What User Information They Collect and Share.

no.	App	Developer, country	Study field or courses	Target user	User rating (out of 5)	Price	Designed for	Information they collect	Information they share
Interactive mobile apps with the learning content									
1	NCEA Algebra	NextLevel Apps, New Zealand	Algebra	Secondary school, New Zealand	5	$1.75	Android	**No Privacy Policy available for users to read**	
2	Algebra Tutor	Shane Fulmer, USA	Algebra	All ages	4.1	Free	Android	**No Privacy Policy available for users to read**	
3	Mind-Snacks	MindSnacks Inc., USA	Languages	All ages	4.5	Free	iPhone, iPad	They collect personal info that users provide; aggregated data; cookies.	- May share personal data with the authorized third parties located in the United States. - May share this non-PII and aggregate data with its affiliates, agents and business partners, and to other third parties for lawful purposes.
4	Gidimo	Gidi Mobile Ltd, Nigeria	Various	Africans under 25	4.6	Free with in-app pur-chases	Android, Nokia, Blackberry	- User contacts; - Transmission data; - Cookies; - Aggregate Data; - Location (collected without association with the user individually)	- Location information with any third parties. - Aggregate Data – with vendors and affiliated companies. - End user info – with the governmental authorities. - Business transfers.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
5	Math	Classmate L.L.C., USA	Math	5th grade to college	4.5	Free installation with additional in-app purchases	iOS	- Gather PII when users contacts the developers by mail, phone, e-mail; visit their website; or fill out requests for information through the advertisements and promotions; and subscribe to newsletters. - Collect personal information provided by users: name, address, phone number, e-mail address, responses to specific questions (e.g., interest in math and math test preparation services), shipping and billing information. - Gather site usage information and information collected via cookies.	Use non-PII for internal business and marketing purposes, and share such data with third parties, including current or potential business partners. Use PII for billing purposes, to respond to consumers' requests, to provide consumers with special offers, and to notify consumers of new product launches, to personalize user experience and to recommend products May provide user's name, address and telephone number and email address to independent third parties unless a user asks not to disclose this information.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
6	Map-Master	droidplant, USA	Geography	All ages	4.5	$1.22	Android	The app does not collect PII (doesn't collect information such as a user's name, address, phone number or email address). Doesn't collect, use, store or share information about the users' location. Doesn't knowingly contact or collect personal information from children under 13.	MapMaster uses Google Analytics to collect Non-PII in the form of various usage and user metrics when people use their application.
7	Perfect Chemistry	RanVic Labs, USA	Chemistry (quiz game)	All ages	4.5	$1.01	Android	**Privacy Policy and Terms of Use aren't available anywhere to read**	
8	Nature's Notebook	USA National Phenology Network, USA	Biology	Grades 4 – adult	3.5-4.5	Free	iPhone, Android	Collect any information the user shares with the app or uploads on their website.	They don't sell, trade, or give away personal information, which includes a user's name, home address, e-mail address, telephone numbers, and suggestions or comments made by e-mail; But they may share any PII with anyone if this PII was uploaded by the user to their system.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
9	Lumosity	Lumos Labs, Inc., USA	Memory and attention training	All ages	4	$14.99 per month or $79.99 for a subscrip-tion for a year	iPhone, iPod touch, iPad	Automatically collect and store information about the computer, mobile device, or other devices used to access Lumosity and about how their users use Lumosity	- Share PII with third parties to help support business operations, market or advertise Lumosity. - May share user information with Lumosity's corporate affiliates, such as entities under common ownership or control. - Business transfers. Share PII in compliance with law and law enforcement requests, and protection of our rights.
10	Computer Science App	Nikhil A.P	Programming languages; Software Engineering.	All ages	3.9	Free	Android	**No Privacy Policy available for users to read**	
11	Celeste SE	Terminal Eleven LLC	Astronomy	All ages	4	$1.95	Android (but does not work on Samsung Galaxy)	Don't use cookies and don't collect info from anyone under 13. No other information on what they collect from their users is provided.	- Don't share PII with third parties, except with those who help in their product/systems development and who consent to keep user PII confidential. - Share any info when they need to comply with the law or protect their interests. - Share Non-PII with third parties for marketing, advertising or other use.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
12	Themis Bar Review	Themis Bar, USA	Law	Adults	3-4	Free	iOS, Android	Registration information and info via cookies.	Do not reveal PII to third parties for their independent use unless: (1) user requests or authorizes it; (2) the information is provided to help complete a transaction initiated by the user; (3) the information is provided to a user's law school; or (4) the disclosure otherwise is lawfully permitted or required.
13	Project NOAH (Networ-ked Organisms And Habitats)	New York University & National Geographic, USA	Biology	Grades 4 – adult	4.5	Free	iPhone, Android	Collect aggregate data.	Don't sell users' email addresses, personal information, their words, or reuse them without the users' permissions except for promotional purposes or other campaigns within their own website.
14	TripLingo	TripLingo, LLC, USA	Languages	All ages	4+	Free	iPhone, Android	Keep personal data until the user deletes it. Collect device info.	Do not share or store precise geolocation data. Share user info when legally required.
15	Pec apps Adult Education Apps	Paul Coke	Literacy	Adults	N/A	$1.99	Android	**No Privacy Policy available for users to read**	

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
16	Rosetta Course	Rosetta Stone, Ltd., USA	Languages	All ages	4+	Free	iOS	The elements user information they collect may include: - Name; Job title; Company name; Home, shipping &billing addresses, phone & fax number; - Mobile phone number; E-mail address; IP address and browser information; Payment details such as credit card information; - Market research data such as customer usage patterns.	- Share user information in case of Business transfers; and in accordance with legal and regulatory requirements - Use information in aggregate form (so that no individual user is identified) to build up marketing profiles, to aid strategic development, and to audit usage of the site. - Sometimes let third parties set cookies on Rosetta Stone sites for market research, revenue tracking or to improve functionality of the site.
17	Every-Circuit	MuseMaze, USA	Teaches how circuits work	All ages	4.5	$10	iOS, Android	Collect PII, generic and aggregated information, and user log data	Share with third parties aggregated information that does not include personal information – for industry analysis.
18	Memrise – Learn Any Language	Memrise, the UK	Languages	All ages	4.5	Free	Android	Registration information; aggregated information; site usage & cookies information.	Publish and share with third parties aggregated data that does not include personal information – for research purposes.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
19	Biology, Kingdom of Organisms & Micro-biology	WAG Mobile Inc., USA	Biology and Micro-biology	All ages	3.5	Free, with in-app purcha-ses from $2.29	Android, iOS	The Privacy Policy can be found on the developer's website under the Terms of Use. They collect: - IP address, - browser and operating system information, - usage patterns information, - email address, month & year of birth of the users, their real names and other registration info, and additional PII that users may choose to add to their profiles; - payment verification info (credit card number); - any info posted by the users; - user information from Facebook and/or Google+ if a user connects these services to the app.	- Any info that users decide to make public in their public profiles can be accessible not only by other users of the app but in general by anyone. If users linked this app with their social networks' profile, then their activity and usage of the app are automatically shared with those social networks. - May disclose PII to service providers. - Aggregated Non-PII (usage statistics) could be shared with third parties and made publicly available. - Business transfers.
20	Geometry Pro	Larry Feldman, USA	Geometry	All ages	4+	$0.99, $1.04	Android & iOS	The developer has a note on his website that he "does not collect, request, store, or share any personal information or location data."	
21	Chemist	THIX, USA	Chemistry (virtual lab experiments)	All ages	4+	Free, $4.99	Android, iPad	**Privacy Policy and Terms of Use aren't available anywhere to read**	

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
LMS (Learning Management Systems)									
1 (22)	Edmodo	Edmodo, USA	-		3-4	Free	iOS	- Receive and store any information a user knowingly shares/enters on Edmodo services via any device; - Aggregate data; log data; transmission data; - Use cookies and web beacons.	- Use PII to customize services for the users; - Business transfers; - May share any info to comply with the law.
2 (23)	Black-board Mobile	Blackboard Inc., USA	*"Study Field" column is not relevant here, because they can include courses from any and all fields of study*	*The target users for all LMSs are usually higher education institutions or companies that provide online training*	2	Free academic access (if a school is subscribed to this LMS) or $1.99	iOS, Android, Black-berry	- Registration info; - App & site usage data – collected for marketing purposes; - Aggregate data.	May disclose aggregate data (non-PII) to prospective partners, advertisers, or for lawful purposes. They don't sell or share PII with third parties, except when they have a user's permission to do so or when they have to comply with legal process or to protect their rights.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
3 (24)	Skillport 8	SkillSoft Ireland Limited, Republic of Ireland The company complies with the US-EU Safe Harbor framework.	IT and business courses		N/A		Not specified anywhere	- Registration data & log data; - Use cookies; - Collect personal info about the users' personal and professional interests, demographics, past experience with Skillsoft, detailed contact preferences & other PII to improve Skillsoft offerings and promotional offers. - Have a chat service facilitated by some other unspecified third party & that party collects user information if customers use the chat.	- The info that a user submits on discussion board or forum is considered public and not confidential & can be shared with anyone, & not protected in any way. - May share PII with third parties to market Skillsoft products to its users. - Business transfers. - Don't sell, rent, lease or provide PII to third parties, unless required by law or have users' permission, & except above-mentioned cases.
4 (25)	CEU360.com	HomeCEU Connection, USA	Physical Therapy and Occupa-tional Therapy, Athletic Training, etc.	Corpo-rate health-care training for adults	N/A	Quote wasn't available	iPad, iPhone, Android	**Privacy Policy and Terms of Use aren't available anywhere to read**	

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
5 (26)	mTouch (Moodle)	Pragma-Touch, Turkey	LMS for higher education		2.5	$2.99	iPhone & iPod Touch	Non-PII information is tracked and recorder (usage patterns & IP address), but it's not specified if they share this information with anyone.	- They consider all info that users disclose in their public profiles, in forum posts, comments, tracker, or on the public portions of Moodle websites to be public info & it can be accessible to anyone. - Don't share or distribute personal information (including email address), but it may be accessible to those volunteers and staff who administer the site and infrastructure. - Share if required by law.
6 (27)	QLearn Mobile Education Platform	Qualcomm Technolo-gies, Inc., USA	LMS for higher education		5 (based on only one user review)		Android, iOS	- All PII received from the students and all the PII on the students received from their teachers. -Registration, log in data. -Cookies; browser info; IP address; device info.	-Share everything the Leaners upload publicly with their Teachers. -Don't sell users' personal information to any third party. However, will sell in case of a business transaction. -Disclose any information if required by law or to protect themselves or "others'" legal rights (don't specify who are those "others"). -Share users' PII with the company's business affiliates and with third party service providers.

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
7 (28)	iTunesU	Apple, USA	Open-source courses from various universities for everyone		N/A	Free	iOS	"We may collect, use, transfer, and disclose non-personal information for any purpose." (Apple Legal, 2014).	
8 (29)	Desire2Learn	D2L Corporation, Canada			3	Free	iOS	The privacy policy is not easily available for the reader. The company's Privacy Statement can be found on the web, but it's not easy to find it on their website, a user is redirected a couple times. Their Privacy Statement is contains a general description of their privacy practices across their different products. They also note that there might be specific rules for each country where they operate, but they don't elaborate on those differences. This Privacy Statement is too general and doesn't provide adequate information about what exactly is collected from the users and how their data is used. It is written that PII is collected (such as registration data), and it is stated that they may share PII with third parties so that those parties can contact users with marketing/promotional offers. It is also noted that a user can opt-out from receiving promotional offers and opt-in for sharing user data with independent third parties. Also, they don't knowingly collect information on children under 13. They may share any information for legal purposes if they "have a good faith belief" that it would beneficial for them or that it's legally necessary.	

no.	App	Developer, country	Study field or courses	Target user	User rating	Price	Designed for	Information they collect	Information they share
9 (30)	GoClass	Learning-Mate Solutions, USA			4	Free	iOS, Android	Any personal information provided to GoClass is stored securely, and used and disclosed only in accordance with the privacy policies and instructions of the educational organization with which the users are/were engaged. They do not use any personal information provided to them for their own marketing purposes.	
10 (31)	Canvas	Instructure, USA	LMS for higher education			Free	iOS, Android	-Collect registration and log in data. -Retain the following information on behalf of users: files and messages stored by users on their accounts. -Collect and store all content that users provide if they contact the app providers via e-mail. -May collect additional profile information if a user participates in a survey. -Any other types of personal information and demographic information that user provides "voluntarily". -Unique device identifiers -Cookies and web beacons	-Share data with service providers who host their websites or provide email services on Canvas' behalf. -Share any information with unspecified third parties to comply with the law; to protect Canvas' own legal interests; and "in an emergency to protect the personal safety of any person". -Business transfers. -"Share de-identified and aggregated data with others for their own uses" (Canvas' Privacy Policy, 2014). -Can share information with social networking platforms such as Facebook, but users can choose not to connect their account to social networks in the app settings.

In all the reviewed privacy policies it was stated that an application collects and uses their users' personal information *to improve their services*. While I agree that having some personal information on individual users can help in providing personalized user experience, it is not clear why an application needs to collect data on its users about anything beyond their personal preferences regarding the use of this application. For example, it is unclear why the developers of a mobile learning app need to know the users' IP addresses, their unique device identifiers, or business contact information to improve the service for those users. It should be explicitly explained to the users how this information is used to make the user experience better, if it is really the purpose of collecting such information to begin with. Only a couple of the applications profiled for this study elaborated in their Privacy Policy what they do to provide a "better service" for their users (Canvas and QLearn). I suspect that not all of the collected user data is required to maintain a good quality service and to provide a personalised experience, and that a lot of data is gathered not for the benefit of the learners, but to help the application in marketing their own services to the users and to third parties. A more in-depth inquiry on how the mobile learning applications' user data is utilized and manipulated by the service providers and developers can yield interesting insights and should be explored in the further research beyond the scope of this thesis.

All the applications included in the sample may share any user data with the government to comply with the legal processes. In fact, a privacy policy of almost every of the reviewed apps has an identical paragraph on this subject. Since the phrasing is similar, the following sentence should give a general idea to the reader about the content of such paragraph on legal issues:

> *We may release Personal Information when we believe in good faith that release is necessary to comply with the law (such as to comply with a subpoena, a court order, or a search warrant); enforce or apply our Terms of Service and other agreements; or protect our rights, property, or safety of our employees, our users, or others.*

One can argue that sentences phrased in such manner could release the apps' providers from any responsibility of keeping user data confidential.

Most of the developers warn that the users should use caution when deciding what information and content to share through their apps. They also add that if they provide links to the third parties' websites or apps on their m-learning application, they are not responsible if a user clicks on those links. It is also stated in ToSs that that the app's providers cannot guarantee the safety of user's information and cannot inform what type of personal information could be accessed by the party that the link belongs to, and how the user's data could be used by this party if the user clicks on the link provided by the developer. Simply put, the providers and developers wash their hands of the responsibility over the protection of the user information if a user follows the links suggested by the developer. Shifting a responsibility for the information protection to the users is not an optimal solution when it comes to designing a secure user-centric and safe mobile application for learning. The developers should avoid designing solutions that would direct the users to the untrusted third parties.

Generally speaking, all of the m-learning apps that had a privacy policy share user information with some third parties. We can assume that the apps that did not have an

explicit privacy policy or even a ToS, operate by the similar principles. The only difference is that the users have no way of knowing what information is being collected from them and how this information is stored, shared, and protected.

In conclusion, none of the applications reviewed were transparent about what information they collect from their users and how they use this information. This lack of transparency was manifested in different ways: 1) some applications didn't use clear language describing what they do with user information; 2) a couple of the apps had a redirection loop – Privacy Policies referred to ToS for more information, while ToS said that the information about user data collection can be found in the Privacy Policy, but neither of these documents provided any information on the issue; 3) some apps didn't make their privacy information easily available and some didn't provide it at all.

As was briefly mentioned in Chapter 2, in the spring of 2014, the GPEN Sweep took place and assessed 1,211 mobile apps (not only mobile learning apps, but also various types of applications for mobile devices). This sweep involved 26 privacy enforcement authorities from around the world, including the Office of the Privacy Commissioner (OPC) of Canada. 43% of the assessed apps did not tailor their privacy policies for small screens, which means that users cannot easily read these apps' the privacy information on mobile devices. The OPC examined 151 of the 1,211 apps and found that 26% of those examined don't have a presence of a privacy policy. (Cohen, 2014.) Based on this review, the OPC developed a 10-step guideline for the mobile apps developers and providers. The guidelines are broken down into three categories that suggest the developers to (A) be more transparent, (B) explain what they do with user information, and (C) make privacy policies accessible for users. These suggestions were composed to

help the providers present the privacy communications to their users in an accessible way, to achieve better transparency between the apps providers and the users, to gain user trust and implement better business practice. In addition, these steps could help the developers and providers comply with Personal Information Protection and Electronic Documents Act (PIPEDA). (OPC Fact Sheets, 2014.) The developers of the m-learning apps' included in the sample for the study in this thesis should take these recommendations under consideration as well. More detailed information on the OPC's recommendations can be found in Appendix B.

The review of the privacy policies and ToSs helped identify what information is collected on the user and in what cases and with whom this information, or a part of it, can be shared. This review clearly established that companies differentiate between PII and Non-PII, and collect these data for different purposes. This knowledge raised a question whether the users care for what purposes and, more importantly, what information exactly is shared and with whom. This was explored in the survey research discussed in the next chapter.

Chapter 5 – Results of the Survey Study

5.1. Data Preparation Process

As described in Chapter 3, data were collected from the respondents through an online survey tool over a period of 56 days. I used FluidSurveys online survey software to collect the data. After the data were collected, the raw responses of 267 completed questionnaires were exported into Excel for initial analysis. Next, I manually entered the raw data from Excel into SPSS Statistics 22 to create data file and data output for analysis.

The accuracy of the entries was checked several times by visually comparing the entries in the SPSS and the raw data in Excel, as well as by conducting a basic descriptive analysis within FluidSurvey, and then in Excel and SPSS to ensure that there were no discrepancies. The SPSS data file was also checked for mistakes such as out of range scores. Such mistakes were unlikely, because data was exported to Excel and then copied into SPSS from there; but the data file still had to be checked for common errors in the data entry.

Initially, 75 variables were created in SPSS Statistics 22 data file for 21 questions of the survey, because some questions investigated the respondents' view on several issues of concern. Two sets of separate variables were entered for two questions that allowed the participants select more than one answer choices. One of those variables was deleted after the visual examination of the dataset revealed that no one chose that answer

option (Answer "I don't know" for Question 9: "Which of the following features you hope/expect to see in m-learning application? Choose everything that applies."). Later, additional 2 variables were created to analyse demographic information provided by the participants. Therefore, a total of 76 variables were created for the survey analysis.

For the next step in the analysis, the data file was checked for internal respondent errors. There was the possibility that some respondents might click on the same response option for all the questions to go through the survey quicker. Three such questionnaires were found and excluded from further analysis.

Next, I examined the data for missing values. Initial examination indicated that most of the participants didn't skip many questions or provided an answer for every question of the survey. However, two questionnaires contained the answers only for the questions about the respondents' age or gender and residence, with all other values missing. These questionnaires were excluded from further analysis as they contained no data relevant to the study.

