Developing a pedagogical model to improve higher education students' online privacy management strategies

by

Choy, Mei Chun

A Thesis Submitted to

The Education University of Hong Kong

in Partial Fulfilment of the Requirement for

the Degree of Doctor of Education

March 2021

Statement of Originality

I, CHOY, Mei Chun, hereby declare that I am the sole author of this thesis, and the material presented in this thesis is my original work except those indicated in the acknowledgement. I further declare that I have followed the University's policies and regulations on academic honesty, copyright and plagiarism in writing the thesis, and no material in this thesis has been submitted for a degree in this or other universities.

Abstract

According to the statistics provided by the Office of the Communications Authority of the government of Hong Kong SAR, mobile subscriber penetration rate in Hong Kong is 286.6% (2021). This figure indicates that mobile devices have become ubiquitous as Hong Kong people are increasingly using them to surf the Internet. Although smartphones and tablets, the two most popular categories of mobile devices, provide prevailing features for users in this information age, they also become prevailing targets for collecting users' personal data. As higher education institution (HEI) students are usually active users of mobile devices for surfing the Internet, visiting social networking platforms, using instant messaging applications (hereinafter 'apps') and making online purchases, this research, as an exploratory study, investigated their online privacy concerns.

This study aims at providing background information and insight for educators to enhance existing privacy education and also for policymakers in developing privacy policy in tertiary level and thus elevate students' concerns on protecting their online personal data privacy while using mobile devices.

Communication privacy management theory developed by Petronio (2002, 2013) was employed in this study to design the teaching materials including teaching notes and student assignments. Design-based research (DBR) approach with convergent mixed method design was adopted in this study as the mixed methods approach is able to maximise the validity and increases the objectivity and reliability of the current research. In addition, most DBR literature agree that the mixed methods approach is proper for collecting and analysing data (Alghamdi & Li, 2013; Bell, 2004; Design-Based Research Collective, 2003; Wang & Hannafin, 2005). Therefore, in DBR methodology, qualitative and quantitative research methods were adopted to address the research questions (Bogdan & Biklen, 2006; Li & Chu, 2018; MacDonald, 2008). To collect quantitative data, a set of self-administrated questionnaires were given to 124 HEI students who were studying in a private university in Hong Kong in 2018. In the collection of qualitative data, eight participating students were invited to join the post-teaching interviews. In this study, the DBR approach includes four iterations or teaching rounds. The foundation round was first conducted to explore an initial pedagogical model, then three enhancement rounds were arranged to obtain the final pedagogical model. Findings showed that the pedagogical model, which included case video teaching, designated CPM-based teaching materials and student assignment, was a relatively effective model to develop HEI students' privacy management strategies.

This research also revealed that, for HEI students with better privacy attitudes, the privacy attitude and privacy behaviour were unrelated when they are using their mobile devices. This contradicting phenomenon could be explained by the privacy paradox.

Keywords: Online privacy, Communication Privacy Management, privacy paradox, Designed-based Research, privacy attitude.

Acknowledgements

I would like to express my heartfelt thanks to my principal supervisor Dr. Lai, Yiu Chi for his generous, constructive feedback and advice and patient support on the long and demanding journey in my doctoral study. I also want to thank my associate supervisors Dr. Song, Yanjie, Dr. Sun, Daner and my external associate supervisor Dr. Wu Keung Fai, Joseph, for their concern and insightful comments.

Moreover, I express my eternal gratitude to my family for their unwavering encouragement, unconditional support and constant patience throughout this endeavour. My family always stands by me to share my happiness in every progress I have made and cheers me up in every challenge I faced in the journey. Their utmost solicitude fosters my unremitting efforts in my academic pursuits. My deepest gratitude goes to my adoring mother and my brother. I dedicate this thesis to my beloved family.

Table of Content

List of Abbreviations

5G	Fifth-Generation Wireless Telephone Technology
CPM	Communication Privacy Management
DBR	Design-based Research
DPP	Data Protection Principle
EDB	The Education Bureau of Hong Kong
ER1	Enhancement Round 1
ER2	Enhancement Round 2
ER3	Enhancement Round 3
FR	Foundation Round
HSUHK	The Hang Seng University of Hong Kong
IM	Instant Messaging
LMS	Learning Management System
Mobile App	Mobile Application Software
OPA	Online Privacy Attitude
OPMS	Online Privacy Management Strategies
PCPD	The Office of the Privacy Commissioner for Personal Data
PIP	Personal Information Privacy
SNS	Social Networking Site
SPSS	Statistical Package for Social Sciences

List of Tables

List of Figures

Chapter 1 Introduction

1.1 Background of the Study

One undeniable feature that makes mobile devices extremely popular is its portability which allows users to connect to the Internet anytime and anywhere (Alzahrani, Alalwan & Sarrab, 2014). Notably, mobile devices dominate Internet usage (comScore, 2016; eMarketer, 2016; Ericsson, 2019; Smith, 2015). As desktop usage for Internet access drops from 47% to 35%, the time spent by Internet users visiting digital media via mobile devices reaches 65%, and the majority are using mobile apps (comScore, 2016). Smartphones play a vital role among mobile devices more than tablets and e-readers. Research estimated that the number of smartphone users will increase from 7.9 billion in 2019 to 8.8 billion by 2024 (Ericsson, 2019).

According to the statistics provided by the Office of the Communications Authority (2021) of Hong Kong SAR, mobile subscriber penetration rate in Hong Kong is 286.6%. This figure points out that mobile devices have become ubiquitous as Hong Kong people are increasingly using them to connect to the Internet. This finding is in line with the global trend. Given that smartphones and tablets, the two major categories of most popular mobile devices, provide excellent features for users, they have become top targets for data collection. With the rapid development of information and communication technologies, marketers are becoming increasingly competent in collecting and analysing online customers' data and thus in creating their individual personal profiles to set up more effective marketing strategies for higher monetary gains (Vesanen, 2007).

The rapid development of big data technologies brings forth a new era of information age. Sectors like media, education, healthcare, and economic are the beneficiaries. Through collecting, analysing, processing and aggregating individuals' data, they can produce better solutions and predications for decision making (Couldry & Turow, 2014; Huser & Cimino, 2015; Kshetri, 2014). However, a growing body of research noticed that these big data technologies unquestionably worsened the problem of privacy invasion (Kshetri, 2014; Paul, 2012). The era of big data is not only characterised by massive opportunities for social progress, but also bountiful information security threats, elevating the concern of personal data protection. Inevitably, strengthening professional private information security technologies and individuals' awareness of privacy protection is a prerequisite for privacy protection of big data information and the implementation of privacy information security (Zhang, 2018).

The Office of the Australian Information Commissioner of the Australian government (2014) has put vast effort to protect their citizens' personal information, which may be collected by mobile devices, by establishing a set of guidelines called 'Mobile privacy: a better practice guide for mobile App developers' to help all mobile application developers better observe Australian privacy law and best practice while developing their mobile apps.

The next generation mobile network, 5G, will unveil a new age of technology. Ericsson (2019) reported that 5G will cover up to 65% of the world's population by the end of 2025 with 2.6 billion subscriptions. However, concerns regarding data privacy under the expansion of 5G network have been raised. The issue on Huawei is a hot topic in recent years. The U.S. government worries that if Huawei is allowed to install the key elements of 5G networks in the country, Huawei may spy on the traffic passing through them (Reuters, 2019). Another concern is about wearable devices and smart appliances (MarTeach Advisor, 2019). If they were connected to a 5G network and transmitted personal and sensitive information, such as heart rate or personal medical data, through the network, these data may be spied as well. Location data are an alarming privacy concern with 5G Internet. The coverage area of 5G is smaller than that of 4G. Hence, more cellular towers need to be installed within a smaller radius. MarTech Advisor pointed out that under a 5G network, mobile operators can track their users' location or movement trail very precisely. Besides, the detailed data of users could be sold to or even stolen by third parties.