According to Dong and Peng (2013), there is no established standard in the literature on what proportion of missing data is acceptable: some researchers suggest 5%, while others assert that the results of the analysis can be biased if more than 10% of data is missing. Referring to Tabachnick and Fidell (2012), they make a point that patterns in the missing data have a greater effect on the results than the percentage of missing data in general (Dong & Peng, 2013). The dataset for this research was further analysed for missing values and two cases were found with more than 10% responses missing. These cases were examined closely and it was uncovered that the data were missing not at

random: it was obvious that the respondents skipped a set of questions for some reason (e.g., the respondents were undecided about their opinion on the issues, experienced fatigue or boredom, or were anxious to finish the questionnaire quicker). For this reason, these questionnaires had to be eliminated, which left us with 260 responses for the formal in-depth statistical analysis of the results.

5.2. Sample Profile

400 people agreed to participate in the study, but only 267 of them took the questionnaire and completed it, which indicates a completion rate at 67%. The average completion time for the survey was 10:09 minutes. As was discussed in the previous section, after the responses were entered in SPSS Statistics 22, the data were examined and cleaned, and 7 questionnaires were eliminated from the sample. Thus, the final sample for the analysis included 260 completed questionnaires.

Among the participants who chose to reply to the question about their year of birth (230 out of 260), the age range was 53 years, with the respondents of the survey being from 18 to 71 years old. The average age of the participants was 35. The majority of the respondents were between 25 and 34 years old (see Figure 5-1 below).

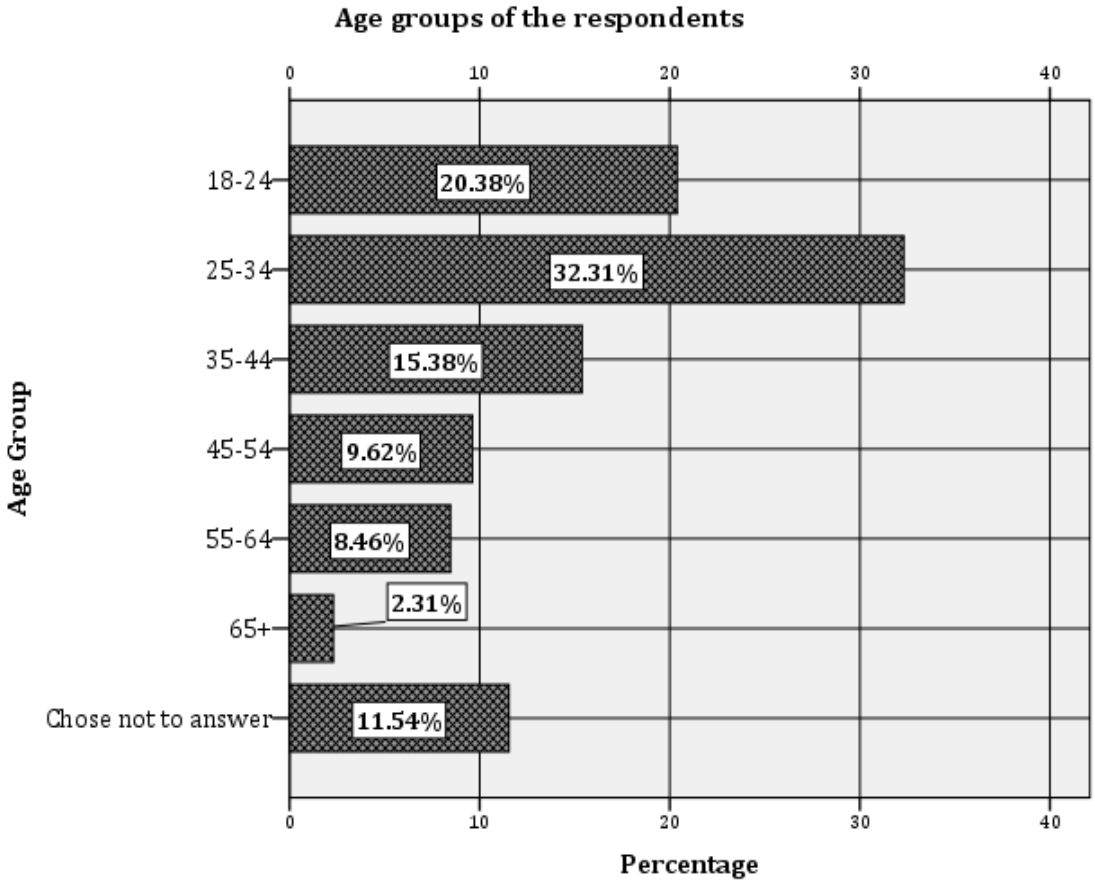


Figure 5-1: Age groups of the respondents

Among the 260 respondents 55.4% were female (N = 144), 42.3% were male (N = 110), two people chose “Other” response option (typed in “Genderqueer” in the response text box), and 2 more people or 1.2% of the respondents chose not to answer the question about their gender.

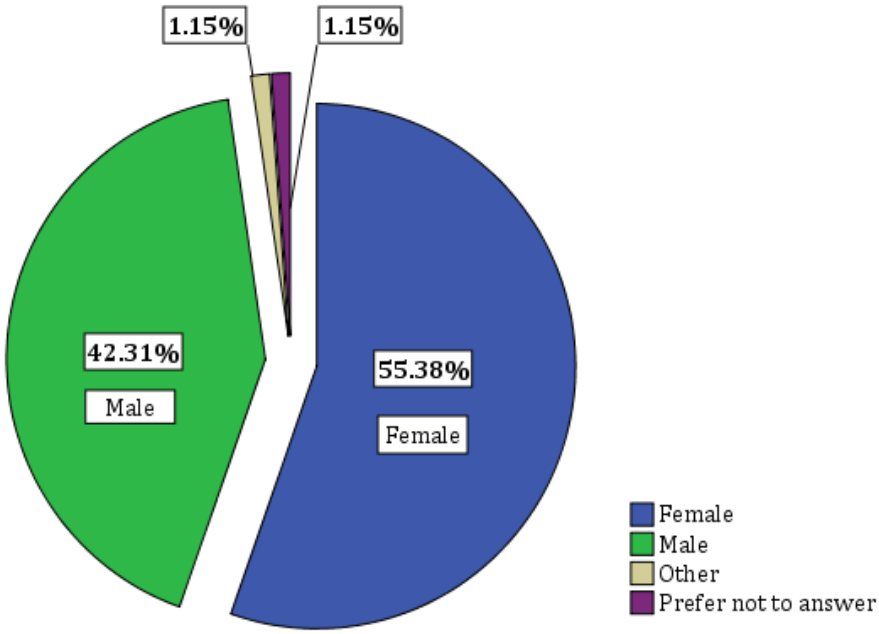


Figure 5-2: Gender of the respondents

Roughly 86% of the respondents had some post-secondary education (Figure 5-3). Some respondents selected "Other" in response to the question about their education and provided comments about their degrees/levels of education. Those comments included answers such as "LLM" (Master of Laws), "LLB" (Bachelor of Laws), "A-Level" (college equivalent in Wales, the UK), "Bachelor of Arts", etc. All those degrees could be classified between other categories provided in the answer choices: High School level, College, Undergraduate degree, Master's or equivalent, or Doctorate degree. Therefore, I changed the responses "Other" to the equivalent response according to the comments provided by the participants and the option "Other" was eliminated. The education levels of the sample can be seen in the Figure 5-3 below.

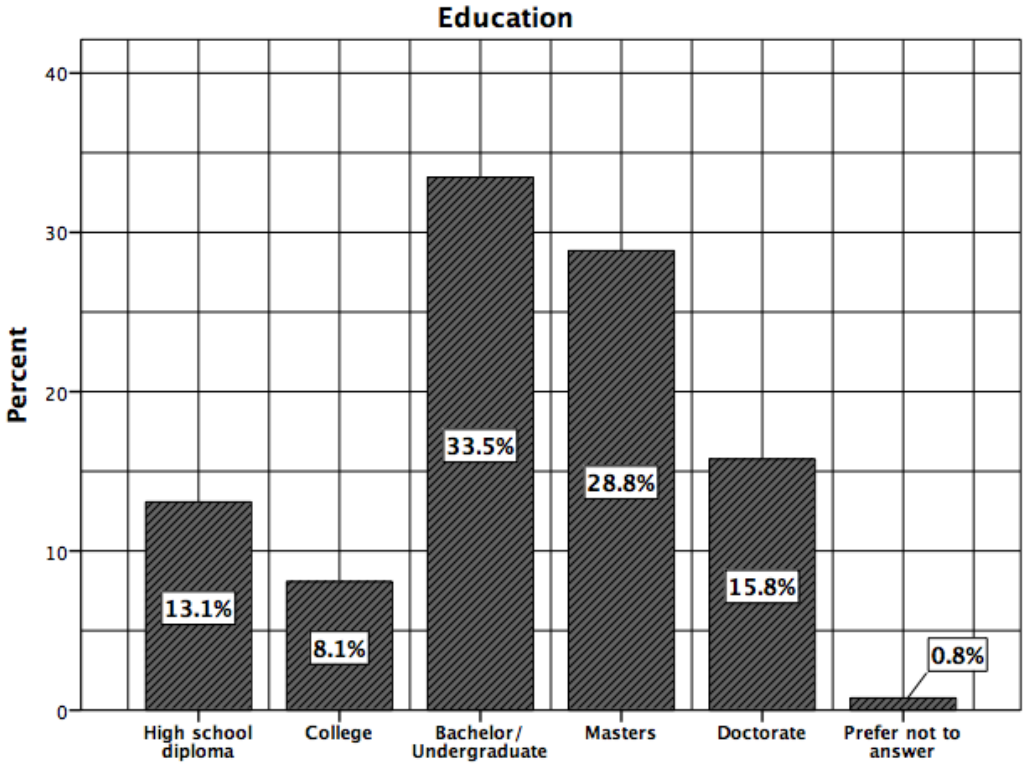


Figure 5-3: The level of education of the survey respondents

Almost 72% of the respondents (N = 187) were residents of the province of Ontario. 21.2% (N = 55) of the people who completed the survey indicated that they live outside of Canada with majority of those in Europe or in the USA.

90% of the participants left a response for the question about their occupation. Many respondents wrote that they are students (28.5%, N = 74), second most common occupation was some kind of teaching position or being a university professor or instructor (16.2%, N = 42). The third most reported job was a clerical or administrative position (10.8%, N=28). Other responses included engineering positions, different business and managerial positions, consulting jobs, medical professions, scientific research occupations, practicing law, working in media, and many other occupations. Appendix H provides a summary of the sample's demographic profile.

5.3. The Sample's Familiarity With M-Learning Applications

Among 260 participants, 117 people (45% of the respondents) said that they have used or are currently using mobile learning applications. 63 respondents (24%) were familiar with m-learning applications, but have never used them before. Almost 31% or 80 people responded that they were completely unfamiliar with such applications and have never used them. This means that only 45% of the participants were m-learning app users, while the rest of the sample can be considered potential users of such apps. Almost 70% of the participants knew about m-learning applications regardless whether they have ever used such applications (Figure 5-4).

When respondents were asked whether they have ever used m-learning applications, 55% responded that they have not; yet on the question about how often the participants use these apps only 48.1% (N=125) responded that they never use m-learning applications. This difference in the results indicates that there was some inconsistency in the participants' answers.

21.2% (N=55) of the participants replied that they use the m-learning applications at least sometimes, and 21.5% or 56 people said they use them rarely. Only 2% of the participants reported using m-learning applications "a lot".

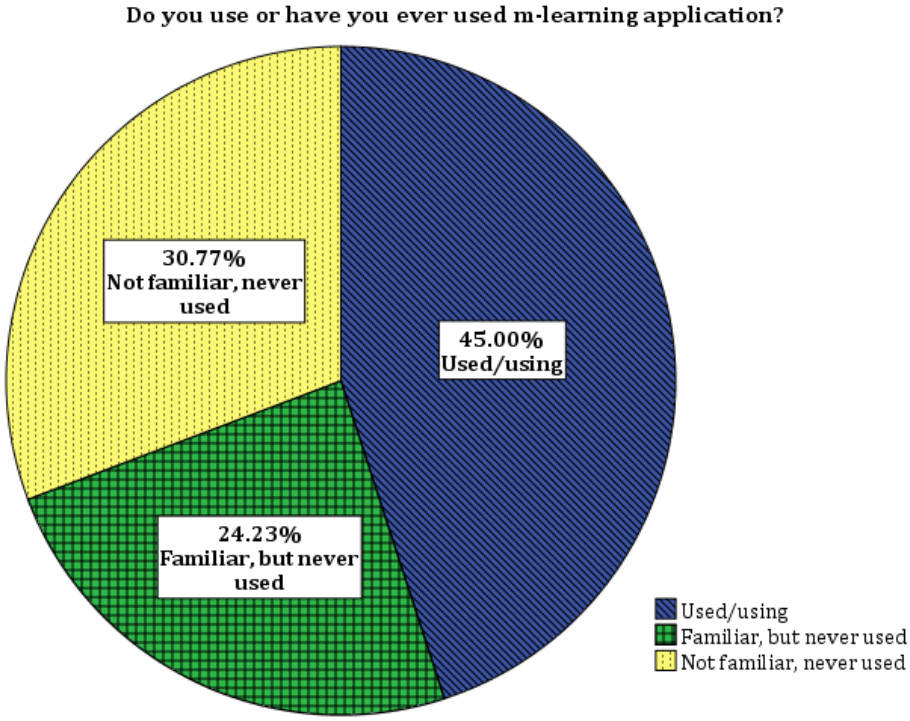


Figure 5-4: The familiarity of the sample with m-learning apps

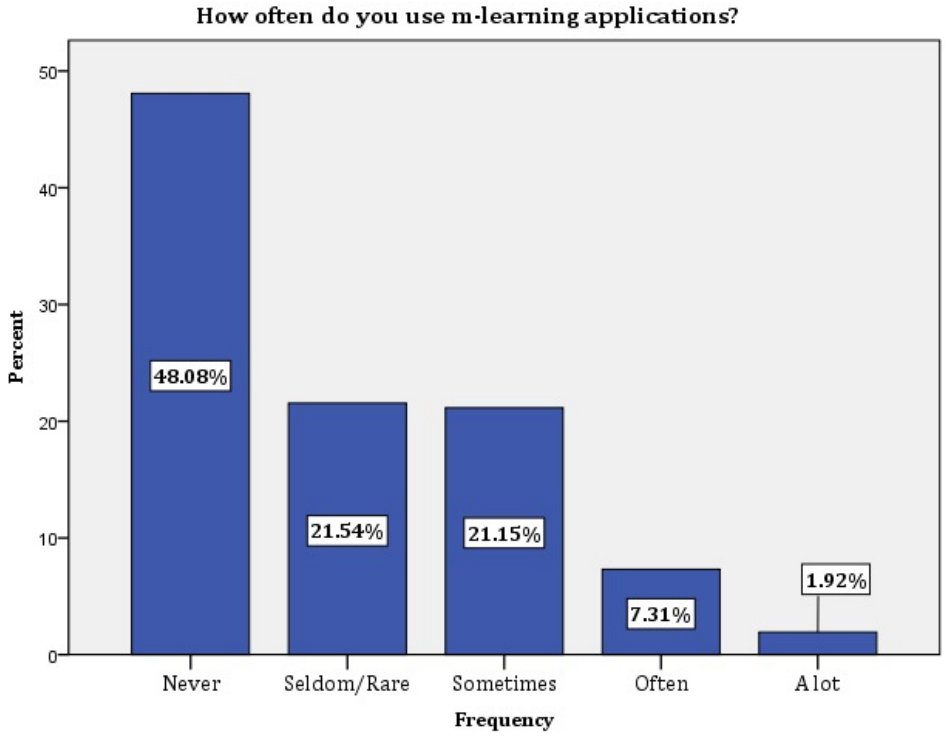


Figure 5-5: Frequency of use of m-learning application

The question about the frequency of use of the apps was composed using 5-point Likert scale items with the answer choices from 1 – for *never* using the m-learning apps, to 5 – using such apps *a lot* (Figure 5-5). The mean for this question was 1.93 and the standard deviation was 1.076.

The results of the survey indicate that the people who are the most familiar with m-learning apps are adults under 34. People who had Master's and/or undergraduate degrees used m-learning apps most often. No significant differences were identified in the familiarity with m-learning applications and frequency of use of these tools between men and women. The following bar charts (Figures 5-6 to 5-11) were created to visually present the results about the use of m-learning apps in correlation with the sample's demographic information.

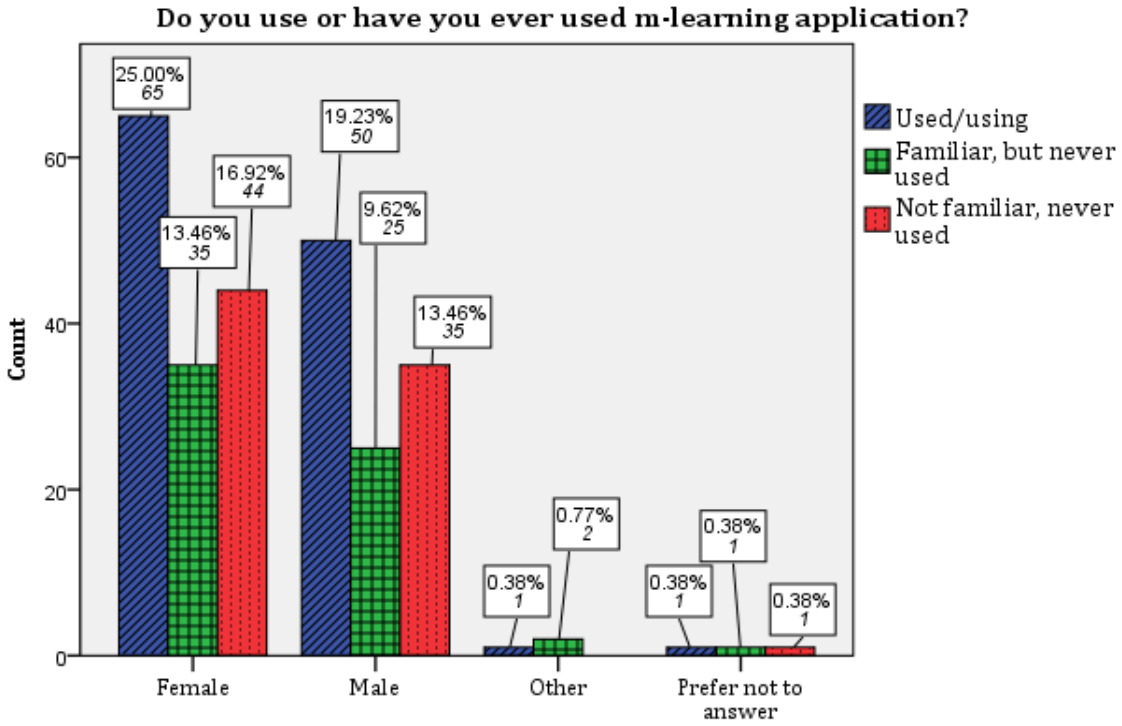


Figure 5-6: Different genders' familiarity with m-learning apps

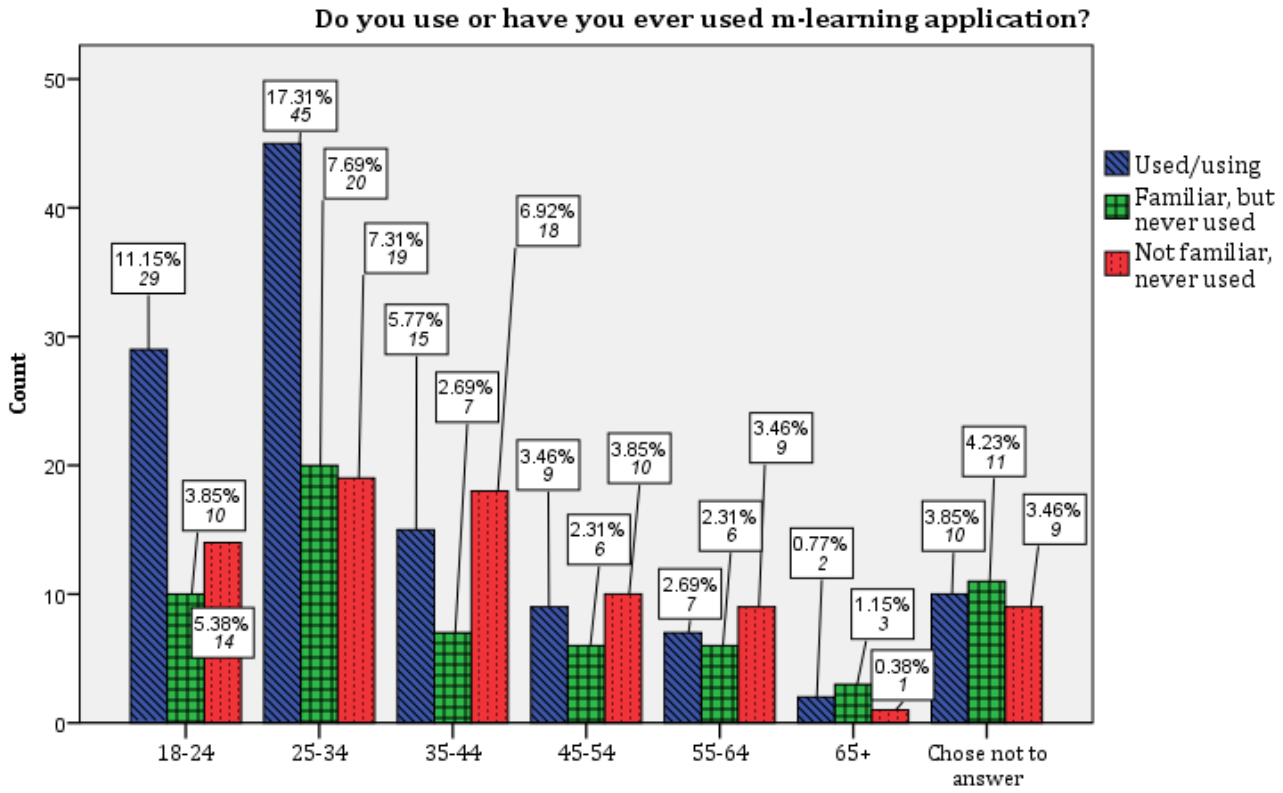


Figure 5-7: Age of the respondents and their use of m-learning apps

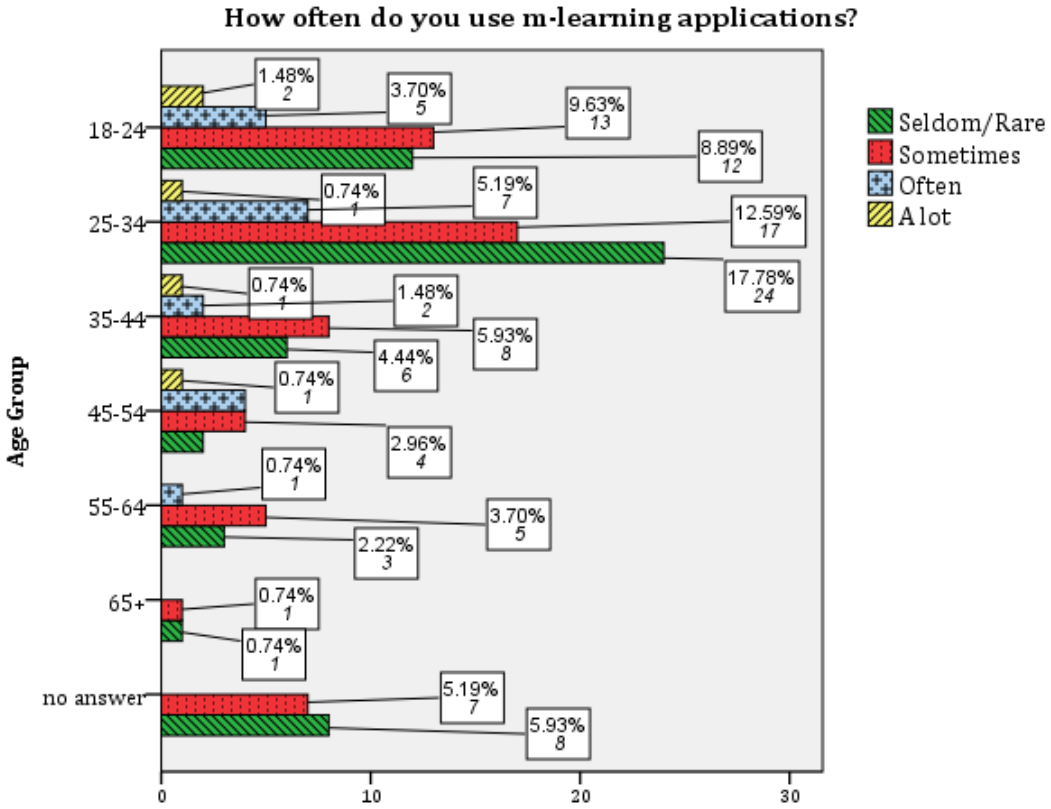
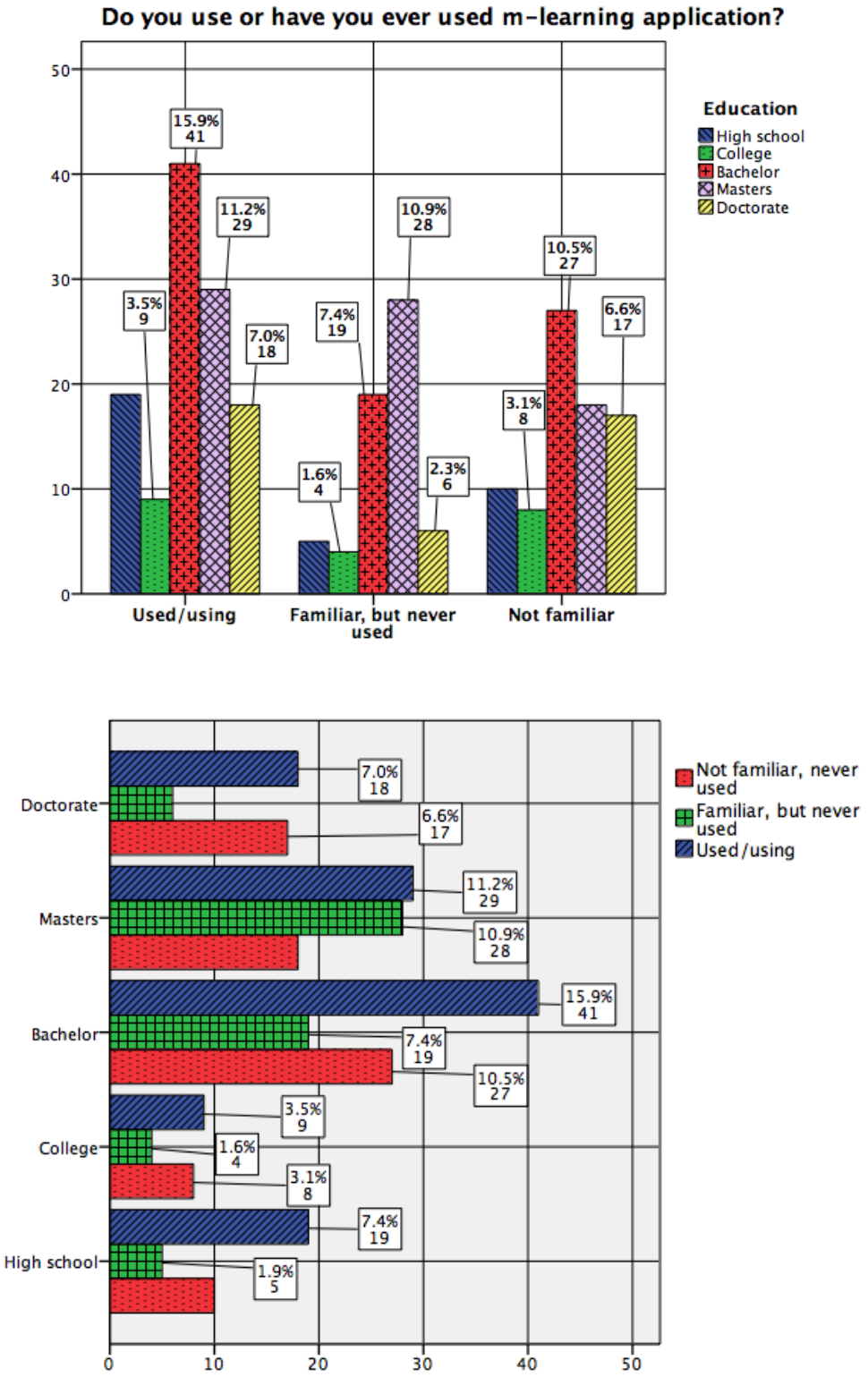


Figure 5-8: Frequency of use of the m-learning apps and the sample's age groups



Figures 5-9 and 5-10: The participants' education levels and their use of the m-learning apps

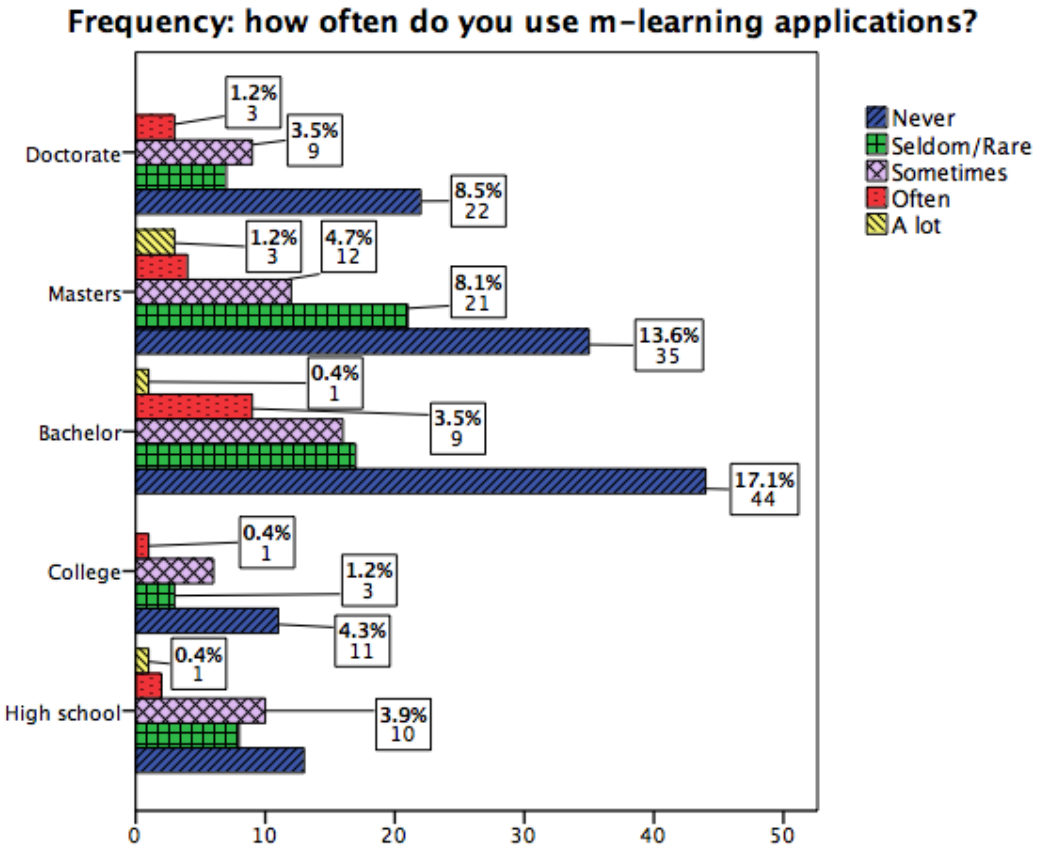


Figure 5-11: Frequency of use of m-learning application and the participants' education levels

Among people who said that they have never used m-learning apps before, the most common reasons for not using such applications were:

- "Didn't need to use" – 31.4%
- "Didn't know about such apps" – 28.6%

8.5% of the participants, who have never used m-learning apps, said the reason for this is that they didn't want to pay for such apps. All the other reasons provided by the respondents for not using m-learning apps were less significant. Only 2 people replied that they have never used m-learning apps, because they did not agree with privacy settings of the apps they wanted to install. 2 other people said they did not use m-learning apps, because they did not want to give the required permissions to those apps.

Thus, privacy settings were not a major reason for the respondents to decide not to use m-learning apps. The importance of the privacy settings and permissions for the users is explored further in this report.

5.4 Privacy Concerns and the Importance of Privacy Settings

The majority of those who reported using m-learning applications said that they use those apps mostly on smartphones (65.8%). Tablets were on the second place as the preferred device for accessing m-learning content (29.1% of the respondents who use/used m-learning apps).

I became familiar with different types of applications, their features and functionalities after conducting a literature review and reviewing of the privacy information of different m-learning apps. This knowledge helped me in composing the survey questions regarding what types of features they customized in their m-learning apps and what type of features they would like to see in the m-learning apps that they use or could use in the future. The respondents were allowed to choose multiple options for those questions. The following figures present findings about features that the participants would value the most in the m-learning apps.

113 respondents said that they customized some features in m-learning applications. Figure 6-12 shows that 41 (or 36%) of those respondents customized privacy settings of their m-learning apps. 34 respondents (30% of 113 people who made some changes in their m-learning apps) customized the permissions. 4 people (3.5%) chose answer

option “Other” for this question, and three of them elaborated on the changes they made. They customized the following:

- *“Referencing announcements, assignments, lecture notes and course documents I have previously posted for students on Blackboard.”*
- *“Content (chose to study simplified rather than traditional Chinese characters).”*
- *“Notifications.”*

See Table I-1 in Appendix I for the details on information presented in Figure 5-12 below.

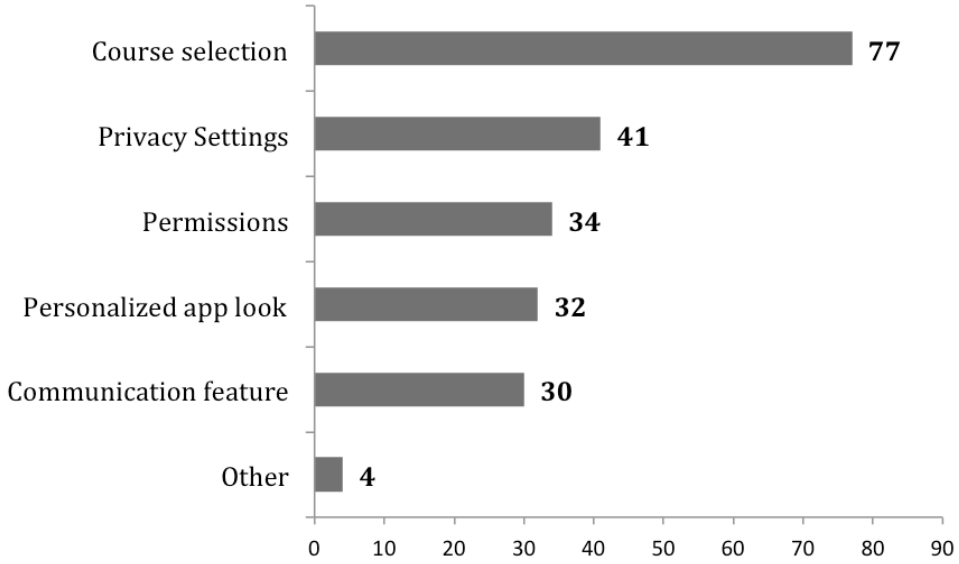


Figure 5-12: Settings that the users have customized in their m-learning apps

The questions about the desired features (“What features would you like to have in a mobile learning app?”) were addressed to all of the participants, even to those who have never used a mobile learning application in their lives, because people who are not using mobile applications for learning can still become users in the future. It is equally important to find out the opinions of the potential users as that of the current users.

Almost 50% (N=128) of all participants said that they would like to be able to see and customize privacy settings in the m-learning apps. Almost 40% (N=103) reported that they would like to be able to customize permissions (see Figure 5-13 below and Table I-2 in Appendix I for more details). Figure 5-13 presents different features from most selected to the least selected by the participants and the corresponding numbers of respondents or how many people from the sample want to have each of following features. Some of the participants who chose "Other" answer option left a comment that they would like to see full replication of PC environment in a mobile learning app.

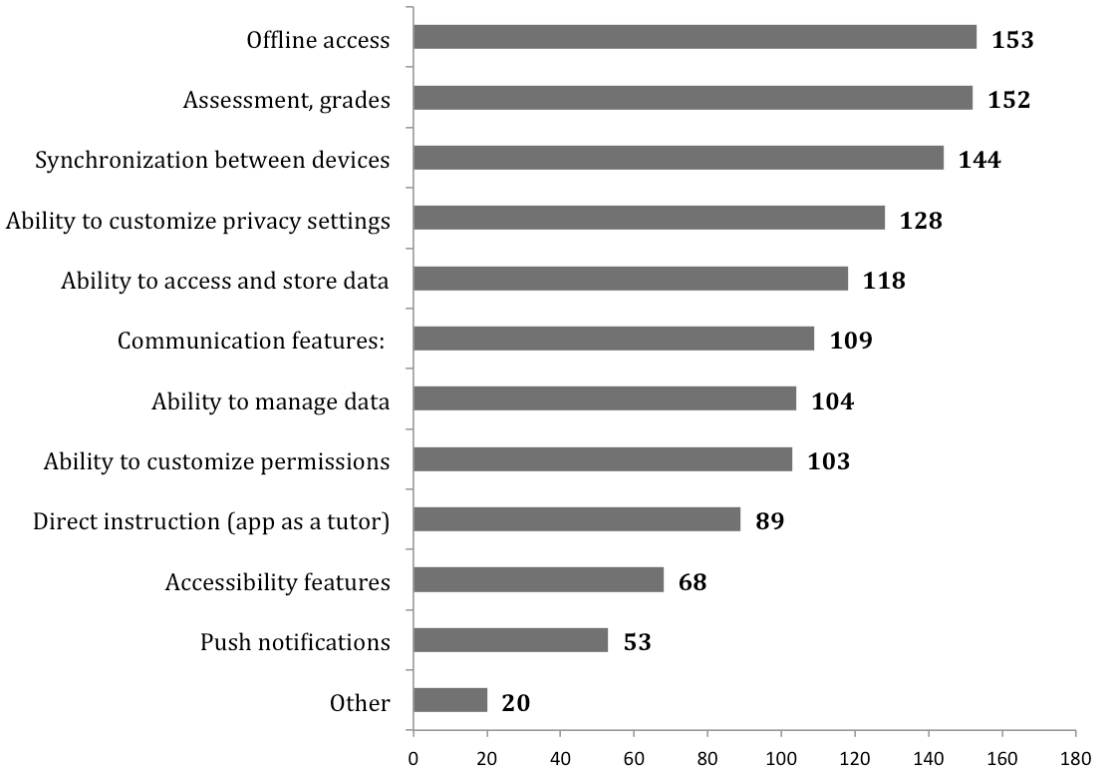


Figure 5-13: The features that the participants hope/expect to see in m-learning apps

The participants were also given 10 variables that could potentially affect their decision-making when/if they have to select a mobile learning application for their

study, training, learning and/or teaching purposes. They had to rank the importance of each factor on the scale from 1 (Very important) to 7 (Not at all important). Based on the survey results, an app's Privacy Policy would be ranked 5th in order of importance for the participants. The means in the Figure 5-14 indicate that application security is "important" for the survey participants, and the privacy policies and permissions of the apps are either "important" or "somewhat important" (See Appendix J for the detailed tables of means with the standard deviation values). The most important factors in the user decision-making about m-learning apps seemed to be their device compatibility, the content of an app, and its price. The participants were less concerned with how popular the application was (i.e., how many times it was downloaded and installed); many people chose to answer that the app's popularity is either "somewhat important" or "somewhat not important" for them.