Several Hong Kong news outlets reported that some app companies have seriously invaded users' privacy. Specifically, three 'call blocker' mobile apps collect users' contacts and integrate them to form a public database that contains approximately 3 billion users' personal information with their identities, and allows users to track the identity of a phone number's holder and even his or her social networking site (SNS) account (Apple Next Media, 2016). In addition, the mobile check-app of Hong Kong Airlines is accused of violating passengers' privacy because general users of the app can access the information of other passengers such as their full English names and travel document numbers (Oriental Daily, 2016). Evidently, third parties such as the aforementioned companies do not have a strong intention to put effort in protecting individuals' online privacy. The COVID-19 pandemic forced many people to work from home. Hence, businesses, schools and social groups utilised video-conferencing on a large scale in 2020. Zoom, a video-conferencing software, suddenly became popular. Its daily meeting participants surged from 10 million in December 2019 to 200 million in March 2020, and then to 300 million in April 2020 (Keane, 2020a & 2020b). Along with this popularity, Zoom’s privacy risks befell a huge number of users. From its built-in attention-tracking features to the recent upticks in ‘Zoombombing’ (that is, Zoom meetings disrupted by strangers often with porn and hate images), Zoom then faced at least three lawsuits, and its security issue drew global attention (Hodge, 2020).

1.2 Research Gap

In this study, three major reasons explain the need to develop Hong Kong higher education students' online privacy management strategies for mobile devices.

Firstly, in 2012, under the commission of the Office of the Privacy Commissioner for Personal Data (PCPD), the Centre for the Advancement of Social Science Research of Hong Kong Baptist University carried out a survey among Hong Kong smartphone users. The result of the survey indicated that the age group between 15 and 20 has lesser online privacy concerns about smartphone security and a higher potential of data leakage from their smartphones than other age groups (PCPD, 2012).

Secondly, students in HEIs, who are under the age group of 15 to 20, are normally active users of mobile devices for surfing the Internet.

Thirdly, mobile devices and mobile apps are becoming exceedingly essential and inseparable from the life of HEIs students, as they often use them to play online games, access SNSs such as Facebook or Twitter and communicate with others through instant messaging (IM) apps such as WhatsApp, Telegram or Signal. Hence, these students should develop good online privacy management strategies on how such technologies should be used with their mobile devices (Ito et al., 2008).

1.3 Statement of the Problems

The advancement of mobile technology has changed the life of humans in this information age. The positive side of which is that users are now able to obtain information quickly and communicate with one another easily, and whenever and wherever necessary. However, the negative side is the invasion of users' privacy, as this kind of ubiquitous mobile digital connection makes their private information exposed and accessible to third parties (Eastin, Brinson, Doorey, & Wilcox, 2016). With the advancement of big data technology, Internet companies are now able to continuously record users' information. When visitors or users access many common Internet platforms, such as Microsoft, Facebook and Google, their information is automatically captured and stored by the platforms for future use (Weber, 2016).

This raised an important issue of privacy that individuals themselves should address, for they not only have the right but also the reason to protect and manage their own privacy. Thus, unavoidably, individuals should play an active role in protecting and managing their own privacy. In this regard, the present research, as an exploratory study, investigates the online privacy concerns, including protecting and managing their own as well as others' privacy, of Hong Kong higher education students who frequently use mobile devices to search information on the Internet, visit SNSs and use IM software for online purchases.

1.4 Purpose of the Study

To address the statement of the problems, this research has the following major purposes.

As the usage of mobile apps to play online games, access SNSs and communicate with others through IM becomes a significant part of students' life to connect with society, this research will investigate the online privacy attitude of Hong Kong higher education students when using their mobile devices. It will also explore how effective HEI students develop their online privacy management strategies when using their mobile devices. Having grown up in an information age and a digital world, the HEI students of this generation are active users of mobile devices. In addition, given that students' online privacy concerns on the security of their mobile devices were low (PCPD, 2012), this research will explore an effective pedagogical model to improve HEI students' online privacy management strategies of using mobile devices.

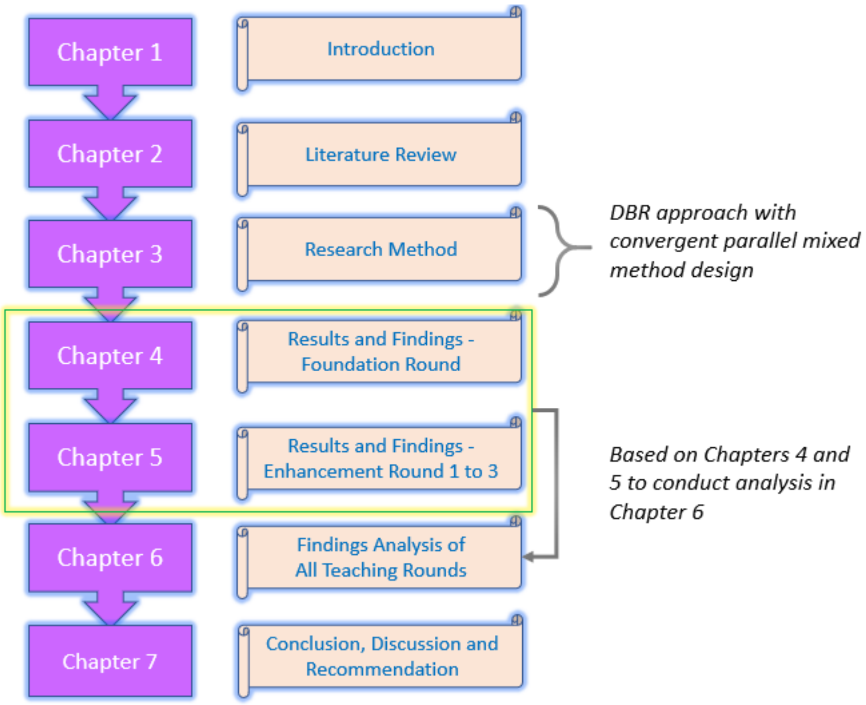
1.5 Significance of the Study

This research can be beneficial to Hong Kong youth, educators and education policymakers. First of all, the Education Bureau (EDB) of Hong Kong does not include sufficient education about online privacy in the formal curricula in any school level. The ICT curriculum (2015) suggests only one to two teaching hour(s) for online privacy education. Higher education institutions (HEIs) do not emphasise this issue as well. For example, HSUHK does not offer mandatory privacy course for students. The only channels for students to learn the importance of privacy protection are their parents or the news in the media. Moreover, with regard to privacy management, students are not provided with any systematic privacy education at any Hong Kong education system level. Therefore, this exploratory study investigates online privacy concerns and develops online privacy management strategies for Hong Kong higher education students who frequently use mobile devices to search for information on the Internet, visit SNSs, use IM software and purchase online. The findings can provide insights for HEI educators and education policymakers regarding the pedagogical model of teaching online privacy.

1.6 Organisation of the Thesis

This thesis consists of seven chapters. Figure 1 shows the holistic structure of this research. The first chapter is the introduction which contains the background of the study, statement of the problems, purpose and significance of the study. Chapter 2 reviews the literature on privacy issues, privacy management theory and privacy management strategies. Chapter 3 reports the methodology of the study, which includes research questions, research approach and research design. This research employed design-based research (DBR) approach, which adopted a convergent parallel mixed methods design. Four teaching rounds were conducted. The results and findings of the foundation round of teaching are presented in Chapter 4, whereas the results and findings of the remaining teaching rounds are reported in Chapter 5. Chapter 6 exhibits the findings analysis of all teaching rounds. Finally, Chapter 7 encapsulates the research findings and implications together with the recommendation, research limitations and further studies.