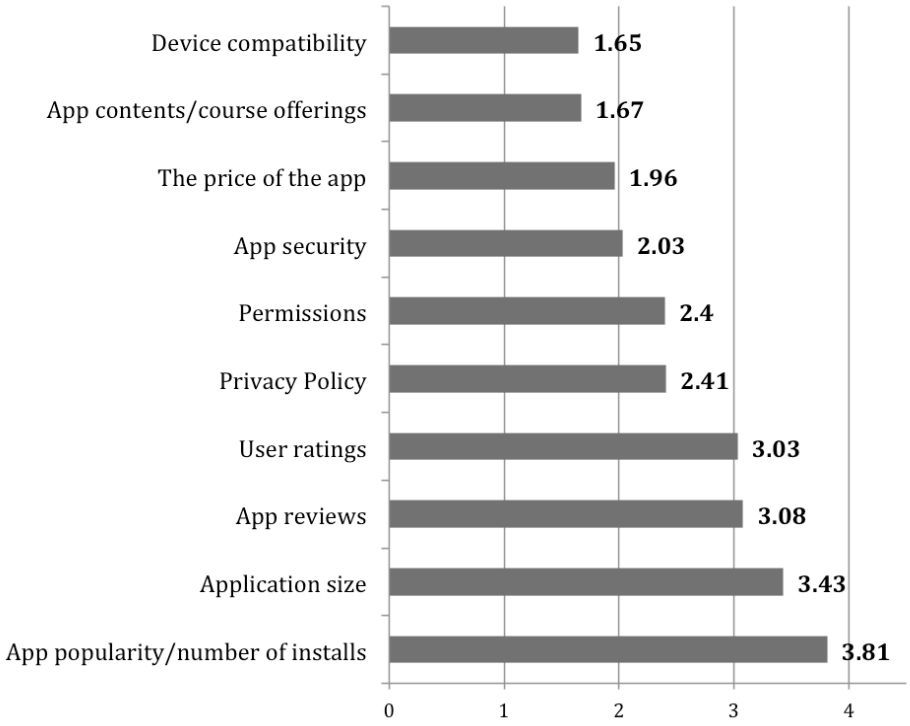


Figure 5-14: The importance of m-learning apps features or functionalities for the respondents, rated from 1 – very important to 7 – not at all important

The review of the privacy policies (see Chapter 4) revealed that all m-learning applications collect some information from their users to provide a better user experience. As was previously discussed, some personal information has to be collected to allow the application to function properly and to provide a personalized experience for the users; however, sometimes it is unclear why some applications collect certain user data. For instance, if an app presents information on mathematical formulas and teaches its users to apply those formulas in different problems, why would it collect location data and ask an access for user contacts? I asked the participants how much they agree that a mobile learning application could collect their personal information in order to "improve" the mobile learning apps' services, as the apps state in their privacy policies. Figure 6-15 presents the results in a bar chart of means: the means were calculated based on a 7-point Likert scale question, in which the respondents chose a reply on a scale from 1 – for "Strongly Agree [that this information should be collected]", to 7 – "Strongly Disagree [that this information should be collected]". As can be seen from Figure 6-15, the participants tend to strongly disagree that an app should collect their credit card information to allow for basic use of the app. The participants tend to be undecided about whether they would agree or disagree that an m-learning app should request to collect their users' browser information, email addresses, and even user names.

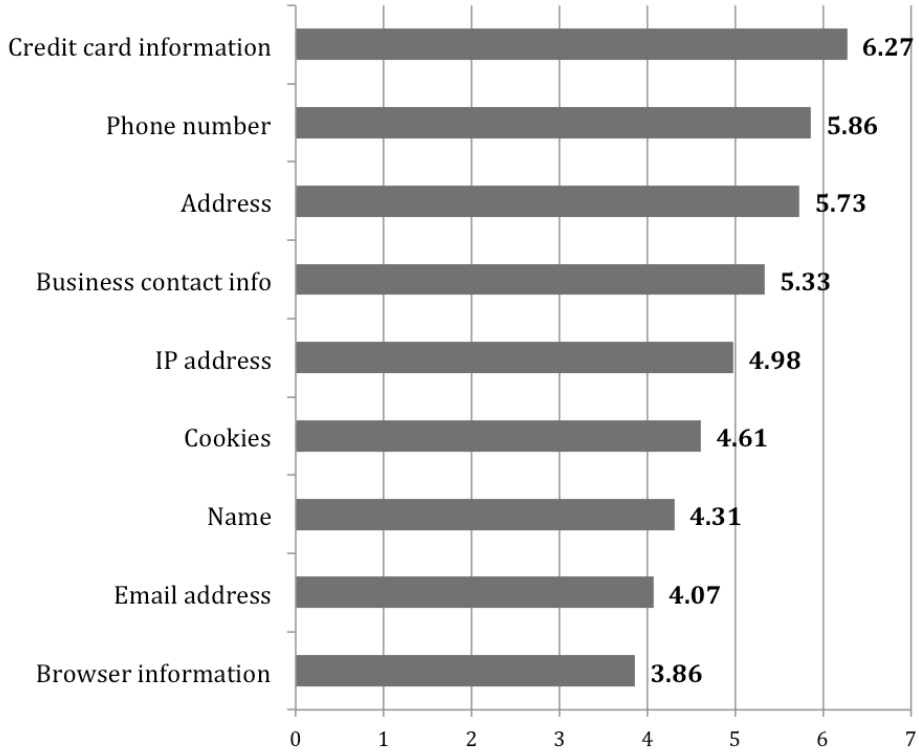


Figure 5-15: User attitude towards mobile learning apps collecting their information

Figure 5-16 presents a bar chart of means generated from the answers on the question about user concerns regarding their information sharing with third parties. The chart presents types of user information that the participants would be concerned to share with third parties (rated on a scale from 1 – the most concerned, to 7 – the least).

Next, Figure 5-17 presents results on the investigation regarding levels of users concerns on granting certain permissions for a mobile learning app in order to use it: the bar chart of means for the scale from 1 – Very Concerned, to 7 – Not Concerned At All.

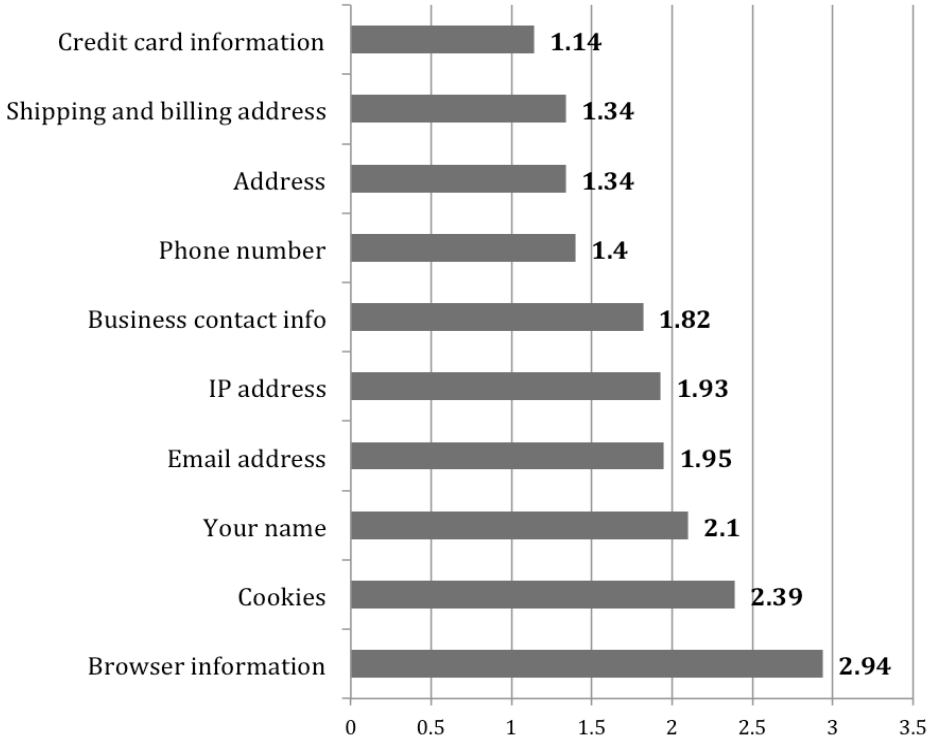


Figure 5-16: Levels of users concerns when a mobile learning app shares their information with third parties

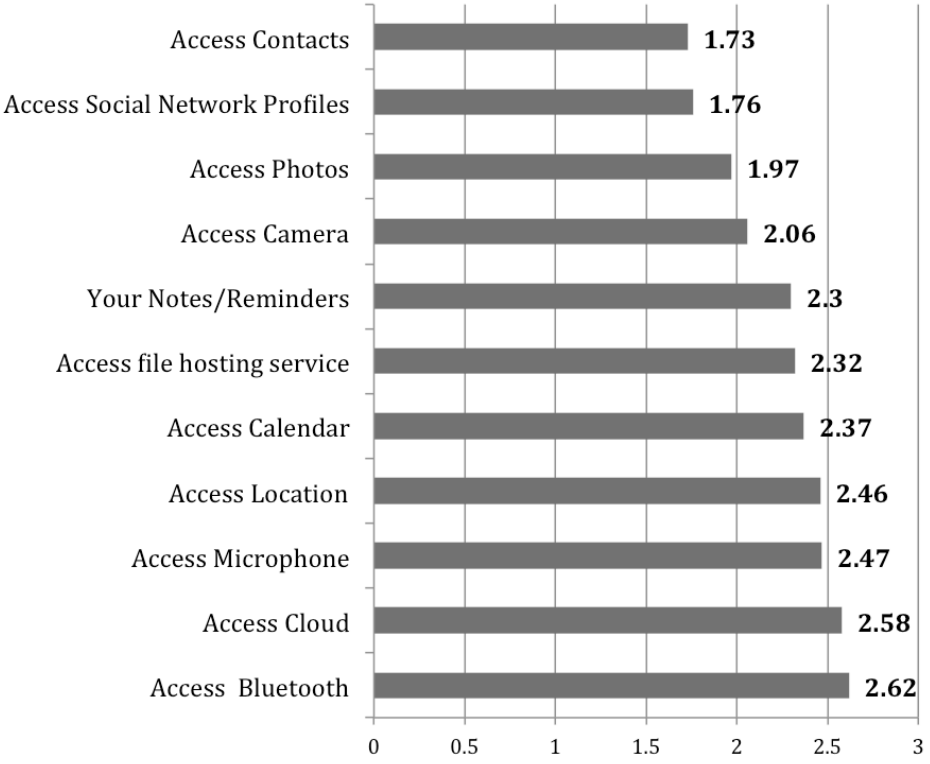


Figure 5-17: Levels of users concerns about a mobile learning app's permissions

Figure 5-18 presents a bar chart of means for the results from the questions 14-19 of the survey. This set of questions was designed to find out how the users would feel if they find out that a mobile learning app they use shares their personal information with the government or with some unknown third parties for marketing purposes. See Appendix J for more detailed descriptive statistics.

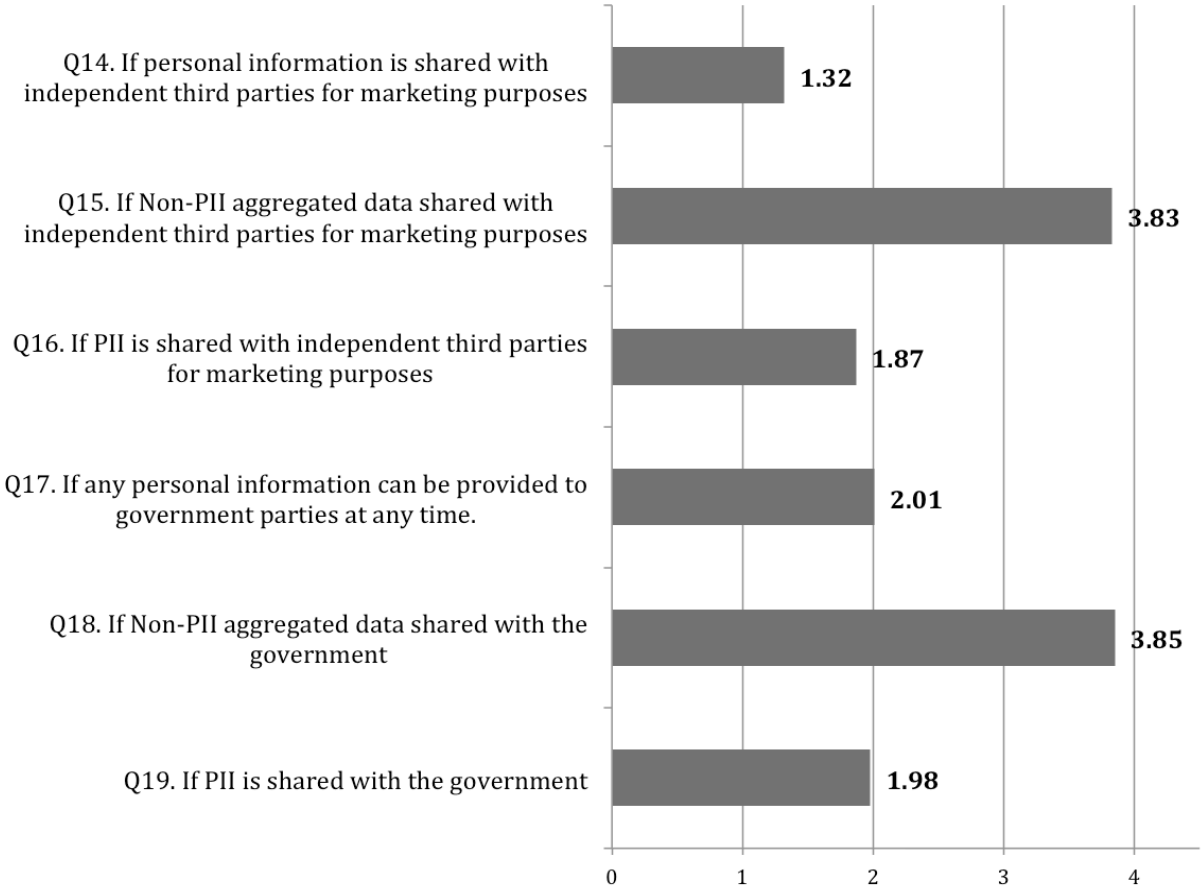


Figure 5-18: Levels of user concerns about an m-learning application sharing their PII or Non-PII with third parties for commercial purposes or with the government, means on a scale from 1 – Very Concerned, to 7 – Not At All Concerned.

I tested the relationships between the participants' demographic profile and privacy-related items of the questionnaire. For this purpose, a separate data entry was created in SPSS Statistics 22, that included only 50 variables: 4 independent (age group, gender, education, and the participants' familiarity with m-learning apps) and 46 dependent variables for 7-point Likert scale items. The latter items mostly explored user concerns and feelings about m-learning apps collecting and sharing user data with third parties. I created 184 contingency tables and performed chi-square tests based on the survey data to see if there were any observable relationships. I used a separate data file and a separate output for this analysis for convenience purposes only, i.e., not to mix chi-square test results with other tests and tables in the analysis. Chi-square tests did not reveal that the participants' levels of familiarity with m-learning apps made any difference in their opinions about m-learning apps' practices of collecting and sharing user information. In other words, the responses about the preferred features and concerns about privacy did not vary depending on whether the respondents used m-learning apps before or did not know anything about such apps. In general, chi-square analysis did not provide much insight into possible relationships between the participants' demographic profile and their responses; nevertheless, high significance levels were observed for some variables. I looked for results where $p < 0.05$, because the p-value associated with a 95% confidence level is 0.05. Results where $p < 0.01$ had a confidence level of 99%.

The chi-square results suggested that there might be a relationship between users age group and how important is a size of an application for them if they want to install it ($p = 0.008$). There was also an indication that there was a significant difference between the sexes in the responses about the importance of device compatibility in an app ($p =$

0.000), as well as the importance of course offerings (p = 0.08), user ratings (p = 0.016), app reviews (p = 0.027), app size (p = 0.000), and privacy policy (p = 0.028).

5.4.1. ANOVA analysis results

To determine if there was indeed a difference in responses between sexes and also between participants with different levels of education or between different age groups of respondents, I conducted one-way ANOVA tests. The answer choices "Prefer not to answer" were not included in the ANOVA analysis, because those replies were equivalent to skipped questions and could not be used as dependent variables in a comparison of means. Also, because there were only 6 respondents who were 65 or older, this group of the respondents ("65+") was combined with the age group from 55 to 64 years old into a new age group "55+". I have also disregarded the differences in responses between genders that were not female or male: only three people chose to reply "Other" on the question about their sex, and this number of respondents was too small to draw any statistical trends from their responses.

The importance of different features in m-learning apps for the respondents

The ANOVA test revealed that there is a significant difference in responses between sexes about the importance of a size of an application (p = 0.000) and its Privacy Policy (p = 0.004) if the participants would have to choose a mobile learning application to use. The results indicate that men tend to be rather undecided whether the size of an application is important for them, while it is somewhat important for women. Women tend to respond that an m-learning apps' Privacy Policy is important for them, while it is only somewhat important for men (see Appendix K for details).

Price has different importance for users of different age groups: the results indicate that the older respondents tend to care less about the price of an application when they decide whether to install a mobile learning app. The comparison of means revealed that people between 18 and 24 care about the price much more than people between 45 and 54, which makes sense, because 45 years old or older users most likely have more steady income than people under 24 (see Appendix K).

There was also a variation in responses between people with different levels of education and how important are such factors as course offerings (or content) of an application and an app's size. People with a Doctorate degree or equivalent cared about the content of an app a bit more (Mean = 1.42 on a scale from 1 to 7, were 1 is "Very important") than people who graduated from college (Mean = 2.05) or had a Masters degree (Mean = 1.93). People without post-secondary education also mostly replied that a "course offerings" is an important factor (Mean = 1.67). Those with a higher level of education cared less about the size of an application. People with just a High School diploma replied that size is somewhat important, but people with Master's or Doctorate degrees mostly replied that it's somewhat not important to them.