Figure 1: Organisation of the Thesis


Chapter 1
Introduction
Chapter 2
Literature Review
Chapter 3
Research Method
DBR approach with convergent parallel mixed method design
Chapter 4
Results and Findings - Foundation Round
Chapter 5
Results and Findings - Enhancement Round 1 to 3
Based on Chapters 4 and 5 to conduct analysis in Chapter 6
Chapter 6
Findings Analysis of All Teaching Rounds
Chapter 7
Conclusion, Discussion and Recommendation

Chapter 2 Literature Review

This chapter reviews the recent research articles related to this study. It consists of six sections. Section 2.1 describes the privacy theories. It also explains the relationships between privacy and the Internet, and the privacy concerns of HEI students. Section 2.2 describes three common privacy issues. Section 2.3 reviews the privacy management theories. Section 2.4 describes the privacy management strategies that will be employed to teach students privacy management. Section 2.5 explicates the privacy paradox. Section 2.6 reviews the pedagogical models. Finally, Section 2.7 provides a summary for this chapter.

2.1 Privacy

Privacy has many definitions on the basis of different views. Primarily, privacy is the ability of people to control the conditions under which their personal information is captured and used (Westin, 1967; Culnan, 1995; Campbell, 1997). With this underlying meaning, privacy was further explained as the ability of a person to control how his/her private information is released or delivered, to regulate the amount and types of social communication and to stop someone from obtaining his/her personal information (Stone & Stone, 1990).

2.1.1 Privacy and the Internet

After the emergence of the Internet technology, researchers turned their attention to relevant technologies such as cookies, which are data files used by online platforms; these files may put users' privacy at risk (Kruck et al., 2002). The advancement of the cloud computing technology not only brought forth a significant breakthrough in data storage but also raised people's privacy concerns. Cloud computing opens up a new way for users to store their personal data such as the data in their mobile devices. However, cloud storage is vulnerable to privacy risks; hence, various cloud infrastructures provide users with different levels of control over their information by implementing different encryptions and security controls (Weber, 2016). Moreover, Weber (2016) ascertained that numerous problems such as data breaches, tracking users' behaviours and non-transparent privacy policy are common in the public cloud; therefore, he proposed that privacy, as a basic human right, should be well-protected by individuals, companies and societies as a whole.

2.1.2 Online Privacy Concerns

Initial research articles on online privacy concerns suggested that personal information privacy (PIP) was mainly the responsibility of Internet users themselves (Smith et al., 1996). Nevertheless, online privacy in the contemporary digital age has become a complicated concept that relates to trade-offs between privacy concerns of collecting and disclosing personal information for gaining benefits (Smith et al., 2011). On the basis of this trade-off, privacy was explained as the right of an individual to define when, how and to what extent information is given out (Westin, 1970). Westin did not mention the management of personal information, such as the legitimate intention or agent on collecting, storing and managing personal data. He also did not take into account the setting in which privacy trade-offs occur.

In the 1990s, the fast growth of the Internet, the emergence and extensive use of social media and mobile technologies, and the expanding application of data mining and artificial intelligence have led to a great impact on privacy concerns in various aspects (Smith et al., 2011).

Many researchers focused their studies on the privacy of demographic information, such as name, date of birth, phone number and transactional information (Cheung, Chan, and Limayem, 2005; Smith, et al., 2011). Collection, unauthorised use, improper access and errors were identified as the key dimensions of information privacy concerns from studies that endeavoured to distil the concept of personal information privacy, avoid linear perspectives and concentrate on measures of privacy concern.

Malhotra et al. (2004) further distilled the concept and suggested the view of Internet User Information Privacy Concerns being connected to the collection, control and awareness of privacy practices. By merging this with other studies, the concept of personal information privacy has gradually focused on data collection, secondary use, ownership/control accuracy, awareness and access as key dimensions (Smith et al., 2011; Hong and Thong, 2013).

In today's cyberworld, aiming to protect personal demographic and transactional data is not sufficient, as a large range of personal data are being frequently shared. Thus, as technology advances, the ability of Internet users to control what personal information can be can be accessed, collected and shared and who can access it, these data also need to evolve.

The rapid adoption of data mining greatly enabled enterprises to collect, store and merge personal information of individuals. For instance, the doctrine of open government proliferated the number of public records on the Internet; hence, individuals, institutions, enterprises or other organisations can easily access and combine huge amounts of the general public's personal information.

2.1.3 Online Privacy of HEI Students

Several recent studies addressed the privacy concerns of students (Kaufman & Christakis, 2008; May & George, 2011; Lewis; Kelly & Seppälä, 2016). These studies featured great diversity of the issue of privacy, which could be classified into two categories. The first group of research articles put emphasis on how commercial websites gain access to and use the personal information of children and youth without obtaining their consent (Montgomery, 2000, Moscardell & Liston-Heyes, 2004; Youn, 2009). Another group of studies unfolded a new perspective of privacy concerns of youth and put less concern on the youth's privacy protection. Prensky (2001) created a new term for the generation born after the 1980's as 'digital native', indicating that they were raised and grew up in a digitally mediated world saturated with Internet technologies such as SNSs. He believed that digital natives knew how to protect their own information while accessing the web. However, this view has not yet been proven by empirical studies.

In recent decades, the upsurge in SNS has been accompanied by growing concerns on personal privacy. Youngsters, including HEI students, regularly disclose their personal information on SNS profiles, which can be seen by strangers; thus, their personal information can be used in harmful ways (Kevin, Jason & Nicholas, 2008). HEI students belong to the age group that will most welcome new communication technologies to articulate with their compact and 3D social networks (Quen-Haase, 2007). Unlike other ways of communication, contemporary SNSs allow HEI students to present themselves, express their opinion and develop or maintain social relationship (Ellison, Steinfield, & Lampe, 2007).

The number of Facebook users in Hong Kong reached 3.56 million in 2017 (Statista, 2018a). Facebook is the most popular SNS with a 75% penetration rate (Statista, 2017). Another popular SNS is Instagram. According to Statista (2018b), more than 31% of global Instagram users were aged between 18 and 24, which, again, was the age group of HEI students.

SNSs not only allow HEI students to establish friendships, but also to send text and voice messages to friends, upload photos or videos, join various groups and try new apps. However, HEI students need to examine the privacy settings of these apps carefully; otherwise, their private information may be viewed and monitored by strangers easily (Kevin, Jason, & Nicholas, 2008).

Some common online privacy issues that are important to HEI students will be described in the next section.

2.2 Online Privacy Issues

This section introduces two common and important online privacy issues, namely Internet cookies and malware, related to the privacy and data protection principles of PCPD.

Internet cookies are one elementary component for the web to work, similar to Wi-Fi, HTML, or electricity (Hill, 2015). A cookie is a small text file sent from a web server and placed on a user's hard drive when the user is browsing the website (Kannamanani, 2008). With the help of cookies, web servers can identify users and remember their data. Cookies can help users navigate a website and make full use of the logins, preferences, language settings, themes and other features of the browser (Felten & Schneider, 2000).

Lou Montulli, who developed two of the earliest Web browsers, Lynx in 1991 and Netscape in 1994, introduced cookies (Randall, 1997). He was responsible for other web innovations, including the blink tag, server push and client pull and HTTP proxying.