There was also a slight variation in responses about the importance of an app's popularity for the users. People without any post-secondary education tended to respond that number of an app installs (or how popular an app was among users) was somewhat important for them, while is was not very important for people with undergraduate degrees.

The participants' reaction to user data collection didn't vary much between different groups of respondents. Figure 5-15 in this Chapter presented the general respondents on this subject. The only slight variation observed was related to the collection of **email address** from the users. Most participants were undecided whether an app really needs to ask them for their emails, but people from 35 to 44 years old tended to reply that they somewhat disagree that an application has to collect their email addresses to allow for basic functionalities.

User concerns about Permissions

The ANOVA test results revealed there was a significant difference in responses between genders about user attitudes towards granting to a mobile learning app such permissions as access to data sharing via Bluetooth and access to the user's Cloud. The survey results indicate that women are concerned when an app asks them to grant access to their Bluetooth and the Cloud, while men are only a little concerned about it. (See the tables with comparison of means and ANOVA results in Appendix K.)

Other observed differences in responses about m-learning applications' permissions and how users feel about granting those permissions varied between participants of different age and education levels. Significant differences in responses (with 95% confidence level) between age groups included different levels of concerns about permissions to access contacts on the devices of the respondents (p = 0.013), access calendars (p = 0.002), notes and reminders on the devices (p = 0.001), and access to social networks (p = 0.004). A comparison of means revealed the following trends (see Appendix K for descriptive tables):

- When looking at the responses of people from 18 to 44, the more concerned they were about granting to an application permission to **access their contacts**. This trend seems to start moving in another direction in responses of participants from 45 and older. The greater difference (p = 0.024) was in responses between people under 24 (generally concerned) and in the age group from 35 to 44 (very concerned).
- A clear trend can be seen in responses about granting an app permission to **access calendar**: younger respondents were somewhat concerned about it, leaning towards undecided (participants from 18 to 24 years old), and the older the participants were, the more they were concerned (people over 45 were the most concerned about it).
- Similar trends were observed in responses about concerns if an application required permissions to the **Notes/reminders.** People under 24 were somewhat concerned, but then the levels of concern rose according to the ages of the respondents. People from 45 to 54 were the most and very concerned. However, the concern level then falls again to generally "concerned" in responses of participants over 55.
- The observed trend in responses about concern levels when an app requires **access to social networks' profiles** was the same as with access to notes and reminders. From 18 to 54, the older the respondents were, the more concerned they reported to be about an app accessing their social networks' profiles (from just concerned to very much concerned). There was no difference in responses between people from 34 to 44 and over 55 years old. The greatest difference (p = 0.049) was in responses between people under 24 and from 45 to 54: younger

respondents were significantly less concerned about granting permissions to access social networks.

- The older the participants were, the more they were concerned about granting permissions to **access Bluetooth**. People over 55 were concerned about it more than people under 34, but post-hoc analysis showed the difference was not too dramatic. Answers varied from "concerned" (for older people) to "somewhat concerned" (for younger respondents).
- Comparison of means revealed a clear trend of people being "somewhat concerned" (Mean = 2.81) when an app requires permission to **access Dropbox** or any other file sharing app used by the respondents, when the respondents were under 24, but the level of concern grew to "concerned", leaning towards "very concerned" among older respondents. The greater difference in responses was between people under 24 and people over 55.

Similar trends were observed for all the other permissions: in the responses of people from 18 to 54 there was a clear progression and growth of concern levels. The older respondents were, the more concerned they were about granting different permissions. But in responses of people over 55 the levels of concerns dropped compared to responses of people from 45 to 54. In general, reported levels of concerns of people over 55 were almost the same as those of people from 35 to 44. The biggest difference in responses was always between people of 18-24 and 45-54 years old. However, for all other types of permissions those differences weren't significant enough to claim that there were some correlations.

ANOVA tests revealed significant differences in responses between people with different levels of education about permissions to access photos (p = 0.049), access calendar (p = 0.017), access notes or reminders (p = 0.020), access social networks' profiles (p = 0.006). I used Bonferroni procedure for comparisons between data groups after the one-way ANOVA analysis to find out the most significant differences in answers between respondents with different education. The most significant differences were between the following groups:

- Between people who completed undergraduate schools and people who had Ph.D. or equivalent level of education in their replies about concerns regarding permission to **access calendar** (p = 0.027). Respondents with Bachelor's degrees tended to be somewhat concerned about it, but participants with Doctorate degrees were much more concerned.
- Very significant difference was observed in responses about **access to social networks** between people with Doctorate degrees and people who finished High School but had no post-secondary education (p = 0.004). Less educated people were concerned about granting this type of permission, but respondents who completed graduate schools were more concerned about it (most of them responded being very concerned if an app requires access to social media profiles).

Post-hoc analysis revealed that differences in responses between groups of interest for other variables were not significant enough to report. However, a comparison of means still revealed some interesting tendencies:

- The higher was the education level of the respondents, the more they were concerned if an app required permission to access their photos, access contacts, access calendar, and access social networks' profiles.
- People with graduate degrees were more concerned about granting permissions to access their file-sharing apps compared to respondents with undergraduate degrees or just a High School diploma.

User levels of concern when an app shares their user data with third parties

I asked the participants how concerned they would be (on the scale from 1 – strongly concerned, to 7 – not concerned at all) if a mobile learning application shares their information with third parties. One of the questions presented different types of information that could be collected from the users, and I asked the participants how would they feel if some of their particular data were shared (see Figure 5-16 in this Chapter for the average responses of the sample) with any independent third party. I didn't specify the purpose of the data sharing. There were no significant differences in responses for this question between different genders. The ANOVA test revealed differences in responses between age groups about the concerns if an app shares such user information as a user name (p = 0.002), phone number (p = 044), and email (p = 0.000). The post-hoc test found the most significant differences between multiple groups, in particular:

- Responses of people between 18 and 24 were significantly different from those of people in the age groups 25-34 (p = 0.030), 35-44 (p = 0.003), and over 55 years old (p = 0.018). The comparison of means showed that people under 24 are only a little bit concerned if an app shares their names with third parties, while older people are generally concerned if that happens.

- People between 35 and 44 answered differently about how worried they would be if an app shares their phone number with anyone, compared to the answers of people under 24 ($p = 0.046$): the older respondents were very concerned about such possibility, while younger people were concerned, but not as much.
- The comparison of means revealed a linear trend that the older the respondents were, the more concerned they were about a possibility that an app could share their email addresses with some unknown third parties. People under 24 were somewhat concerned about it, and the reported levels of concern increased according to the respondents' age to the point that the participants over 55 were very concerned about their apps sharing their emails with third parties.

There were also differences in responses about third-party sharing of the users' information among people with different education. Significant differences in responses were observed only regarding sharing email addresses ($p = 0.000$) and phone numbers ($p = 0.005$). There was a strong indication that the higher degree the respondents had, the more they were concerned about those issues (see Appendix K for the table of means). Concerns about a possibility that a user's phone number could be shared with some unknown third parties ranged from generally just "concerned" to "very concerned". People without post-secondary education tended to reply that they were "somewhat concerned" if an app shares their emails with somebody. The levels of concern on this issue rose proportionally to the levels of the respondents' education, and people with graduate and postgraduate education were very concerned about it.

Levels of concern if a mobile learning app shares user data with independent third parties for commercial purposes

When the participants were asked about their concern level if an app would share their personal information (PII) with any third party for marketing purposes, the responses did not differ much between sexes, but there was a variation in responses between people of different age ($p = 0.017$). A post-hoc analysis revealed that the biggest difference in responses was between groups of people from 18 to 24 in comparison to the responses of people over 55 ($p = 0.043$). Older people were more concerned about the possibility that an m-learning app they use (or would like to use) could share their personal information with anyone for commercial purposes.

While the variation in responses between people with different levels of education was not significant, it is worth mentioning that the comparison of means presented a slightly noticeable trend: the higher level of education of the respondents, the more they were concerned if an app shares their personal information with third parties for marketing purposes. It would be interesting to explore if a larger and more random sample of respondents could increase the significance level (p-value) of this trend, or, in other words, demonstrate a bigger difference in responses between less and more educated people.

The participants were also asked if they were concerned that a mobile learning app they use could share their usage patterns with independent third parties for commercial purposes. The usage patterns of a mobile application would include data about how often the application is used, which courses/topics are accessed the most by the individual users, and how much time a user spends on different tasks or topics. When it

was said that such information could not be linked to an individual user (i.e., would not be personally identifiable), the respondents were mostly undecided if they should be concerned about it. There were no significant differences in responses of people of different genders or education levels. Although, the comparison of means showed that people with Doctorate degrees tended to respond that they were somewhat concerned about it, while people with undergraduate or lower degrees were mostly undecided. There was a significant variance in responses of the participants in correlation with their age: people under 24 were undecided on the issue with slight inclination of being "somewhat not concerned", but the older the participants were, the more their responses leaned towards "somewhat concerned". Thus, the biggest difference on this matter was in responses between groups of 18-24 year old participants and those of 55 and older.

When the participants were asked about their attitudes towards third-party sharing for marketing purposes if the usage patterns shared would be personally identifiable (PII), the respondents tended to answer that they were concerned about it (see Figure 6-18). The responses did not differ between people either according to their genders or age. However, people with college education were less concerned about it in comparison with people who had a Master's degree (p = 0.043).

Levels of concern if a mobile learning app shares user data with the government

The participants reported to be concerned when I asked how much they would care if the personal they provided to their m-learning app was shared with the government for any reason. Females were slightly more concerned about it (Mean = 1.82; on a 7-point Likert scale from 1 – very concerned, to 7 – not concerned at all) than males (Mean =

2.31). However, there were no significant relationships between the opinions on this issue and the age or education of the respondents.

Just as with the question about third-party sharing of aggregated usage patterns data (Non-PII) for commercial purposes, the participants tended to be undecided if they would be concerned in case an app shares their Non-PII with the government. ANOVA tests did not reveal any differences in responses on this question between people of different age, education or gender. However, when I asked the participants how would they feel if such shared usage patterns data would be personally identifiable, they tended to reply that they would be concerned about it. Those responses did not differ depending on the participants' demographic profile.

Further interpretation of the results is presented in the next and concluding Chapter 6.

Chapter 6 – Discussion

6.1. PbD Approach

The review of PbD as a theory revealed that it is not specific enough to be used as a technical guide for the m-learning app developers; however, it could be adopted as a regulatory framework to set the ethical standard of the best privacy practices for the developers and providers of the mobile learning tools. For instance, following PbD Principles, m-learning app developers should limit the information they collect from their users to only what is absolutely necessarily for the app to function. According to PbD, it is insensitive (and potentially dangerous to the user) to collect user information that is unnecessary for an app to function, but may be perceived by the developers as something that might be useful in the future. Furthermore, even if an app doesn't collect anything from their users, the developers have to make it explicit to the users that nothing is collected. If an app claims to collect Non-PII, then it should be explicitly stated what kind of information they consider Non-PII, because users should not be left guessing about what exact information is collected from them, and they may disagree that certain information cannot be linked to them personally.

The PbD concept stresses that it is important to think about privacy from the beginning, from the design and development stage of any product. In the process of conducting this research, I have talked to different developers and it's obvious from those conversations that none of them intend to violate their users' privacy. However, developers may prioritize other issues above privacy concerns, or they may just not care enough to look

into privacy vulnerabilities and limit the information that would be automatically collected from the users. This is precisely why the PbD principle of "Proactive – Not Reactive" is important for developers to adopt. There might be privacy risks to the users that even developers cannot anticipate and it is important to develop privacy-preserving solutions into the development process itself, well before user privacy is violated. The Principles of PbD can be used as a guide for the developers on what to consider (from the user perspective) when deciding what information needs to be collected from the users and how to communicate to the users about how and why their information is collected.

6.2. Findings from the Privacy Policies Review

One of the primary research questions for this project was "What are the user privacy concerns regarding m-learning applications and what effect do these concerns have, if any, on the use of m-learning applications?" I reviewed the privacy policies of several mobile learning applications to identify some of the issues that needed to be explored: e.g., what could worry the users and with what they might disagree. This research revealed that there is a lack of transparency in the privacy policies of m-learning applications. The privacy policies of 31 applications were reviewed for this research, and not all of those applications had a privacy policy or any privacy statement. Some privacy policies were merely a few sentences of text stating that they don't collect personal information from their users, but may collect personally non-identifiable data for use in analytics.

The review of the m-learning apps' privacy policies show little to no existing adoption of the Principles of PbD, at least not obviously so. As was mentioned earlier, the privacy policies are not transparent and clear enough with the users about how their data is collected and used, which is violates the 6th principle of PbD ("Visibility and Transparency"). Most of the privacy policies made it obvious that they seek to accommodate and protect the providers and developers rather than users (e.g., in almost every privacy policy it was said that the app would share user information with the government if they feel that that would be in their interests, which is a somewhat ambiguous reason to provide user data to the government parties). It is understandable that the developers and providers would want to protect themselves from any legal action or misunderstanding with their users and with third parties about the use of the data they collect. However, in keeping with the "Full Functionality" Principle of PbD, I feel that the approach to privacy protection and communicating privacy information should not necessarily have trade-offs, meaning that protecting developers' interests should not mean neglecting users' interest. PbD is a valuable concept because it dictates that users' privacy is something that should never be ignored or traded for something else, e.g. for security or some functionality.

6.3. Survey Findings

A survey study was conducted to find out how and if users' attitudes towards some privacy issues affect their use of m-learning applications and how concerned people may be about their privacy when they use these apps. I could not find explicit support for PbD from the survey results of the potential and current users. The results indicate that privacy policy is not a very important factor in the users' decision-making when

they have to select a mobile learning application to install. However, the respondents still replied that a privacy policy of an app would be somewhat important to them; women considered it to be a bit more important factor than men did. The survey study revealed that participants don't agree that a mobile learning application has to collect their users' credit card information, phone number, address and business contact information for the stated purpose of allowing for basic functionalities and to provide a better service for the users.

The research revealed that the respondents' concerns about m-learning applications did not have an effect on their use of m-learning apps. The survey showed that the main reason people do not use m-learning apps is because they are unaware of them or don't believe they need them, and not because they are concerned about privacy or security issues. This is consistent with the Technology Acceptance Model (Davis, 1989), which states that one of the main factors influencing users' decision whether to use new technology is the perceived usefulness of this technology. The observed lack of familiarity with m-learning apps explains why the respondents provided very generic answers regarding their opinions about the collection and sharing of user information by m-learning apps. It is simply difficult to have a strong opinion on a specific aspect of a service you are not using frequently.

According to Blank, Bolsover and Dubois (2014), who proposed "a new privacy paradox", young people are more concerned about their privacy on the internet than their elders. Assuming that the perception of privacy depends on social circles, younger people are more sensitive to privacy issues, because their social circles are rapidly expanding (Blank et. al, 2014). I thought that the younger generation might have more

privacy-related concerns about their use of m-learning apps, because they might be more familiar with the technology and with how apps use their data than older generations. I also assumed that younger people might be more aware about digital privacy issues and worry about privacy much more than older people, but it would seem that I was absolutely wrong in this assumption. The results of my survey are not directly related to Blank et. al's "new privacy paradox", but they contradict their findings that younger people are more concerned about privacy than their elders. The analysis of the survey results showed that the older the respondents were and the higher their level of education was, the more concerned they were about the different issues explored in this study. These issues and items of interest included granting an app the permissions to access contacts, Bluetooth, and any file sharing service (e.g., Dropbox) on the users' devices. Furthermore, people under 24 were generally less concerned than the older respondents if a mobile learning app shares their user information with third parties.

The participants with higher levels of education than other respondents were more concerned that an app might share their phone numbers and email addresses with some third parties. In addition, more educated people (e.g., the respondents who had a graduate degree compared to those who just attended college or had no post-secondary education) were more concerned about granting permissions to access social networks, calendars, photos and contacts on their mobile devices. More educated people were also more concerned about a fact that mobile learning apps share their aggregate Non-PII for commercial purposes. On average, the participants tended to be undecided on whether they should be concerned about it or not. They were also rather undecided about their feelings regarding sharing Non-PII with the government and there were no significant

differences in the responses between people of different age, education, or gender. The results also suggest that the users have a tendency to be less concerned about sharing their Non-PII aggregated data with any third parties rather than sharing their PII. Based on these findings, we can hypothesize that the levels of user concern or their attitudes about m-learning apps sharing their user information with third parties depends on the types of the information being shared and not the identities of the those third parties.

In addition, the survey results presented what features or characteristics of m-learning apps are the most important for the users. In the survey study, the users shared what is the most important for them when they select which mobile learning application to install, and what would they want for mobile applications to be able to do in future or how they would improve those apps. In general, most respondents wanted a possibility of using their mobile learning apps offline (i.e., when they don't have internet connection on their mobile devices) and they also wanted a possibility to see their learning progress or see their grades. Those findings would be valuable for the developers of mobile learning solutions and they can use this information to develop new functionalities and offer what their users want in these applications.

6.4. Limitations

Despite the comprehensiveness of this study, it had several limitations. First, I used convenience sampling. Some of the respondents were people subscribed to the Privacy and Cyber Crime Institute's newsletter. The fact they are subscribed to those updates means that they are probably aware of some digital privacy issues and may think about privacy more than any other average person. This awareness and their general interest

in the privacy-related issues might have been reflected in their answers. Second, the surveyed population for this research appeared to be mostly highly educated, which made it hard to ascertain whether there was a strong relationship between their level of education and their familiarity with the m-learning apps or how they felt about some privacy-related issues. A random probability sampling method would have reduced a sampling error and bias, but it couldn't be applied due to exploratory nature of this study.

6.5. Implications and Further Research

The review of the PbD framework revealed that it cannot be applied as a theoretical model and could not be used to make any predictions or develop a testable model for this research. To analyse any phenomenon or test a hypothesis and understand a problem, a theoretical model should not only have a set of variables needed for analysis, but also should define those variables and be able to establish relationship between them, explain and/or predict behaviour of those variables, make assumptions, and interpret results/outcomes. The relationships between the PbD Principles and their impact on the product design or user behaviour are not sufficiently established and need further development to be used as a theoretical model in a research. However, PbD Principles can help the developers better communicate privacy information to their users. Moreover, PbD could be applied as a regulatory framework or a quality standard for privacy practices for developers and providers of mobile learning applications. The work on PbD development into a more practically applicable tool should be continued, and some specific examples should be added for every one of the 7 Principles to help achieve compliance with PbD.

The survey findings indicate that there is a need to raise awareness amongst the Ontario population about the app-based m-learning technology and also about privacy threats in mobile applications in general. It seems that most people don't see the benefit in m-learning to use it on their own (i.e. if neither their school nor workplace requires them to use m-learning for their education or professional development). The survey results suggest that user concerns regarding Privacy Policies, Terms of Service, Permissions, or app design are not the primary barrier to the use of m-learning apps. Instead, use is limited because there is a general lack of awareness that m-learning applications exist, and those that know of them often feel that they do not *need* to use such applications. The researchers and the m-learning applications' developers should explore this concept of *need* to find out what makes the users feel like they *need to use* a particular application. Theories such as the Technology Acceptance Model, Uses and Gratifications theory and Diffusion of Innovation theory are likely to apply in this context and could provide a valuable insight into why people don't use m-learning apps more often. Such inquiry into the users' motivations and intentions to use an app would also be beneficial for the marketers, because it could reveal how to appeal to the customers that *don't feel the need* for using m-learning tools. It would be a great step forward for the m-learning industry development if the learners would choose to use m-learning apps not because they *need* or *have to* do it (e.g., when they are driven by some external factors such as school requirements or an obligatory corporate training program), but because they genuinely *want* to use such applications on their own initiative for their personal or professional development.