When a user logs in to a secure area of a website, cookies help the website server authenticate the user. As login information is stored in a cookie, the user can enter and leave the website without having to go over the same authentication procedure again and again (Sipior, Ward & Mendoza, 2011). Session cookies and persistent cookies are the two major standard first-party cookies. Session cookies store information about user page activities to make it easy for the user to pick up the webpage they left off. Through session cookies, when a user enters a website again, he or she needs not navigate the site all over again, as the website server knows what webpages the user has visited. Moreover, ordering information is also stored in these cookies; without them, shopping carts will not work and users will have to remember all the items they have previously selected (Charters, 2002; Miyazaki, 2008). Persistent cookies store user preferences. Many websites allow users to select their preferred site layout or theme and thus customise the way that information is presented to them. Therefore, persistent cookies personalise a site and make navigation easy for a user.

2.2.1 Internet Cookies

Concerns on Internet Cookies: Privacy vs. Cookies

Third-party cookies are created and placed on a user's device by different third parties operating on a website that the user is visiting (Google, 2020). They are, in fact, the main types of cookies that cause privacy concerns for users (Simon, 2005). Advertisements that a user is browsing on various websites are the main provider of these cookies. Through these cookies, servers of these advertisements track the user behavioural information, which enables them to customise advertisements to the user on another website (Simon, 2005; Sipior, Ward, & Mendoza, 2011). On the basis of a user's surfing history and the content he or she has visited, his or her behavioural profile is generated and saved in these servers (Luzak, 2014; Sipior, Ward, & Mendoza, 2011). Hence, third-party cookies are considered the most undesirable types of cookies that may give rise to privacy and security risks (Simon, 2005).

2.2.2 Malware and Privacy

Malware refers to any kind of malicious software that is harmful to installed computers. Generally, a malware infects computers with viruses, worms, spyware, Trojan horses and adware. Some malwares are known to collect users' personal information and sell it to advertisers or third-party companies. They can also covertly monitor users' activities. Salomon (2006) stated that spyware, such as keystrokes and screen dumps, monitors users' activity secretly, collects their information and then passes them to third parties. They are usually freeware and are installed automatically with or without the consent of a computer user. Some of them are so guilefully written that detecting and removing them become very difficult (Salomon, 2006).

Mobile Malware

As stated in Section 1.1, mobile devices have become popular nowadays. Hence, they have become targets of malware. According to Kaspersky (2020), two types of malware threaten mobile phone users' privacy: mobile spyware and mobile adware.

After being loaded as a programme onto mobile devices, mobile spyware can monitor mobile owners' activity, record their location and steal their private data, such as Internet banking usernames and passwords. Spyware usually hides themselves in other apparently benign software and covertly collects data. As such, mobile owners may not be aware of the presence of spyware until the performance of their mobiles degrades or they scan their infected mobiles with anti-malware scanner apps.

Mobile adware is obtrusive pop-ups that collect mobile owners' private data in the beginning. Their income is based on the number of downloads they receive. Mobile adware has now developed 'malvertising' codes that can infect and root mobile devices. These codes force them to download and install specific adware that can enable attackers to steal mobile owners' information.

Malware Threatens Privacy

Mobile malware programmes are intentionally developed to collect mobile owners' personal information and relay it to advertisers and other third parties. They are typically designed to gather users' browsing and shopping preferences, IP address, or identification information on mobile devices (UMass, 2020).

2.2.3 Data Protection Principles of Hong Kong

The Personal Data (Privacy) Ordinance (the PDPO), one of Asia's most comprehensive data protection laws, was passed in 1995; except for certain provisions, it has been in effect from December 1996 (PDPC, 2020b). In 2012, to meet the need of new privacy challenges and respond to public concern, the ordinance was amended. The most significant amendment was the introduction of direct marketing provisions and other additional protection.

The PDPO has three features: technology-neutral, principle-based and applicable to the private and public sectors (PDPC, 2020a). The Data Protection Principles (DPPs) in Schedule 1 pointed out to data users how they should collect, handle and use personal data with the objective of ensuring that data subjects should be fully informed before their personal data is collected in a fair and minimal manner. The PDPO (2020a) also stipulated that collected personal data should only be used for the original collection purpose, be processed in a secure way and be erased after the collection purposes were fulfilled. In addition, data subjects should be given the right to access and to correct their data (PCPD, 2020a).

2.3 Privacy Management Theory

Information flows are of vital importance in running global businesses, because the main obstacles to online trust are consumers' concerns about their privacy and the security of their personal information. Hence, perceptions on privacy and security have been considered the antecedents of trust (Hoffman, Novak, & Peralta, 1999); and accordingly, electronic commerce companies employed different privacy frameworks to study privacy protection for their customers. The PCPD adopted the privacy framework of Asia-Pacific Economic Cooperation (APEC) in 2010 to establish the information privacy protection policy and ordinances in Hong Kong. The APEC Privacy Framework was endorsed by APEC ministers in 2004. They have recognised that the cooperation to balance and promote effective information privacy protection and the smooth flow of information in the Asia-Pacific region is the key to improving consumer confidence and ensuring the growth of electronic commerce. Understandably, people often collect, store and use personal information for personal, family or household purposes. For example, students' mobile devices often contain their personal address books, phone lists, family notes and photos. However, as the APEC Privacy Framework is developed to provide guidelines for electronic commerce within the Asia-Pacific region, it is not applicable to the protection and management of individuals' personal information in relation to family or household activities (APEC Privacy Framework document, 2005).

Alan Westin, a pioneer scholar of privacy study, developed a well-known privacy theoretical framework (Westin, 1970). This framework focuses on what personal information an individual wishes to keep private rather than on how this information is managed (Conger et al., 2013). In this big data age, with the rapid expansion of the

Internet and the increasing application of mobile and information technologies, mobile users are facing bigger privacy concerns and more challenges in personal information management in different ways (Smith et al., 2011). Therefore, students not only need to know how to protect their own privacy, but also that of other people. However, Westin's framework does not consider the protection and management of other people's privacy (Martin et al., 2016; Conger et al., 2013).

Petronio (2002, 2013) developed communication privacy management (CPM), which was originally known as communication boundary management (1991). CPM is a systematic research framework adopted by many studies. The uniqueness of CPM is that it does not only help students understand how to protect and manage their own privacy, but also others' privacy. Students almost cannot control how other parties use or even collect their personal data. However, after having learned the importance of protecting their own or others' privacy, when students have the chance to become policymakers, they might then consider these privacy aspects simply because they had learned CPM today.

As technology is developing in a fast pace, we should not rely on current technologies to protect our privacy (Martin et al., 2016). Instead, we should educate our students to understand the importance of protecting their personal data in all aspects regardless of the kind of devices they are using.

Thus, the theoretical framework of CPM theory developed by Petronio (2002, 2013) was adopted to prepare the teaching materials in this study. CPM considers two related basic concepts: the process of revealing private information and the ways of concealing private information. Petronio and Durhan (2015) pointed out that a dialectical tension exists between these two concepts; hence, revealing and concealing come about through a rule management system manner.

CPM theory was employed to study how people maintain and reveal their privacy to others in their daily life (Petronio, 2009; Kennedy-Lightsey et al., 2012; Petronio & Kovach, 1997; Ngwenya, Farquhar, & Ewing, 2016; 2010; Thompson, 2011; Petronio & Jones, 2006; Rauscher & Durham, 2015). In reality, people need to provide their private information to others for attaining medical care, keeping friendships, sustaining family relationship, creating bank accounts and applying for a job. Researchers also used CPM theory to explain the process of self-disclosure in social and online environments (Petronio, 2002; Youn, 2009; Anitha & Aakash, 2015). CPM theory states that people are the choice makers who believe that they own their information. It describes that people are able to develop boundaries to control their personal information. The theory also defines a basic principle in which people share and withhold information according to a system of rules, which is set by their own decision criteria such as cultural, gender, motivational, contextual and risk–benefit criteria. When individuals share their private information with others, the information becomes co-owned. Others become co-owners of people's private information according to rules regarding linkages, permeability and ownership. Mistakes will be made if people do not follow these privacy rules, and turbulence will emerge. Table 1 concludes these three stages, namely, ownership, control and rules and turbulence.

Table 1: Stages of Communication Privacy Management Theory

Stage	**Name**	**Description**
1	Ownership	◎ People believe they own the information about themselves. ◎ Others become co-owners of people's private information.
2	Control and Rules	◎ People develop boundaries to control their personal information. People share and withhold information according to a system of rules.
3	Turbulence	◎ When the rules are not followed and mistakes are made, turbulence emerges.

CPM theory was widely used to study various issues especially social communication issues. Table 2 shows the explored areas. The following table also includes studies that mainly employed a questionnaire as the instrument to investigate their topics.

Table 2: Applications of CPM theory

Study	Area	Target participants	Number of participants	Research method	Findings (Relevant to CPM)
Kennedy-Lightsey et al., 2012	Friend communications	HEI students (U.S.)	200	Questionnaire survey	Disclosers perceived that receivers had less ownership over riskier information. Hence, facing hypothetical dissemination of high-risk information, they experienced negative emotional reactions. For low-risk information, as they perceived that their friends have more ownership, they reported positive emotional reactions. On the side of the receivers, when they perceived they had ownership over the information, they were more likely to disseminate it.
Spottswood & Hancock, 2017	Social networking	HEI students (U.S.)	144	Questionnaire survey	Disclosure behaviour was linked to explicit cues indicating disclosure frequency norms. In addition, implicit social norm cues (i.e. surveillance primes) increase overall disclosure frequency and affect disclosure accuracy when explicit cues discourage disclosure. Moreover, explicit cues that indicated others' privacy settings could increase the strictness of participants' privacy settings. However, implicit cues had no such effect.
Yang, Pulido & Kang, 2016	Social media network	HEI students (U.S.)	183	Questionnaire survey	Regression analyses concluded that Control and Boundary Rules of Private Information on Twitter significantly predict daily minutes spent on Twitter accounts. However, the same CPM variables did not predict college students' other Twitter usage behaviours (e.g. weekly inquiries and total months of using Twitter). The other two CPM variables, permeability rules and linkage rules of private information on Twitter, did not predict college students' Twitter usage behaviours.

Study	Area	Target participants	Number of participants	Research method	Findings (Relevant to CPM)
Jin, 2013	Social media network	HEI students (U.S.)	375	Questionnaire survey	Regarding the multiple dimensions of private information, such as daily lives, social identity, competence, socio-economic status and health, data collected from current Twitter users show multiple levels of private disclosure boundaries on Twitter and significant differences at the descriptive and inferential levels. Private information on daily lives and entertainment was located at the outermost layer of the disclosure onion and was easily disclosed. However, being hidden in the innermost layer of the disclosure onion, health-related private information was carefully concealed.
Ngwenya, Farquhar & Ewing, 2016	Interpersonal health	Adults (England)	37	Semi-structured interviews	Cancer patients perceived that they own the news of their cancer and the rights as to how, when and whom to share the news with. Their family members understood that they need to follow the patients' rules in sharing this news. Patients and their family members had to follow these communication boundaries to maintain their trust relationship and avoid damaging it.
Thompson, 2011	Sport management	HEI students (U.S.)	37	Semi-structured interviews	Athletic/academic advisors experienced different types of dilemmas, which revolved around private information that student-athletes disclosed regarding academic, athletic and personal issues. This research presents specific dilemmas that advisors experienced.
Jin, 2012	Interpersonal health	HEI students (U.S.)	134	Questionnaire survey	This study suggested that to design an effective e-health website, a vital component that health service providers need to systematically understand is health consumers' motivational factors.

Study	Area	Target participants	Number of participants	Research method	Findings (Relevant to CPM)
McKenna-Buchanan et al., 2015	Culture and Communications	Adults (U.S.)	29	Semi-structured interviews	Interview transcripts were thematically analysed by using communication privacy management (CPM), for privacy rule criteria and disclosure/concealment strategies. The study magnified five strategies for disclosing or concealing sexual identity: selection, reciprocity, ambiguity, deflection and avoidance.
Metzger, 2007	E-commerce	HEI students (U.S)	213	Questionnaire surveys	This study suggested that online consumers set up boundaries around personal information and establish rules to decide when to disclose information. The rules are consistent with CPM theory.
Heo, 2011	Education platforms	HEI students (U.S)	103	Questionnaire surveys	Depending on who the audiences were, participants were willing to share, in varying extent, their social information. This finding indicated that they were balancing privacy and disclosure as described in CPM theory.

2.4 Privacy Management Strategies

The privacy issue of SNSs has lately aroused public attention. At the same time, the remarkable development of Facebook begins to capture the attention of researchers who are interested in privacy issues. In addition to the high adoption of SNSs is the widespread use of IM mobile applications such as WhatsApp, Line and WeChat among HEI students. Recently, researchers have studied the relationship between the privacy awareness of HEI users and SNSs (Ellison, N. B. et al., 2007, Kevin et al., 2008; Quan-Haase, 2007). However, with the growing public scrutiny on online activities and increasing concerns about privacy policy or permission on the Internet, studies on the privacy practices, privacy management of HEI students were still scarce and only few relevant empirical data were collected (Kevin, Jason, & Nicholas, 2008).

2.5 Privacy Paradox

Barnes (2006) was the first researcher to mention the privacy paradox in his study. He described that ‘Adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the Internet’.

Acquisti (2004) and Barnes (2006) claimed that there existed the tendency towards online privacy-compromising behaviour. This tendency resulted in a dichotomy between privacy attitudes and actual behaviour. Besides, risk perception was not enough to motivate people to apply privacy protection strategies (Oomen and Leenes, 2008). Thus, although many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behaviour, such awareness rarely translates into actual protective behaviour (Joinson et al., 2010; Pötzsch, 2009; Tsai et al., 2006).

The privacy paradox was, however, not supported by some studies (Joinson, Reips, Buchanan, & Paine Schofield, 2010; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Mohamed & Ahmad, 2012). Krasnova et al. (2010) discovered that the perceived privacy risk, an idea very similar to privacy concerns, was closely related to the amount of private information that a respondent disclosed on SNSs. Mohamed and Ahmad (2012) concluded that ‘Information privacy concerns explain privacy measure use in social networking sites’ (p. 2366).

Prior research investigated the privacy paradox on the basis of the SNS (Dienlin & Trepte, 2015; Muliati, Rabiah, & Othman, 2018). Owing to the rapid development and utilisation of mobile technology, an urgent question emerges: Does the privacy paradox still exist in the use of mobile devices among HEI students?

2.6 Pedagogical Models

This section reviews three pedagogical models namely case-based learning, event-based learning and interactive classroom.

2.6.1 Case-based learning

Case-based learning usually uses case studies to enhance teaching and learning. These learning activities are referred to as case teaching with online video which are also described variously as case analysis. This pedagogy is a well-developed instructional method and was found useful in technology-enhanced settings (Demetriadis, Papadopoulos, Stamelos, & Fischer, 2008). Case teaching using online video is a popular teaching strategy in higher education subjects such as education, medicine, law and policy studies (Okamoto, Helm, McClain, & Dinson, 2012; Sslamet, Dwi, & Cucu, 2017; Tan, 2006; Zhang, Miller, & Harrison, 2008). Isiaka (2007) pointed out that this strategy allowed students to apply ideas, theories and concepts to realistic problem-solving situations.