The findings of this thesis revealed that the majority of the respondents are quite concerned that m-learning applications could collect their PII and share it with third parties. The responses indicate that users don't really know if they have to be concerned about aggregated Non-PII that is collected from them and shared with various third parties for analytics and for marketing purposes. It means that there is a lack of understanding about what aggregated data is and whether Non-PII can pose any privacy or security threats to the users. Further research is needed to explore if people know the difference between personally identifiable information and personally non-identifiable information, and what concerns they might have regarding one or the other.

The results of the survey showed that people are slightly more concerned about a possibility that an app might share their information for commercial purposes than if an app shares user information with the government. Considering that most of the respondents were Canadians and residents of Ontario, we can infer from the results that Canadians trust the government more than they trust corporations or commercial organizations. In addition, ANOVA analyses revealed that women are marginally more concerned than men that an app may share their information with the government. The survey results also revealed that women are more concerned than men about granting an app the permission to access their cloud or the ability to share information via Bluetooth. Further research is needed to determine generalizability of these findings and to explore why there is a difference in response between genders regarding these types of permissions.

Finally, based on the observed trends in the participants' responses for my survey, I suggest that older people and more educated people are more concerned about their

privacy and how applications use their information than younger people, because they probably have more knowledge about the privacy risks. Further research is needed to develop this proposition.

Appendices

Appendix A – The 7 Foundation Principles of Privacy by Design

Principle	Description
1. ***Proactive*** not Reactive; ***Preventative*** not Remedial	Privacy by Design is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.
2. Privacy as the ***Default Setting***	We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, *by default.*
3. Privacy ***Embedded*** into Design	*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4. Full Functionality – ***Positive-Sum***, not Zero-Sum	*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy **vs.** security, demonstrating that it ***is*** possible to have both.
5. End-to-End Security – ***Full Lifecycle Protection***	*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***	*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify.
7. ***Respect*** for User Privacy – Keep it ***User-Centric***	Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Source: Cavoukian, A., Prosch, M. (2010).

Appendix B – The Tips for Communicating Privacy Practices to The Apps' Users, as Suggested by the Office of the Privacy Commissioner of Canada

Recommendation/Step		Explanation
Be Transparent.		
1	*Make sure privacy information comes from you.*	The user can find out about what information an app collects from them from various sources such as media, academic research or publication, analysis by a third party or anyone else. To generate users' trust, the app developers should ensure that users find out about privacy information from developers and not by accident from some other third party.
2	*Be specific.*	Generic and overly broad information makes it harder for users to give their meaningful consent, which is why app developers have to be very specific in their privacy communication. If there are any changes in the privacy policy, the users should be notified.
3	*Speak to your audience.*	The app providers should know their users and communicate in the accessible and comprehensive way with their users. They should use the language that their audience can understand.
4	*Tailor to the environment.*	Developers of mobile apps should cater for small screens and make the privacy information accessible for the mobile devices.
Explain the data you are requesting and collecting.		
5	*Describe how your app uses the permissions it seeks.*	It is insufficient to inform the users what permission the app would ask from them. The users should be informed why the users should grant those permissions.
6	*Explain the data you gather through social media logins.*	Many applications ask or require users to log in or register using social media accounts. It should be explain what information is collected through these accounts.
7	*Permission to access is not necessarily consent to collect, use or disclose!*	"*Absent additional information*, the fact that a user has been notified of the app's ability to access certain personal information would not

		necessarily constitute his or her meaningful consent for the collection, use or disclosure of that information." It should be explained why the application needs access to the certain information on the users' mobile devices and what it intends to do with this information.
Make, and keep, privacy information accessible.		
8	*Provide privacy information, even if you don't collect any personal information.*	Users shouldn't guess whether an app collects personal information from them or not. The apps should have privacy policies and tell their users that they don't collect personal information, if they don't, or what types of personal information they collect, if they do.
9	*Include privacy information, and/or a link to it, in your app.*	"Making individuals exit your app to explore your website (or find the app's listing in a marketplace) in order to locate information about the app's personal information handling is onerous for users, both in terms of privacy practice transparency and general usability."
10	*Allow individuals to re-visit privacy information.*	Regardless of the ways the privacy information is presented, the users should be able access it more than once to enhance their understanding of the service and to be more comfortable with the application. The communication of privacy information to the users should not be a "one-time-only" event.

(Source: OPC Fact Sheets, 2014.)

Appendix C – Research Ethics Board Approval

RYERSON UNIVERSITY
RESEARCH ETHICS BOARD

To: Daria Ilkina
Ted Rogers School of Management

Re: REB 2014-235: Investigating and Addressing Insecurities and User Privacy Concerns in Mobile Learning Applications from Privacy by Design Perspective

Date: July 25, 2014

Dear Daria Ilkina,

The review of your protocol REB File REB 2014-235 is now complete. The project has been approved for a one year period. Please note that before proceeding with your project, compliance with other required University approvals/certifications, institutional requirements, or governmental authorizations may be required.

This approval may be extended after one year upon request. Please be advised that if the project is not renewed, approval will expire and no more research involving humans may take place. If this is a funded project, access to research funds may also be affected.

Please note that REB approval policies require that you adhere strictly to the protocol as last reviewed by the REB and that any modifications must be approved by the Board before they can be implemented. Adverse or unexpected events must be reported to the REB as soon as possible with an indication from the Principal Investigator as to how, in the view of the Principal Investigator, these events affect the continuation of the protocol.

Finally, if research subjects are in the care of a health facility, at a school, or other institution or community organization, it is the responsibility of the Principal Investigator to ensure that the ethical guidelines and approvals of those facilities or institutions are obtained and filed with the REB prior to the initiation of any research.

Please quote your REB file number (REB 2014-235) on future correspondence.

Congratulations and best of luck in conducting your research.

Lynn Lavallée, Ph.D.
Chair, Research Ethics Board

Appendix D – Recruitment Scripts for Posts on Social Media

Twitter

Script 1: Please take this academic survey on concerns about mobile learning apps: http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/ Participation is anonymous and takes 10 min.

Script 2: I'm collecting data about the use of mobile apps for learning and user concerns. More info and link to the survey: http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/

Script 3: Survey about apps for learning: http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/ Could you take it & share the link?

Facebook

Script 1:

"Dear friends, colleagues, fellows and acquaintances,

I'm collecting data about user concerns regarding the use of m-learning apps (mobile applications for learning). I would greatly appreciate if you take this survey, it takes about 10 minutes to complete and the participation is anonymous: http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/ (Answer choices are provided)

The survey has been approved by the Ryerson's Ethics Board. You have to be 18+ to participate. Click the link provided to read more information about the survey, view consent form and access the questions.

I would greatly appreciate if you share this link with your friends and contacts.

Thank you!"

Script 2:

"Hello all,

Could you please take this survey about mobile learning apps (your participation is anonymous and you can expect to complete the survey in about 10 minutes): http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/ I would greatly appreciate if you share this link with your friends and contacts. Thank you!"

Couchsurfing

"Dear Couchsurfers,

I am a Master of Management Science Candidate at the Ryerson University, and I am currently conducting a thesis research on mobile learning to meet my program requirements. To complete my research project, I have to collect and analyze quantitative data on user privacy concerns regarding the use of mobile applications for learning. To do that, I have created an online survey, which I kindly ask you to take. The participation is anonymous and voluntary. You can expect to complete this survey in 10 minutes. You have to be 18 or older to participate in this study.

For more information, to view the consent form and to take the survey, please follow this link: http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/

It would also help this research a lot if you share this link with your friends. Thanks a lot in advance for your participation!"

Reddit

- Subreddit: "SampleSize".

The SubReddit "SampleSize" is a special Reddit category for posting online surveys. This SubReddit has their own regulations to how the links should be posted. The form is as follows: "[Academic/Casual] Topic of the survey (Demographic)". If you post the same link more that one time, you have to indicate that that is a repost. Therefore, according to the rules of the SubReddit, the scripts for posting the survey are as follows:

Script 1: "[Academic] About Mobile Learning Apps (Everyone 18+)"

Script 2: "[Repost] [Academic] About Mobile Learning Apps (Everyone 18+)"

LinkedIn

"Dear friends and colleagues,

I'm collecting data about user concerns regarding the use of m-learning apps (mobile applications for learning). I would greatly appreciate if you take this survey, it takes about 10 minutes to complete and the participation is anonymous:

http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/

(Answer choices are provided)

The survey has been approved by the Ryerson's Ethics Board. You have to be 18+ to participate. Click the link provided to read more information about the survey, view consent form and access the questions.

I would greatly appreciate if you share this link with your friends and contacts.

Thank you!"

GooglePlus

"Dear friends and colleagues,

I'm collecting data about user concerns regarding the use of m-learning apps (mobile applications for learning). I would greatly appreciate if you take this survey, it takes about 10 minutes to complete and the participation is anonymous:

http://fluidsurveys.com/surveys/ryerson-RzH/m-learning-apps-user-concerns-2/

(Answer choices are provided)

The survey has been approved by the Ryerson's Ethics Board. You have to be 18+ to participate. Click the link provided to read more information about the survey, view consent form and access the questions.

I would greatly appreciate if you share this link with your friends and contacts.

Thank you!"

Appendix E – Consent Form for the Participation in the Study

Dear respondent,

Before you give your consent, please read the following information about your involvement.

You are being asked to voluntarily participate in a research study. This research study is being conducted by Daria Ilkina, a MMSc Candidate from Ted Rogers School of Management at Ryerson University.

This survey is designed to learn about your opinions and/or experience using mobile learning (m-learning) apps. In this questionnaire, m-learning app is an application that offers course materials and facilitates learning on mobile/handheld devices. For example, apps like iTunes University, Blackboard Mobile, Algebra Tutor, Lumosity, Rosetta Course, TripLingo, etc. are m-learning apps.

The results from this study will provide new insights for the m-learning app developers and designers on what are the user concerns, what is important for potential and current users of m-learning applications.

All individual responses will remain anonymous and confidential. The data may be used in scholarly and professional publications or conference presentations. The data collected through this survey will be stored securely on the researcher's computer, and then destroyed in a year after the research completion.

While the survey is online, the data will be hosted on Canadian servers. However, there is a small chance that data submitted through the site may be routed through other localities and so we cannot guarantee absolute confidentiality of data, though the data will still be anonymized.

You should expect to be able to complete this questionnaire in 10 minutes. There're minimum risks associated with the participation in this study. At most, you may feel fatigued or slightly inconvenienced after taking this survey. Should you feel uncomfortable answering any of the questions presented in this survey, you may stop your participation at any time by closing your web browser to exit the survey, effectively withdrawing your consent to participate. The information that you provided prior to the withdrawal of your consent will not be collected in case you choose to discontinue your participation in this study.

You should be 18 or older to participate in this study.

If you have any questions or comments about your participation, please contact the researcher who is conducting this study, Daria Ilkina: daria.ilkina@ryerson.ca.

You can also contact Daria Ilkina's supervisor, Dr. Avner Levin, via this email: avner.levin@ryerson.ca.

This study has been reviewed by the Ryerson University Research Ethics Board. If you have questions regarding your rights as a participant in this study please contact:

Lynn Lavallée, Ph.D.

Chair, Research Ethics Board

Associate Professor

Ryerson University EPH-200C

350 Victoria St., Toronto, ON

(416)979-5000 ext. 4791

lavallee@ryerson.ca

rebchair@ryerson.ca

http://www.ryerson.ca/research

Toni Fletcher, MA

Research Ethics Co-Ordinator

Office of Research Services

Ryerson University

(416)979-5000 ext. 7112

toni.fletcher@ryerson.ca

http://www.ryerson.ca/research

Answering Yes to the question below indicates that you have read the information in this agreement and agree with the above terms.

Do you agree to participate in this survey?

- Yes, I agree to participate in this study and I'm 18 or older.
- No, I will not participate.

Appendix F – Survey Questions

1. What is your year of birth?

_____ [Note: a selection is given in a drop-down menu in the online survey]

- Prefer not to answer

2. What is your gender?

- Female
- Male
- Other: _____ (text box for answer here)
- Prefer not to answer

3. What is your highest education degree earned?

- High school diploma
- College
- Bachelor/Undergraduate School
- Masters (of Arts, Science or other discipline)
- Doctorate
- Other: _____
- Prefer not to answer

4. Do you use or have you ever used a m-learning application?

(Reminder: in this questionnaire, m-learning app is an application that offers course materials and facilitates learning on mobile/handheld devices. For example, apps like

iTunes University, Blackboard Mobile, Algebra Tutor, Lumosity, Rosetta Course, TripLingo, etc. are m-learning apps.)

- I have previously used or am currently using m-learning applications.
- I am familiar with m-learning applications, but have never used them.
- I am not familiar with m-learning applications and have never used them.

5. How often do you use m-learning apps?

- Never
- Seldom/Rare
- Sometimes
- Often
- A lot

6. What do you use the most for accessing m-learning?

- Smartphone
- Mobile feature phone
- Tablet
- I don't use m-learning applications.
- Other: _____

7. What settings have you customized, if any, in a m-learning application? Choose everything that applies.

- Selection of courses and/or lessons
- Discussion board/communication feature
- Personalized app look (e.g., chose different colours, display look, etc.)

- Permissions
- Privacy Settings
- Other: _____
- Not applicable

8. If you have never used an m-learning application, choose the reason why from the choices below:

- I didn't want to pay for the m-learning application
- I didn't know about m-learning applications
- I didn't need to use m-learning app
- I don't own a mobile device
- The app I wanted to install is not available for my mobile device
- I didn't agree with the Terms of Use of the app
- I didn't agree with the Privacy Settings of the app
- I didn't want to give the Permissions to the app that app required me to give
- I didn't like the design of m-learning application(s)
- Other: _____
- Not applicable

9. Which of the following features you hope/expect to see in m-learning application? Choose everything that applies.

- Communication features: discussion boards/chats/forums
- Assessment, grades
- Ability to access and store data
- Ability to manage data

- Offline access
- Synchronization between devices
- Ability to customize privacy settings
- Ability to customize permissions
- Direct instruction (app as a tutor)
- Push notifications
- Accessibility features (voice over, zoom, large text, mono audio, assistive touch, etc.)
- Other: _____
- I don't know

10. Consider a situation where you have to choose a m-learning app for your study, learning or teaching goals. On the scale from 1 (Very important) to 7 (Not at all important), how important are the following factors for you in your decision-making?

	1 - Very Important	2 - Important	3 - Somewhat Important	4 - Undecided	5 - Somewhat Not Important	6 - Not Important	7 - Not At All Important
Device compatibility							
Price of the application							
App contents/ course offerings							
User ratings							
App reviews							
App popularity/ number of installs							
Application size							
Privacy Policy							
Application security							
Permissions							

11. Many applications state in their Privacy Policies that they collect some information about their users in order to "improve their services". On a scale from 1 (strongly agree) to 7 (strongly disagree), rate how much you agree that an m-learning application could collect the following information from you in order to improve the service and your experience as a user?

	1- Strongly Agree	2 - Agree	3 - Somewhat Agree	4 - Undecided	5 - Somewhat Disagree	6 - Disagree	7 - Strongly Disagree
Your name							
Your address							
Phone number							
E-mail address							
Your business contact info							
Credit card information							
Your IP address (a unique number that identifies your access account on the Internet)							
Your browser information (which typically includes browser type, version, host operating system and browser language)							
Information collected through the use of cookies							

12. Assuming the following information is collected and stored by a mobile learning application that you are using, how concerned would you be if the application shares this information with third parties, on the scale from 1 (strongly concerned), to 7 (not concerned at all)?

	1- Very concerned	2- Concerned	3- Somewhat Concerned	4- Undecided	5- Somewhat Not Concerned	6 – Not concerned	7- Not Concerned At All
Your name							
Your address							
Your shipping and billing address							
Phone number							
E-mail address							
Your business contact info							
Credit card information							
Your IP address (a unique number that identifies your access account on the Internet)							
Your browser information (which typically includes browser type, version, host operating system and browser language)							
Information collected through the use of cookies							

13. Assuming that a mobile learning application requires you to grant the following permissions for its installation and use, how concerned would you be about using an application that requires you to grant those permissions?

	1 - Very Concerned	2 - Concerned	3 - Somewhat Concerned	4 - Undecided	5 - Somewhat Not Concerned	6 - Not Concerned	7 - Not Concerned At
Access Photos							
Access Contacts							
Access Location							

Access Camera							
Access Microphone							
Access Calendar							
Access to your Reminders/Notes							
Access to your Social Network Accounts							
Access to the ability to share data via Bluetooth							
Access to the Cloud							
Access Dropbox or any other file hosting service that you use							

Next set of questions will introduce scenarios that could happen to the mobile learning application user. Assuming that any of the described situations could happen to you, how would you feel about it? (The response choices will be provided).

14. You found out that personal information that you shared with the app (e.g., name, address, telephone number, your email) is shared with independent third parties for marketing purposes. How do you feel about it?

Very concerned

- o Concerned
- o Somewhat concerned
- o Undecided
- o Somewhat not concerned
- o Not concerned
- o Not concerned at all

15. How do you feel about the fact that your usage patterns of the application (such as how often do you use the application, which courses/topics do you access the most, how

much time you spend on different tasks/topics/courses/chapters, etc.) can be shared with independent third parties for marketing purposes, but this is meta-information that cannot be linked to you personally (i.e. non-identifiable aggregated data)?

- Very concerned
- Concerned
- Somewhat concerned
- Undecided
- Somewhat not concerned
- Not concerned
- Not concerned at all

16. How do you feel about the fact that your usage patterns of the application (such as how often do you use the application, which courses/topics do you access the most, how much time you spend on different tasks/topics/courses/chapters, etc.) can be shared with independent third parties for marketing purposes if this information is personally identifiable?

- Very concerned
- Concerned
- Somewhat concerned
- Undecided
- Somewhat not concerned
- Not concerned
- Not concerned at all

17. How do you feel about the fact that any personal information that you shared with an m-learning app (e.g., name, address, telephone number, your email) can be provided to government parties at any time?

- Very concerned
- Concerned
- Somewhat concerned
- Undecided
- Somewhat not concerned
- Not concerned
- Not concerned at all

18. How do you feel about the fact that your usage patterns of the mobile learning application (such as how often do you use the application, which courses/topics do you access the most, how much time you spend on different tasks/topics/courses/chapters, etc.) can be shared with the government, but this is meta-information that cannot be linked to you personally (i.e. non-identifiable aggregated data)?

- Very concerned
- Concerned
- Somewhat concerned
- Undecided
- Somewhat not concerned
- Not concerned
- Not concerned at all

19. How do you feel about the fact that your usage patterns of the application (such as how often do you use the application, which courses/topics do you access the most, how much time you spend on different tasks/topics/courses/chapters, etc.) can be shared with the government, if this information is personally identifiable?

- Very concerned
- Concerned
- Somewhat concerned
- Undecided
- Somewhat not concerned
- Not concerned
- Not concerned at all

20. In which area do you live?

- Province of Ontario
- Other area in Canada
- Other: _____
- Prefer not to answer

21. What is your occupation?

_____ (The text box for an open answer is provided)

Thank you for your participation in this survey!

Appendix G – Study factors and items/variables for the survey

Study factors	Questions & question no.	Survey items
M-learning apps usage	4. Do you use or have you ever used a m-learning application?	Use m-learn app;
	5. How often do you use m-learning apps?	Frequency of use;
	6. What do you use the most for accessing m-learning?	Device;
	8. Why you have never used an m-learning application, if you haven't?	Reasons not a user;
The most important m-learning apps' features for the users, and the factors affecting user choice of a m-learning app	7. What settings have you customized in the m-learning applications?	Custom settings;
	9. What features you hope/expect to see in a m-learning application?	Desired features;
	10. Consider a situation where you have to choose a m-learning app for your learning or teaching goals. How important are the following factors (a list is provided) for you in your decision-making?	Device compatibility; Price; App contents; User ratings; App reviews; App popularity; Size; Privacy Policy; App security; Permissions;
User information access and data collection	11. What information you agree that m-learning application can collect from you in order to improve your user experience?	Collect name; Collect address; Collect phone number; Collect email; Collect business info; Collect credit card info; Collect IP address; Collect browser info; Collect cookies info;
	13. Assuming that a mobile learning application requires you to grant the following permissions for its installation and use, how concerned are you about using an application that requires you to grant those permissions?	Access photos; Access contacts; Access location; Access camera; Access microphone; Access calendar; Access

		notes/reminders; Access social networks; Access Bluetooth; Access cloud; Access Dropbox;
Sharing data with third parties	12. Assuming that the following information (list is provided) is collected and stored by a mobile learning application that you are using, how concerned would you be if the application shares this information with third parties?	Share name; Share address; Share shipping and billing address; Share phone number; Share email; Share business info; Share credit card info; Share IP address; Share browser info; Share cookies info;
	14. How do you feel about the m-learning app sharing your personal information with independent third parties for marketing purposes?	Share info for marketing;
	15. How do you feel about the fact that your usage patterns of the application can be shared with the independent third parties for marketing purposes if it is meta-information that cannot be linked to you personally?	Share aggregate Non-PII for marketing;
	16. How do you feel about the fact that your usage patterns of the application can be shared with the independent third parties for marketing purposes if this information is personally identifiable?	Share PII for marketing;
	17. How do you feel about the fact that any personal information that you shared with an m-learning app can be provided to government parties at any time?	Share info with gov;
	18. How do you feel about the fact that your usage patterns of the mobile learning application can be shared with the government if this is meta-information that cannot be linked to you	Share aggregate Non-PII with gov;

	personally (i.e., non-identifiable aggregated data)?	
	19. How do you feel about the fact that your usage patterns of the application can be shared with the government if this information is personally identifiable?	Share PII with gov.

Appendix H – Demographic Information of the Sample

Variables	*Number of Respondents (N)*	*Percentage of Respondents (%)*
Gender		
Female	144	55.4
Male	110	42.3
Other	3	1.2
Chose not to answer	3	1.2
Total responses	260	100
Age		
18-24	53	20.4
25-34	84	32.3
35-44	40	15.4
45-54	25	9.6
55-64	22	8.5
65+	6	2.3
Chose not to answer	30	11.5
Total responses	260	100
Highest education degree earned		
High school diploma	30	11.5
College	20	7.7
Bachelor/Undergraduate School	84	32.3
Masters (of Arts, Science or other discipline)	72	27.7
Doctorate	41	15.8
Other	12	4.6
Chose not to answer	1	.4
Total responses	260	100
Area of residence		
Ontario, Canada	187	71.9
Other area in Canada	2	.8
Other area outside of Canada	55	21.15
Chose not to answer	16	6.15
Total responses	249	93.2

Appendix I – Important Features and Settings in M-Learning Apps for the Users

Table I-1: Settings that the users have customized in their m-learning apps

Q: What settings you customized in the m-learning application (if applicable)?		
Settings/Features	**N**	**%**
Course selection	77	68
Privacy Settings	***41***	***36.3***
Permissions	***34***	***30***
Personalized app look (e.g., changed background picture, colours)	32	28.3
Discussion board / communication feature	30	26.5
Other	4	3.5
Total responses (without those who answered "Not applicable")	**113**	**100**

Table I-2: The features that the participants hope/expect to see in m-learning apps

Q: Which of the following features you hope/expect to see in m-learning apps?		
Settings/Features	**N**	**%**
Offline access	153	58.8
Assessment, grades	152	58.4
Synchronization between devices	144	55.4
Ability to customize privacy settings	***128***	***49.2***
Ability to access and store data	118	45.3
Communication features: discussion boards/chats/forums	109	41.9
Ability to manage data	104	40
Ability to customize permissions	***103***	***39.6***
Direct instruction (app as a tutor)	89	34.2
Push notifications	53	20.4
Accessibility features	68	26.2
Other	20	7.7
Total respondents	**260**	**100**

Appendix J – Tables of Means

Table J-1: The importance of m-learning apps features or functionalities for the respondents, value range from 1 – Very Important to 7 – Not At All Important.

Factors in decision-making	N (Number of respondents)	Min	Max	Mean	Std. Dev.
Device compatibility	256	1	7	1.65	1.151
App contents/course offerings	253	1	7	1.67	1.057
The price of the app	256	1	7	1.96	1.267
App security	***256***	***1***	***7***	***2.03***	***1.432***
Permissions	***253***	***1***	***7***	***2.40***	***1.454***
Privacy Policy	***256***	***1***	***7***	***2.41***	***1.606***
User ratings	256	1	7	3.03	1.510
App reviews	258	1	7	3.08	1.503
Application size	256	1	7	3.43	1.595
App popularity/number of installs	255	1	7	3.81	1.636

Table J-2: User attitude towards mobile learning apps collecting their information.

Q: How much the users agree that a mobile learning app could collect user information in order to improve its service and provide better user experience (on a scale from 1 – Strongly Agree, to 7 – Strongly Disagree)					
Type of user information collected	**N**	**Min**	**Max**	**Mean**	**Std. Dev.**
Credit card information	257	1	7	**6.27**	1.306
Phone number	255	1	7	5.86	1.472
Address	256	1	7	5.73	1.574
Business contact info	257	1	7	5.33	1.764
IP address	258	1	7	4.98	1.814
Cookies	257	1	7	4.61	1.738
Name	258	1	7	4.31	2.183
Email address	259	1	7	4.07	2.043
Browser information	257	1	7	3.86	1.975

Table J-3: Levels of users concerns when a mobile learning app shares their information with third parties.

Q: On a scale from 1 (very concerned) to 7 (not concerned at all), how concerned would you be if the m-learn app would share your information with third parties, assuming the following data is collected from you?					
Type of user information shared	**N**	**Min**	**Max**	**Mean**	**Std. Dev.**
Credit card information	260	1	7	**1.14**	**.684**
Address	258	1	6	**1.34**	**.808**
Shipping and billing address	259	1	6	**1.34**	**.803**
Phone number	259	1	7	1.40	.840
Business contact info	260	1	7	1.82	1.276
IP address	259	1	7	1.93	1.414
Email address	259	1	7	1.95	1.360
Your name	260	1	7	2.10	1.611
Cookies	257	1	7	2.39	1.573
Browser information	260	1	7	2.94	1.985

Table J-4: Levels of users concerns about a mobile learning app's permissions.

Q: On a scale from 1 (very concerned) to 7 (not concerned at all), how concerned would you be about using a mobile learning application that requires you to grant the following permissions?					
Permissions	**N**	**Min.**	**Max.**	**Mean**	**Std. Dev.**
Access Contacts	260	1	6	1.73	1.267
Access Social Network Profiles	260	1	7	1.76	1.223
Access Photos	260	1	7	1.97	1.448
Access Camera	260	1	7	2.06	1.547
Your Notes/Reminders	259	1	7	2.30	1.712
Access Dropbox or other file hosting service	259	1	7	2.32	1.706
Access Calendar	257	1	7	2.37	1.700
Access Location	259	1	7	2.46	1.612
Access Microphone	259	1	7	2.47	1.826
Access Cloud	260	1	7	2.58	1.864
Access ability to share data via Bluetooth	260	1	7	2.62	1.807

Table J-5: Users' feelings about m-learning apps' sharing their information with independent third parties for marketing purposes or with the government.

On a scale from 1 (very concerned) to 7 (not concerned at all).

Survey item	N	Min	Max	Mean	Std. Dev.
Q14. Share info for marketing	260	1	5	**1.32**	**.636**
Q15. Share aggregate Non-PII for marketing	260	1	7	**3.83**	**1.988**
Q16. Share PII for marketing	260	1	7	**1.87**	**1.417**
Q17. Share info with gov.	260	1	7	**2.01**	**1.485**
Q18. Share aggregate Non-PII with gov.	260	1	7	**3.85**	**2.015**
Q19. Share PII with gov.	260	1	7	**1.98**	**1.485**

(Q stands for "questions" with the survey question number.)

Appendix K – ANOVA Tests

Question (10): Consider a situation where you have to choose a m-learning app for your study, learning or teaching goals. On the scale from 1 (Very important) to 7 (Not at all important), how important are the following factors for you in your decision-making?

ANOVA (for gender factor)

		Sum of Squares	df	Mean Square	F	Sig.
Q10. Device compatibility	Between Groups	3.862	2	1.931	1.473	.231
	Within Groups	327.830	250	1.311		
	Total	331.692	252			
Q10. Price	Between Groups	9.613	2	4.807	3.018	**.051**
	Within Groups	398.134	250	1.593		
	Total	407.747	252			
Q10. Contents/ course offerings	Between Groups	4.789	2	2.395	2.143	***.119***
	Within Groups	275.967	247	1.117		
	Total	280.756	249			
Q10. User ratings	Between Groups	1.223	2	.611	.268	.765
	Within Groups	571.109	250	2.284		
	Total	572.332	252			
Q10. App reviews	Between Groups	2.601	2	1.301	.574	.564
	Within Groups	571.140	252	2.266		
	Total	573.741	254			
Q10. App popularity	Between Groups	.767	2	.384	.143	.867
	Within Groups	667.550	249	2.681		
	Total	668.317	251			
Q10. Size	Between Groups	69.970	2	34.985	15.435	**.000**
	Within Groups	566.663	250	2.267		
	Total	636.632	252			
Q10. Privacy Policy	Between Groups	27.837	2	13.918	5.576	**.004**
	Within Groups	624.061	250	2.496		
	Total	651.897	252			
Q10. App security	Between Groups	9.438	2	4.719	2.312	***.101***
	Within Groups	510.167	250	2.041		

	Total	519.605	252			
Q10. Permissions	Between Groups	6.396	2	3.198	1.513	.222
	Within Groups	522.168	247	2.114		
	Total	528.564	249			

Descriptives

		N	Mean	Std. Dev.	Std. Error	95% Confidence Interval for Mean		Min.
						Lower Bound	Upper Bound	
Q10. Device compatibility	Female	141	1.55	.944	.080	1.40	1.71	1
	Male	109	1.75	1.334	.128	1.50	2.01	1
	Other	3	2.33	2.309	1.333	-3.40	8.07	1
	Total	253	1.65	1.147	.072	1.51	1.79	1
Q10. Price	Female	141	1.80	1.064	.090	1.62	1.98	1
	Male	109	2.17	1.488	.142	1.88	2.45	1
	Other	3	2.67	.577	.333	1.23	4.10	2
	Total	253	1.97	1.272	.080	1.81	2.13	1
Q10. Size	Female	141	2.99	1.355	.114	2.77	3.22	1
	Male	109	4.06	1.688	.162	3.73	4.38	1
	Other	3	3.00	1.000	.577	.52	5.48	2
	Total	253	3.45	1.589	.100	3.25	3.65	1
Q10. Privacy Policy	Female	141	2.13	1.400	.118	1.90	2.37	1
	Male	109	2.81	1.787	.171	2.47	3.15	1
	Other	3	2.33	1.528	.882	-1.46	6.13	1
	Total	253	2.43	1.608	.101	2.23	2.63	1
Q10. App security	Female	141	1.87	1.241	.105	1.67	2.08	1
	Male	109	2.24	1.627	.156	1.93	2.55	1
	Other	3	2.67	2.082	1.202	-2.50	7.84	1
	Total	253	2.04	1.436	.090	1.86	2.22	1
Q10. Permissions	Female	138	2.27	1.270	.108	2.05	2.48	1
	Male	109	2.59	1.645	.158	2.27	2.90	1
	Other	3	2.67	2.082	1.202	-2.50	7.84	1
	Total	250	2.41	1.457	.092	2.23	2.59	1

ANOVA (for age factor)

		Sum of Squares	df	Mean Square	F	Sig.
Q10. Device compatibility	Between Groups	3.061	4	.765	.586	.673
	Within Groups	288.620	221	1.306		
	Total	291.681	225			
Q10. Price	Between Groups	20.779	4	5.195	3.367	.011
	Within Groups	340.937	221	1.543		
	Total	361.717	225			
Q10. Contents/ course offerings	Between Groups	2.128	4	.532	.454	.769
	Within Groups	255.316	218	1.171		
	Total	257.444	222			
Q10. User ratings	Between Groups	3.943	4	.986	.435	.783
	Within Groups	500.288	221	2.264		
	Total	504.230	225			
Q10. App reviews	Between Groups	11.558	4	2.889	1.264	.285
	Within Groups	511.927	224	2.285		
	Total	523.485	228			
Q10. App popularity	Between Groups	4.902	4	1.226	.443	.777
	Within Groups	608.538	220	2.766		
	Total	613.440	224			
Q10. Size	Between Groups	10.695	4	2.674	1.061	.376
	Within Groups	556.672	221	2.519		
	Total	567.367	225			
Q10. Privacy Policy	Between Groups	7.896	4	1.974	.754	.556
	Within Groups	578.600	221	2.618		
	Total	586.496	225			
Q10. App security	Between Groups	3.986	4	.996	.477	.752
	Within Groups	461.417	221	2.088		
	Total	465.403	225			
Q10. Permissions	Between Groups	9.955	4	2.489	1.166	.327
	Within Groups	465.300	218	2.134		
	Total	475.256	222			

Post Hoc Test

Multiple Comparisons

Bonferroni

Dependent Variable	(I) Age Group	(J) Age Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Q10. Price	18-24	25-34	-.163	.220	1.000	-.79	.46
		35-44	-.154	.263	1.000	-.90	.59
		45-54	-.908*	.302	.030	-1.76	-.05
		55+	-.715	.295	.160	-1.55	.12
	25-34	18-24	.163	.220	1.000	-.46	.79
		35-44	.009	.241	1.000	-.67	.69
		45-54	-.745	.283	.092	-1.55	.06
		55+	-.552	.275	.461	-1.33	.23
	35-44	18-24	.154	.263	1.000	-.59	.90
		25-34	-.009	.241	1.000	-.69	.67
		45-54	-.754	.318	.187	-1.66	.15
		55+	-.561	.311	.724	-1.44	.32
	45-54	18-24	.908*	.302	.030	.05	1.76
		25-34	.745	.283	.092	-.06	1.55
		35-44	.754	.318	.187	-.15	1.66
		55+	.193	.345	1.000	-.78	1.17
	55+	18-24	.715	.295	.160	-.12	1.55
		25-34	.552	.275	.461	-.23	1.33
		35-44	.561	.311	.724	-.32	1.44
		45-54	-.193	.345	1.000	-1.17	.78

*. The mean difference is significant at the 0.05 level.

Question (13): Assuming that a mobile learning application requires you to grant the following permissions for its installation and use, how concerned would you be about using an application that requires you to grant those permissions? On a scale from 1 – Very concerned, to 7 – Not at all concerned.

ANOVA (for gender factor)

		Sum of Squares	df	Mean Square	F	Sig.
Access Photos	Between Groups	6.269	2	3.135	1.536	.217
	Within Groups	518.260	254	2.040		
	Total	524.529	256			
Access Contacts	Between Groups	2.796	2	1.398	.863	.423
	Within Groups	411.678	254	1.621		
	Total	414.475	256			
Access Location	Between Groups	10.647	2	5.323	2.056	.130
	Within Groups	655.103	253	2.589		
	Total	665.750	255			
Access Camera	Between Groups	3.641	2	1.820	.757	.470
	Within Groups	610.484	254	2.403		
	Total	614.125	256			
Access Microphone	Between Groups	2.279	2	1.140	.339	.713
	Within Groups	851.623	253	3.366		
	Total	853.902	255			
Access Calendar	Between Groups	.015	2	.008	.003	.997
	Within Groups	735.701	251	2.931		
	Total	735.717	253			
Access Notes/Reminders	Between Groups	2.836	2	1.418	.479	.620
	Within Groups	749.398	253	2.962		
	Total	752.234	255			
Access Social Networks	Between Groups	.810	2	.405	.268	.765
	Within Groups	383.711	254	1.511		
	Total	384.521	256			
Access Bluetooth	Between Groups	31.260	2	15.630	4.908	**.008**
	Within Groups	808.880	254	3.185		
	Total	840.140	256			
Access Cloud	Between Groups	46.870	2	23.435	7.072	**.001**
	Within Groups	841.745	254	3.314		

	Total	888.615	256			
Access Dropbox	Between Groups	7.592	2	3.796	1.311	.271
	Within Groups	732.498	253	2.895		
	Total	740.090	255			

Descriptives

		N	Mean	Std. Dev.	Std. Error	95% Confidence Interval for Mean		Minimum
						Lower Bound	Upper Bound	
Access Bluetooth	Female	144	2.36	1.549	.129	2.11	2.62	1
	Male	110	3.01	2.065	.197	2.62	3.40	1
	Other	3	1.33	.577	.333	-.10	2.77	1
	Total	257	2.63	1.812	.113	2.40	2.85	1
Access Cloud	Female	144	2.22	1.601	.133	1.95	2.48	1
	Male	110	3.07	2.084	.199	2.68	3.47	1
	Other	3	2.00	1.000	.577	-.48	4.48	1
	Total	257	2.58	1.863	.116	2.35	2.81	1

Question (12): Assuming the following information is collected and stored by a mobile learning application that you are using, how concerned would you be if the application shares this information with third parties, on the scale from 1 – strongly concerned, to 7 – not concerned at all.

Descriptives

		N	Mean	Std. Dev	Std. Error	95% Confidence Interval for Mean		Min.	Max.
						Lower Bound	Upper Bound		
Share phone number	High school diploma	34	1.85	1.306	.224	1.40	2.31	1	7
	College	21	1.57	1.121	.245	1.06	2.08	1	6
	Undergrad School	87	1.38	.633	.068	1.24	1.51	1	3
	Masters	75	1.31	.805	.093	1.12	1.49	1	5
	Doctorate	40	1.18	.446	.071	1.03	1.32	1	3
	Total	257	1.40	.843	.053	1.30	1.51	1	7
Share email	High school diploma	34	2.82	1.678	.288	2.24	3.41	1	7
	College	21	2.19	1.601	.349	1.46	2.92	1	6
	Undergrad School	87	2.01	1.402	.150	1.71	2.31	1	7
	Masters	74	1.73	1.150	.134	1.46	2.00	1	6
	Doctorate	41	1.39	.737	.115	1.16	1.62	1	4
	Total	257	1.95	1.363	.085	1.79	2.12	1	7

Note: More tables with the ANOVA tests results are available upon request. You can contact the researcher for more information on this analysis at: daria.ilkina@ryerson.ca

Reference List

AllAboutCookies.org. (2014). *Privacy Concerns on Cookies.* URL: http://www.allaboutcookies.org/privacy-concerns/. Retrieved April 21, 2014.