With the rapid growth of the Internet, case teaching using online video has become an important part of education in various classroom settings (Mikalef et al., 2016). Giannakos et al. (2016) defined case teaching using online video as the learning process of acquiring defined knowledge, competence and skills with the systematic assistance of video resources. An essential component of this pedagogical model is an interesting authentic story that relates to learners' experiences (Herreid, 2007). Mikalef, Pappas and Giannakos (2016) pointed out that the story should be relevant to the learner and the topic, arouse interest, create empathy with central characters, provoke conflicts, force decisions and has generality.

When case analysis is used in the online setting, students also develop skills related to electronic technologies. These skills are valuable to students in any profession that they will practice (Salmons, 2003). Salmons also asserted that a case study tells a real story that has happened previously. Therefore, with reference to current developments, students could have a broader understanding of the context for the case.

2.6.2 Event-based learning

In event-based learning, teachers usually use current events as a convenient means to draw students' attention to relevant news topics. Learning activities related to current events often provide a break from the ordinary for teachers and students, and enable them to explore alternative approaches to cover the curriculum (Chica, 2004). Although this pedagogical model was widely employed by teachers, empirical studies that aimed to provide a comprehensive research view on these event-related teaching activities are not sufficient.

Chica (2004) defined an event as a significant occurrence that takes place at a given time and location, and event-based learning as teaching activities that adopt historical or emerging events to achieve a pre-defined set of learning objectives.

This pedagogical model using current events has been adopted in various teaching domains. Grise-Owens, Cambron and Valade (2010) used current events to enliven social work curricula and engage students in contemporary issues and events. This approach promotes invested engagement with classroom materials (Grise-Owens, Cambron, Valade, & Cooper, 2007; Roche, Dewees, Trailweaver, Alexander, Cuddy, & Handy, 1999). In addition, Wright (1992) described that events may be adopted to provide students with a better understanding of the nature of scientific research by allowing comparison of different (possibly contradictory) sets of data about an event. In this way, connections between real-world events and key scientific concepts could be established. Besides, Turner (1995) used current events to educate students to become responsible citizens. Turner encouraged teachers to employ suitable current events in the curricula to achieve the following learning outcomes: developing learners' curiosity about news, helping learners assess current event sources, developing learners' basic knowledge about the world and its leaders, and alerting learners to their power and responsibility within society.

2.6.3 Interactive classroom

Interactive classroom learning using quick response system (QRS) has been widely adopted by educators in recent years (Cain, Black, & Rohr, 2009; Malekigorji & Hatahet, 2020; Ruiz-Martínez, Martinez-Carreras, & Ramallo-Gonzalez, 2020; Stowell, 2015). This educational technology provides an interactive learning environment that allows students to track their own progress over the course of their study and assists them to improve their learning engagement and performance (Stowell, 2015). QRS is one of the functions provided by learning management systems (LMS) such as Moodle. It can function as a standalone application software to collect students' learning progress. QRS is also called classroom response system (or clickers), audience response system and personal response system. Stowell pointed out that different digital learning and assessment technologies are developed to reinforce active learning methodologies. Conventional teaching methods employed in higher education for a large group of students are inevitably accompanied by poor in-class engagement and almost no interaction with the instructor (Malekigorji & Hatahet, 2020). However Malekigorji and Hatahet explained that pedagogical methods involving QRS allow students to interact with teachers and peers anonymously (or in identified modes) and to engage in answering questions or participating in discussion via QRS and smart devices.

QRS is an ideal approach to deliver revision sessions where students can work together to answer questions. As an immediate student feedback system, QRS also benefits the teacher by collecting students' ideas and observing their learning progress to be able to adjust the course structure and teaching mode (Ruiz-Martínez, Martinez-Carreras, & Ramallo-Gonzalez, 2020).

This pedagogical model allows a teacher to use in-class performance as a diagnostic tool by examining students' responses to questions and activities to see if the design of the questions plays an important role in developing the skills that they are learning (Fuad & Debzani, 2014).

2.7 Summary

In this chapter, we have discussed the concept of privacy, addressed the online privacy concerns of HEI students, described the common privacy issues and then reviewed the privacy management theories. In addition, CPM theory was applied to better understand the importance of revealing and concealing information in an online environment. The basic assumption of this theory is that people use a set of rules to systematically manage their own private information and decide to what extent they will disclose and share this information. This study will adopt CPM theory to develop teaching materials regarding privacy management strategies for HEI students. The privacy paradox will be explored, and three pedagogical models will be employed. A pilot study of the research method will be carried out and elaborated in the next chapter.

Chapter 3 Methodology

This chapter presents the research questions. Then, it describes the research approach and explains the rationale of employing convergent mixed method in this study. It also mentions the design of the survey instrument and the procedures of the pilot test for the survey instrument. The four stages of research iteration are explained, namely the design of the lesson, implementation of pedagogical method, analysis of data collected and enhancement of lesson design. The ethical consideration is described as well.

3.1 Research Questions

This study aims at exploring an effective pedagogical model of developing and improving higher education students' online privacy management strategies for mobile devices by using CPM theory. This research is designed to explore the online privacy practice of Hong Kong higher education students when using their mobile devices and to develop their online privacy management strategies. It focuses on investigating how they manage their private information and the personal information of others. With reference to the purpose of this study and the literature review, we generated the following research questions (RQ):

RQ 1: What are HEI students' online privacy attitudes towards using mobile devices?

RQ 2: How effective is using CPM theory in improving HEI students' online privacy management strategies when using their mobile devices?

RQ 3: What kinds of pedagogical models can effectively improve HEI students' online privacy management strategies when using mobile devices?

3.2 Research Approach

In this study, DBR, which could effectively bridge the chasm between research and practice in formal education (Alghamdi & Li, 2013; Anderson & Terry, 2012), is used as a practical research methodology. DBR Collective (2003) argues that DBR, which blends empirical educational research with the theory-driven design of learning environments, is an important methodology for understanding how, when and why educational innovations work in practice. DBR Collective cited Brown (1992) and Collins (1992) and reported that DBR is for the study of learning in context through the systematic design and study of instructional strategies and tools. It also argued that DBR helps develop knowledge regarding creating, enacting and supporting innovative learning environments. Besides, DBR is a popular paradigm used in education research (Anderson & Shattuck, 2012; Schmitz, Klemke, Walhout, & Specht, 2015).

Brown (1992), the first researcher to develop DBR, pointed out that 'an effective intervention should be able to migrate from our experimental classroom to average classrooms operated by and for average students and teachers, supported by realistic technological and personal support' (p. 143). Effective intervention involves a series of iterations of lesson design, implementation of lesson, analysis of data collected and enhancement of lesson design (Anderson & Shattuck, 2012) to address complex educational problems (Wang & Hannafin, 2005).

Given that the mixed methods approach is able to maximise the validity and at the same time increase the objectivity and reliability of current research, most DBR literature agree that the mixed methods approach is proper for collecting and analysing data (Alghamdi & Li, 2013; Bell, 2004; Design-Based Research Collective, 2003; Wang & Hannafin, 2005). Therefore, in DBR methodology, qualitative and quantitative research methods are adopted to address research questions (Bogdan & Biklen, 2006; Li & Chu, 2018; MacDonald, 2008).

In this study, a mixed method research approach is adopted to collect qualitative and quantitative data, so as to triangulate the findings. Applying multiple methods to a study allows researchers to explore divergent viewpoints on the same issue and provide contextual understanding shaped by real-life experiences (Creswell, Klassen, Plano Clark, & Smith, 2011; Morse & Niehaus, 2009).

Creswell and Plano Clark (2011) identified four commonly used basic mixed methods designs in today's educational research, namely, convergent parallel design, explanatory sequential design, exploratory sequential design and embedded design.

In this study, quantitative and qualitative data were collected at the same time, and then merged for comparison. Finally, the results were interpreted or explained for any discrepancy. After comparing the four basic types of mixed methods designs, the convergent parallel mixed methods design was selected as the approach to be employed in this study. Creswell (2012) stated that this type of design consists of the following major steps:

1. Pay equal attention to quantitative and qualitative data.
2. Collect the quantitative and qualitative data at the same time.
3. Analyse the quantitative and qualitative data, and compare their results to see if they are similar or dissimilar.

Figure 2: Research approach: integration of adopting DBR and convergent parallel mixed-methods design

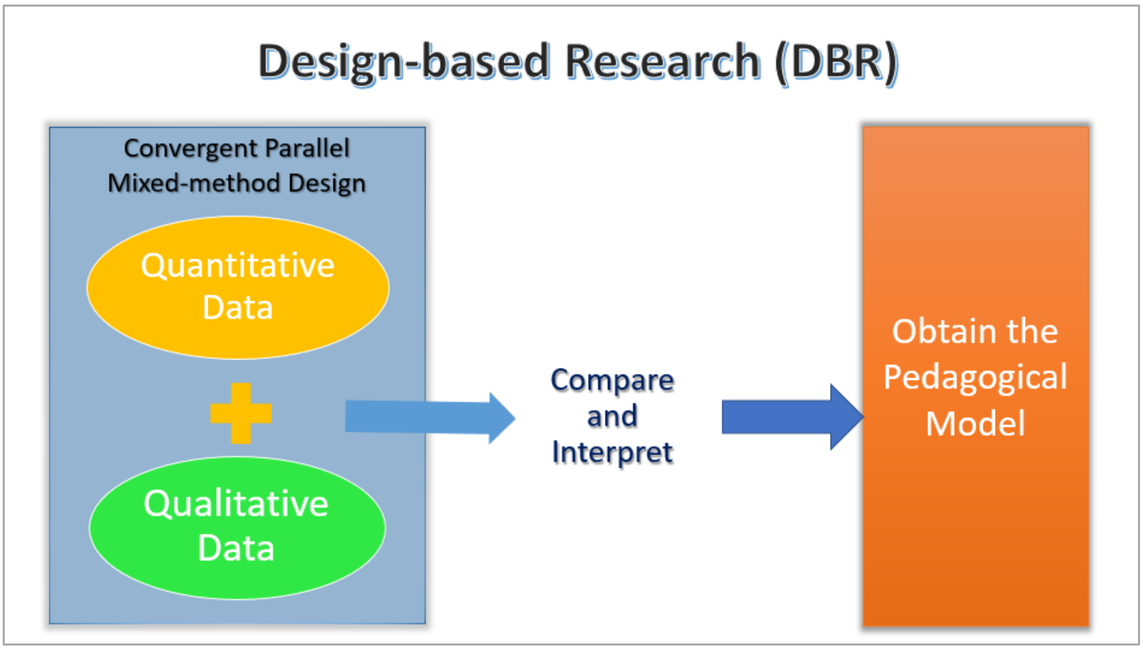

Design-based Research (DBR)
Convergent Parallel Mixed-method Design
Quantitative Data
Qualitative Data
Compare and Interpret
Obtain the Pedagogical Model

Figure 2 displays that this research integrated DBR and convergent parallel mixed-methods design. To obtain an effective pedagogical model, the present study conducted four iterations or teaching rounds. Each iteration involved one class and the collection of quantitative data from the pre-teaching survey, the post-teaching survey and the assignment and qualitative data from the interview of volunteer students. The quantitative data were analysed using the cross tabulation feature of SPSS. The qualitative data were coded into positive, negative and other themes. Each theme was given a label, and the percentage of students contributing to the theme was calculated by NVIVO. The quantitative and qualitative data were compared and used to investigate the perception of students on the effectiveness of the teaching approach. According to these findings, the pedagogical model was adjusted and enhanced and then used in the second research iteration. The four stages of the research iteration will then be repeated and so forth. Figure 3 shows the process to obtain the finest pedagogical model in our study.

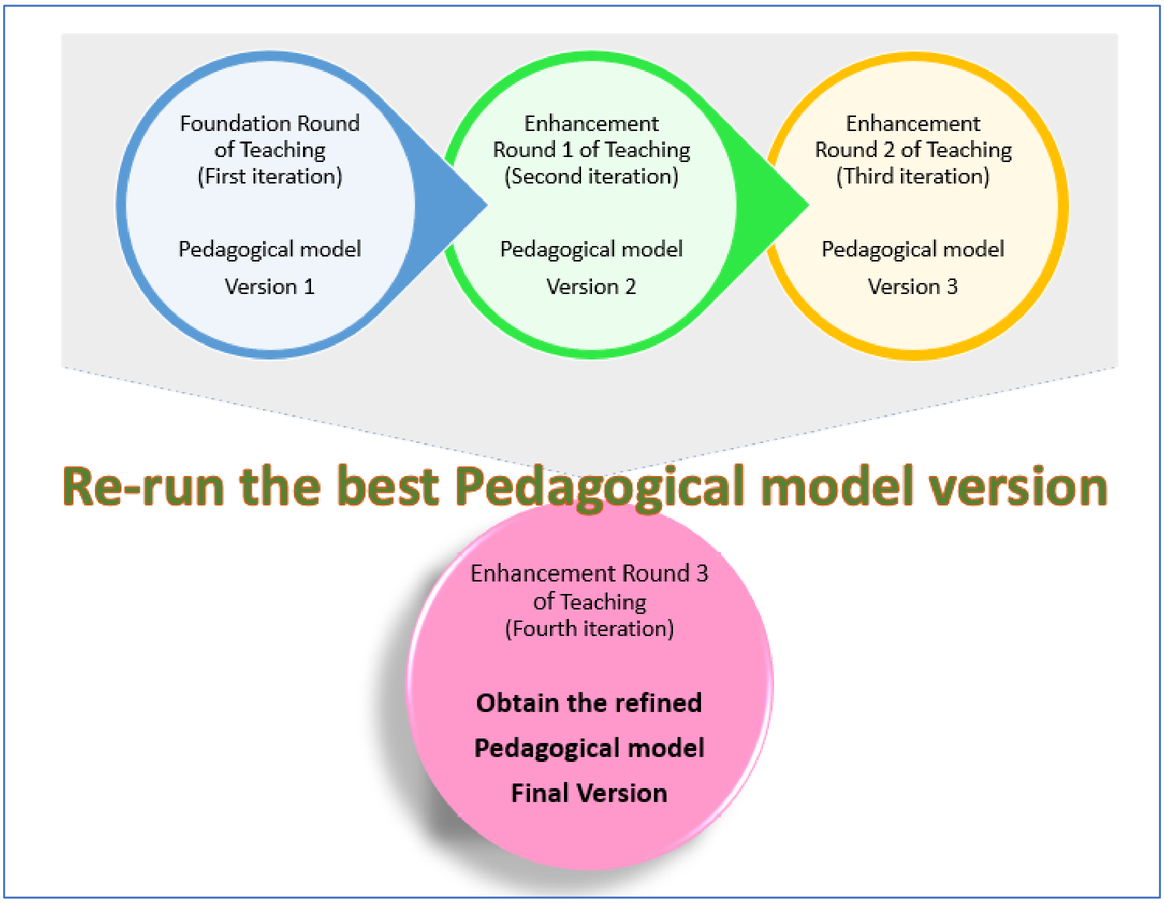

Foundation Round of Teaching (First iteration)
Pedagogical model Version 1
Enhancement Round 1 of Teaching (Second iteration)
Pedagogical model Version 2
Enhancement Round 2 of Teaching (Third iteration)
Pedagogical model Version 3
Re-run the best Pedagogical model version
Enhancement Round 3 of Teaching (Fourth iteration)
Obtain the refined Pedagogical model Final Version