Apple Legal (2014). *Privacy Policy.* URL: http://www.apple.com/legal/privacy/en-ww/. Retrieved April 28, 2014.

Apple Press Info (2007). *Apple Announces iTunes U on the iTunes Store.* URL: https://www.apple.com/pr/library/2007/05/30Apple-Announces-iTunes-U-on-the-iTunes-Store.html. Retrieved June 15, 2014.

Article 29 Data Protection Working Party (2013). *Opinion 02/2013 on apps and smart devices.* 00461/13/EN, WP 202, pp. 1-27. Adopted on 27 February 2013.

Ayoma, M., & Oboko, R. (2013). *M-learning support services for corporate learning.* International Journal of Societal Applications of Computer Science, Vol. 2, Issue 2, February 2013, ISSN 2319-8443.

Birnhack, M. (2013). *Reverse Engineering Informational Privacy Law.* Yale Journal of Law and Technology, Vol. 15, Issue 1, Article 3, pp. 23-91.

Birnhack, M., Toch, E., Hadar, I. (2014). *Privacy Mindset, Technological Mindset.* 55 Jurimetrics 55-114.

Blank, G., Bolsover, G., Dubois, E. (2014). *A New Privacy Paradox: Young people and privacy on social network sites.* Global Cyber Security Capacity Centre: Draft Working Paper. Oxford Internet Institute. URL: http://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf Retrieved March 18, 2015.

Bruck, P.A., Motiwalla, L., Foerster,F. (2012). *Mobile Learning with Micro-content: A Framework and Evaluation.* Conference proceeding at 25th Bled eConference eDependability: Realiable and Trustworthy eStructures, eProcesses, eOperations and eServices for the Future. June 17-20, 2012, Bled, Slovenia, pp. 527-543.

Canvas' Privacy Policy. (2014). *Instructure Paid Canvas Privacy Policy.* URL: http://www.instructure.com/policies/privacy-policy. Retrieved October 27, 2014.

Cavoukian, A. (2011). *Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private.* Information and Privacy Commissioner, Ontario, Canada. URL: http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf. Retrieved April 25, 2014.

Cavoukian, A. (2012). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices.* Information and Privacy Commissioner, Ontario, Canada: Toronto.

Cavoukian, A. (2013a). *Privacy by Design.* Information and Privacy Commissioner of Ontario, Canada: Toronto.

Cavoukian, A. (2013b). *Safeguarding Privacy on Mobile Devices.* Information and Privacy Commissioner, Ontario, Canada: Toronto.

Cavoukian, A. Bansal, N., Koudas, N. (2014). *Building Privacy into Mobile Location Analytics (MLA) Through Privacy by Design.* Information and Privacy Commissioner, Ontario, Canada. URL: http://www.ipc.on.ca/images/Resources/pbd-mla.pdf. Retrieved April 25, 2014.

Cavoukian, A., Jutla, D. (2014). *Privacy Policies Are Not Enough: We Need Software Transparency.* Privacy Perspectives. Information and Privacy Commissioner, Ontario, Canada. URL: https://privacyassociation.org/news/a/privacy-policies-are-not-enough-we-need-software-transparency/. Retrieved July 27, 2014.

Cavoukian, A., Prosch, M. (2010). *The Roadmap for Privacy by Design. In Mobile Communications: A Practical Tool for Developers, Service Providers, and Users.* In Privacy By Design: From Rhetoric To Reality (2014), pp. 101-129.

Cavoukian, A., Reed, D. (2013). *Big Privacy: Bringing Big Data and the Personal Data Ecosystem Through Privacy by Design.* Office of the Information and Privacy Commissioner, Ontario, Canada. Respect Network Corporation: San Francisco.

Cavoukian, A., Weiss, J.B. (2012). *Privacy by Design and User Interfaces: Emerging Design Criteria – Keep it User-Centric.* Information and Privacy Commissioner, Ontario, Canada. URL: http://www.ipc.on.ca/images/Resources/pbd-user-interfaces_Yahoo.pdf. Retrieved April 25, 2014.

Cheon, J., Lee, S., Crooks, S.M., Song, J. (2012). *An investigation of mobile learning readiness in higher education based on the theory of planned behavior.* Computers & Education, 59 (2012), pp. 1054-1064.

Chong, J.-L., Chong, A.Y.-L., Ooi, K.-B., Lin, B. (2011). *An empirical analysis of the adoption of m-learning in Malaysia.* International Journal of Mobile Communications, Vol. 9, No.1, 2011, pp. 1-18.

Cohen, T. (2014). *Office of the Privacy Commissioner of Canada News Release: Global privacy sweep raises concerns about mobile apps.* URL: https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp. Retrieved September 13, 2014.

Crescente, M.L., & Lee, D. (2011). *Critical issues of m-learning: design models, adoption processes, and future trends.* Journal of the Chinese Institute of Industrial Engineers Vol. 28, No. 2, March 2011, pp. 111–123.

Crompton, H. (2013). A historical overview of mobile learning: Toward learner-centered education. In Z. L. Berge & L. Y. Muilenburg (Eds.), Handbook of mobile learning, Florence, KY: Routledge, pp. 80-107.

Cürses, S., Troncoso, C., Diaz, C. (2011). *Engineering Privacy by Design.* Proceeding from the Conference on Computers, Privacy & Data Protection, January 25-28, 2011. URL: https://lirias.kuleuven.be/bitstream/123456789/356730/1/article-1542.pdf. Retrieved October 28, 2014.

Davis, F. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly, Vol. 13, No. 3 (Sep., 1989), pp. 319-340.

De Waard, I. (2013). *Analyzing the impact of mobile access on learner interactions in a MOOC* (a Master of Education thesis). Athabasca University, Faculty of Graduate Studies, February 2013.

De Waard, I., Koutropoulos, A., Keskin, N.O., Abajian, S.C., Hogue, R., Rodriguez, O.C., Gallagher, M.S. (2011). *Exploring the MOOC format as a pedagogical approach for mLearning.* Proceeding from the MLearn 2011 – 10th World Conference on Mobile and Contextual Learning. Beijing, China, 18-21 October 2011.

Dong, Y., Peng, C.-Y. J. (2013). Principled missing data methods for researchers. SpringerPlus 2013, 2:222, pp. 1-17. URL: http://www.springerplus.com/content/pdf/2193-1801-2-222.pdf. Retrieved October 29, 2014.

Educause (2010). *7 Things You Should Know About… Mobile Apps for Learning.* URL: http://net.educause.edu/ir/library/pdf/ELI7060.pdf. Retrieved June 10, 2014.

Elias, T. (2013). *Universal instructional design principles for mobile learning. In Global Mobile Learning Implementations and Trends* (pp. 61-73). China Central Radio & TV University Press: Beijing.

Fekete, M. (2012). *App Developers Take Notice: Privacy Guidelines for Mobile Apps Released*. URL: http://www.osler.com/NewsResources/App-Developers-Take-Notice-Privacy-Guidelines-for-Mobile-Apps-Released/?langtype=4105 Retrieved March 17, 2015.

Garg, A. (2013). *Planning for Mobile Learning Implementation.* In *Global Mobile Learning Implementations and Trends* (pp. 74-85). China Central Radio & TV University Press: Beijing.

Garrison, D. R., Anderson, T. (2003). *E-learning in the 21st century: A framework for research and practice.* RoutledgeFalmer: London.

Gong, Z., Wallace, J.D. (2012). *A comparative analysis of iPad and other m-learning technologies: Exploring students' view of adoption, potentials, and challenges.* Journal of Literacy and Technology, Vol. 13, No. 1, February 2012, pp. 2-29.

Gould, J., Biron, L. (2012). *Security Concerns Hobble U.S. Army's Mobile Learning.* URL: http://www.defensenews.com/print/article/20120620/TSJ01/306200004/Security-Concerns-Hobble-U-S-Army-8217-s-Mobile-Learning. Retrieved March 13, 2014.

Guri-Rosenblit, S. (2005). *'Distance education' and 'e-learning': Not the same thing.* Higher Education, 49, pp. 467-493. Springer.

Haag, J. (2011). *From eLearning to mLearning: The Effectiveness of Mobile Course Delivery.* Proceeding from the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2011.

Information and Privacy Commissioner, Ontario, Canada. (2014). *Privacy: Introduction to PbD.* URL: http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/ Retrieved August 2, 2014.

Kadirire, J. (2009). Mobile Learning DeMystified. In R. Guy (Ed) *The Evolution of Mobile Teaching and Learning.* California, USA: Informing Science Press.

Kam, R. (2012). *The lifecycle of PHI and mobile device insecurity.* Government Health IT. URL: http://www.govhealthit.com/news/lifecycle-phi-and-mobile-device-insecurity#.U8hD44BdV1R Retrieved April 18, 2014.

Kambourakis, G. (2013). *Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art.* International Journal of u- and e- Service, Science and Technology. Vol. 6, No. 3, pp. 67-84.

Keskin, N.O., & Metcalf, D. (2011). *The current perspectives, theories and practices of mobile learning.* TOJET: The Turkish Online Journal of Educational Technology. April 2011, Vol. 10, Issue 2.

Liaw, S. S., Hatala, M., & Huang, H. M. (2010). *Investigating acceptance toward mobile learning to assist individual knowledge management: Based on activity theory approach.* Computers & Education, 54(2), pp. 446-454.

Liccardi, I., Bulger, M., Abelson, H., Weitzner, D.J., Mackay, W. (2014). *Can apps play by the COPPA Rules?* Proceeding from the Twelfth Annual Conference on Privacy, Security and Trust (PST), IEEE 2014, pp. 1-9.

Liu, Y., Li, H., Carlsson, C. (2010). *Factors driving the adoption of m-learning: An empirical study.* Computers & Education, 55 (2010), pp. 1211-1219.

Mallikharjuna Rao, N., Sasidhar, C., Sathyendra Kumar, V. (2010). *Cloud Computing Through Mobile-Learning.* International Journal of Advanced Computer Science and Applications (IJACSA). Vol.1, No.6, December 2010, pp. 42-47.

Marwan, M.E., Madar, A.R., Fuad, N. (2013). *An overview of mobile application in learning for student of Kolej Poly-Tech Mara (KPTM) by using mobile phone.* Journal of Asian Scientific Research, 2013, 3(6), pp. 527-537.

Maske, P., Guhr, N., Köpp, C., Breitner, M.H. (2011). *Towards a sustainable business model for mobile learning services.* URL: http://is2.lse.ac.uk/asp/aspecis/20110249.pdf. Retrieved January 4, 2014.

McConatha, D., & Praul, M. (2007). *Mobile Learning in the Classroom: An Empirical Assessment of a New Tool for Students and Teachers.* A paper (to be) presented at the Society for Applied Learning Technology's Washington Interactive Technologies Conference Sheraton Crystal City Hotel Arlington, Virginia August 22-24, 2007.

Miller, C., Doering, A. (Editors). (2014). *The New Landscape of Mobile Learning: Redesigning Education in an App-based World.* Routledge: New York.

Mohammad, S., & Job, M.A. (2013). *Adaption of M-learning as a tool in blended learning – A case study in AOU Bahrain.* International Journal of Science and Technology. Vol. 3, No. 1, January 2013, pp.14-20.

Mulligan, D.K., King, J. (2012). *Bridging the Gap Between Privacy and Design.* Journal of Constitutional Law, Vol 14(4), pp. 989-1034.

Nasiri, A., Deng, G. (2009). *Environmental factors influence on mobile learning business.* American Journal of Applied Sciences 6 (6), pp. 1225-1234.

OPC Fact Sheets. (2014). *Ten Tips for Communicating Privacy Practices to Your App's Users.* The Office of the Privacy Commissioner of Canada. URL: https://www.priv.gc.ca/resource/fs-fi/02_05_d_61_tips_e.asp. Retrieved October 5, 2014.

Paliwal, S., Sharma, K.K. (2009). *Future trend of education – mobile learning problems and prospects.* Conference proceeding at International Conference on Academic Libraries (ICAL) 2009.

Park, S.Y., Nam, M.W., Cha, S.B. (2012). *University students' behavioral intention to use mobile learning: Evaluating the technology acceptance model.* British Journal of Educational Technology, Vol.43, No.4, pp. 592-605.

Privacy by Design (2014). *PbD official website.* URL: http://www.privacybydesign.ca/. Retrieved April 10, 2014.

QLeanr Privacy Policy. (2014). *Privacy Policy.* URL: http://pages.qualcomm.com/qlearn-privacy.html. Retrieved April 28, 2014.

Ryerson University. (2014). *Research & Innovation.* Human Ethics - Frequently Asked Questions (FAQ). URL: http://www.ryerson.ca/research/services/ethics/human/faq.html. Retrieved July 25, 2014.

Saccol, A.Z., Reinhard, N., Schlemmer, E., Barbosa, J.L.V. (2010). *M-Learning (Mobile Learning) in Practice: A Training Experience with IT Professionals.* Journal of Information Systems and Technology Management, Vol. 7, No. 2, pp. 261-280.

Schroeder, B. (2013). *Mobile and Digital: Perspectives on teaching and learning in a networked world.* In *Global Mobile Learning Implementations and Trends* (pp. 105-118). China Central Radio & TV University Press: Beijing.

Sharples, M. (2006). *Big Issues in Mobile Learning: Report of a workshop by the Kaleidoscope Network of Excellence Mobile Learning Initiative.* University of Nottingham, 2006.

Sharples, M., Taylor, J., & Vavoula, G. (2005). *Towards a theory of mobile learning.* Proceedings from mLearn 2005, 1(1), pp. 1-9.

Shiliang, L., Hongtao, S. (2013). *Changing the Way of Learning: Mobile Learning in China.* In *Global Mobile Learning Implementations and Trends* (pp. 141-155). China Central Radio & TV University Press: Beijing.

Song, J.E., Erdem, M. (2011). *M-learning in Hospitality: An Exploration of Older Workers' Needs and Attitudes.* Workforce Education & Leadership. University of Nevada: Las Vegas.

Spiekermann, S. (2012). *Viewpoint: The Challenges of Privacy by Design.* Communications of the ACM, July 2012, Vol. 55 (7), pp. 38-40.

Sweatt, B., Paradesi, S., Liccardi, I., Kagal, L., Pentland, A. (2014). *Building Privacy-preserving Location-based apps.* Proceeding from the Twelfth Annual Conference on Privacy, Security and Trust (PST), IEEE 2014, pp. 27-30.

Symantec. (2014). *Internet Security Threats Report 2014.* 2013 Trends, Volume 19. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf Retrieved June 10, 2014.

Tan, Q. & El-Bendary, N. (2013). *Location-based learning with mobile devices.* In *Global Mobile Learning Implementations and Trends* (pp. 169-186). China Central Radio & TV University Press: Beijing.

Towards Maturity. (2013). *Mobile Learning at Work: Practical perspectives to help implement mobile technologies effectively.* URL: www.towardsmaturity.org/mobile2013. Retrieved April, 04, 2014.

Training Force. (2014). *What is a Learning Management System?* URL: http://trainingforce.com/kb/what-is-a-lms. Retrieved March 12, 2014.

Traxler, J. (2013). *Mobile learning in international development.* In *Global Mobile Learning Implementations and Trends* (pp. 45-60). China Central Radio & TV University Press: Beijing.

Uden, L. (2007). *Activity theory for designing mobile learning.* International Journal of Mobile Learning and Organisation, 1(1), 81-102.

Ugray, Z. (2009). *Security and privacy issues in mobile learning.* International Journal of Mobile Learning and Organizations, Vol. 3, No.2, pp. 202-218.

Uzunboylu, H., Ozdamli, F. (2011). *Teacher perception for m-learning: scale development and teachers' perceptions.* Journal of Computer Assisted Learning (2011), 27, pp. 544-556.

Vavoula, G. & Sharples, M. (2009). *Meeting the Challenges in Evaluating Mobile Learning: a 3-level Evaluation Framework.* International Journal of Mobile and Blended Learning, Vol.1, No.2, pp. 54-75.

Verma, K., Dubey, S., Rizvi, M.A. (2012). *Mobile Cloud A New Vehicle For Learning: m-Learning Its Issues And Challenges.* International Journal of Science and Applied Information Technology. Vol.1, No.3, July-August 2012, pp. 93-97.

Wu, W.-H., Wu, Y.-C. J., Chen, C.-Y., Kao, H.-Y., Lin, C.-H., Huang, S.H. (2012). *Review of trends from mobile learning studies: A meta-analysis.* Computers & Education, 59 (2012), pp. 817-827.

Glossary

Android: An open-source mobile operating system based on the Linux kernel and currently developed by Google.

Cookies: Simple uncompiled text files that help coordinate the remote website servers and a user's browser to display the full range of features (such as automatic logins and authentication, language settings, preference settings, third party advertisement serving, ad management, shopping cart functionalities, etc.) offered by most of the contemporary websites.

Data encryption: The act of changing electronic information into an unreadable state by using algorithms or ciphers, i.e., the conversion of data into a ciphertext that cannot be easily understood by unauthorized people.

E-Learning: A networked, online learning that takes place in a formal context and uses a range of multimedia technologies.

Feature phone: A mobile phone that incorporates features such as the ability to access the Internet and store and play music but lacks the advanced functionality of a smartphone.

FluidSurveys: Online survey software tool.

iOS: Apple's operational system developed for mobile devices.

IP address: A unique number that identifies a user's access account on the Internet.

Learning Management System (LMS): A software application used for delivery and management of learning content and resources.

M-Learning application: There are many applications that can facilitate mobile learning or help users organise their learning process on mobile device (e.g. sort digital files, bookmarking and/or highlighting, sharing files, making notes, etc.); however, for

the purposes of this research, I considered only applications that offer course materials for m-learning.

Mobile application: An application software designed to run on mobile devices.

Mobile device: In the context of this study, *mobile devices* are all portable handheld computing devices such as smartphones, mobile feature phones, tablets or any other personal digital assistants (PDAs).

Non-personally identifiable information (Non-PII): Any information about an individual that cannot be directly linked to him/her, i.e., cannot be used to identify a person.

Personally identifiable information (PII): Any information that may be used to identify an individual.

Privacy by Design (PbD): Privacy by Design is a concept developed by Ann Cavoukian in the 1990s to address growing and systemic effects of the ICTs and the large-scale networked data systems. According to PbD principles, privacy protection cannot rely solely on regulations and public policies, but the privacy assurance must become an organization's default mode of operation.

VPN or Virtual Private Network: A private network that uses another public network (usually the internet) to connect multiple users. Enables users to connect to the private network from a public network without sacrificing security concerns.

Web Beacons (also called web bugs and clear GIFs): used in combination with cookies to help people running websites to understand the behaviour of their customers. A web beacon is typically a transparent graphic image (usually 1 pixel x 1 pixel) that is placed on a site or in an email. (Source: AllAboutCookies.org, 2014.)