Figure 3: Four teaching rounds (iterations)

3.3 Research Design

This research was conducted at the Hang Seng University of Hong Kong (HSUHK), which is one of the private universities in Hong Kong offering 4-year bachelor (honours) degree programmes. The programmes offered include business, languages studies, journalism and communication, social science and science. This study targets approximately 120 undergraduate students from four classes. Cluster sampling method was applied to select students from different undergraduate programmes. HSUHK uses an open source LMS, Moodle, a customised and unique e-learning platform to facilitate teaching and learning. In HSUHK, all teachers and students have their own LMS account. Teachers can upload their teaching materials to LMS or adopt the utilities provided by LMS, such as quizzes and forum, to support teaching and learning. Moodle is also commonly used worldwide and in other local universities such as the Education University of Hong Kong, the Chinese University of Hong Kong and Lingnan University. In 2019, Moodle has 103,894 registered sites with more than 167 million users across 226 countries (Moodle, 2019).

The purpose of this study is to explore an effective pedagogical model of developing and improving HEI students' online privacy management strategies for mobile devices. The teacher employed CPM theory as a framework to prepare teaching materials so as to focus on the development of HEI students' online privacy management strategies for mobile devices.

3.3.1 Survey instrument for collecting quantitative data

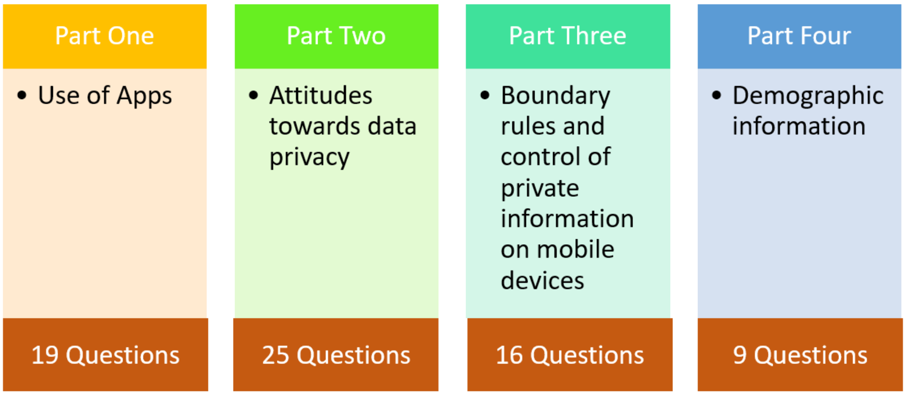
Self-administered questionnaires are employed to collect quantitative data in this research. This section explains the rationale of the survey design and the pilot test for the survey instrument.

3.3.1.1 Rationale of the survey design

Before students participate in this study, their online privacy attitudes and their prior knowledge are analysed. Therefore, the design of the survey instrument of this study was based on simplified CPM theory, which is composed of three stages as stated in section 2.3.

To answer the research questions, the questionnaire consists of four parts, namely usage of mobile devices, attitudes towards data privacy, boundary rules and control of private information on mobile devices and demographic information. The questionnaire was long and consisted of 69 questions. The part on demographic information was put in the last section so that participants can exert more energy into the first three parts and then quickly complete their demographic information in Part 4.

Figure 4: Parts of the Self-administered Questionnaire



Part One	Part Two	Part Three	Part Four
• Use of Apps	• Attitudes towards data privacy	• Boundary rules and control of private information on mobile devices	• Demographic information
19 Questions	25 Questions	16 Questions	9 Questions

3.3.2 Pilot Test for the Survey Instrument

A pilot test of the survey is conducted at the beginning of the study. Two volunteer students from the target classes were invited to answer the pilot questionnaire. This pilot test is aimed at generating an accurate direction for this study and perfecting our survey instrument.

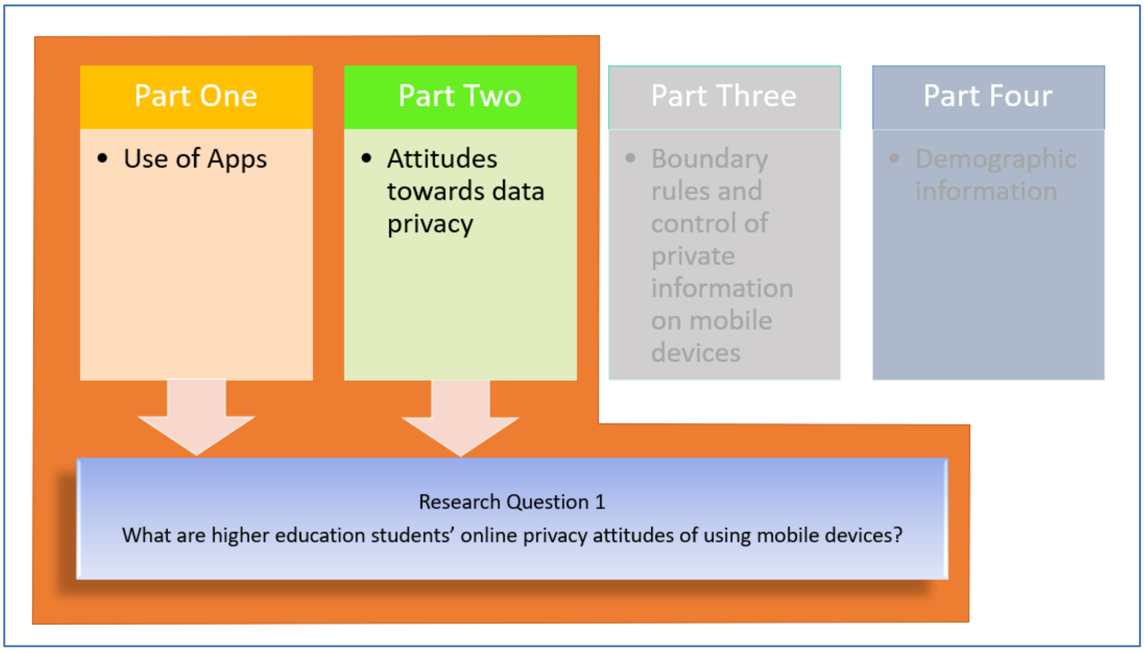
Two expert scholars helped review the survey questions to ensure the face and content validities, the preciseness of the language and the layout of this data collection method. As the original survey has more than 70 questions, some questions were suggested to be removed to prevent participants from being demotivated by a long survey. The final survey consisted of 67 questions. The survey is a self-administrated questionnaire, which protects the identity of participants (Lang, John, Lüdtke, Schupp, & Wagner. 2011). The statistical results were recorded in SPSS files to facilitate our understanding of the survey results later.

To evaluate the reliability of the instrument, the question items were statistically analysed using Cronbach's alpha, which gave a general measure of internal consistency. The Cronbach's alpha reliability coefficient of the question items was 0.907, indicating that the questionnaire was reliable.

3.4 To address Research Question 1

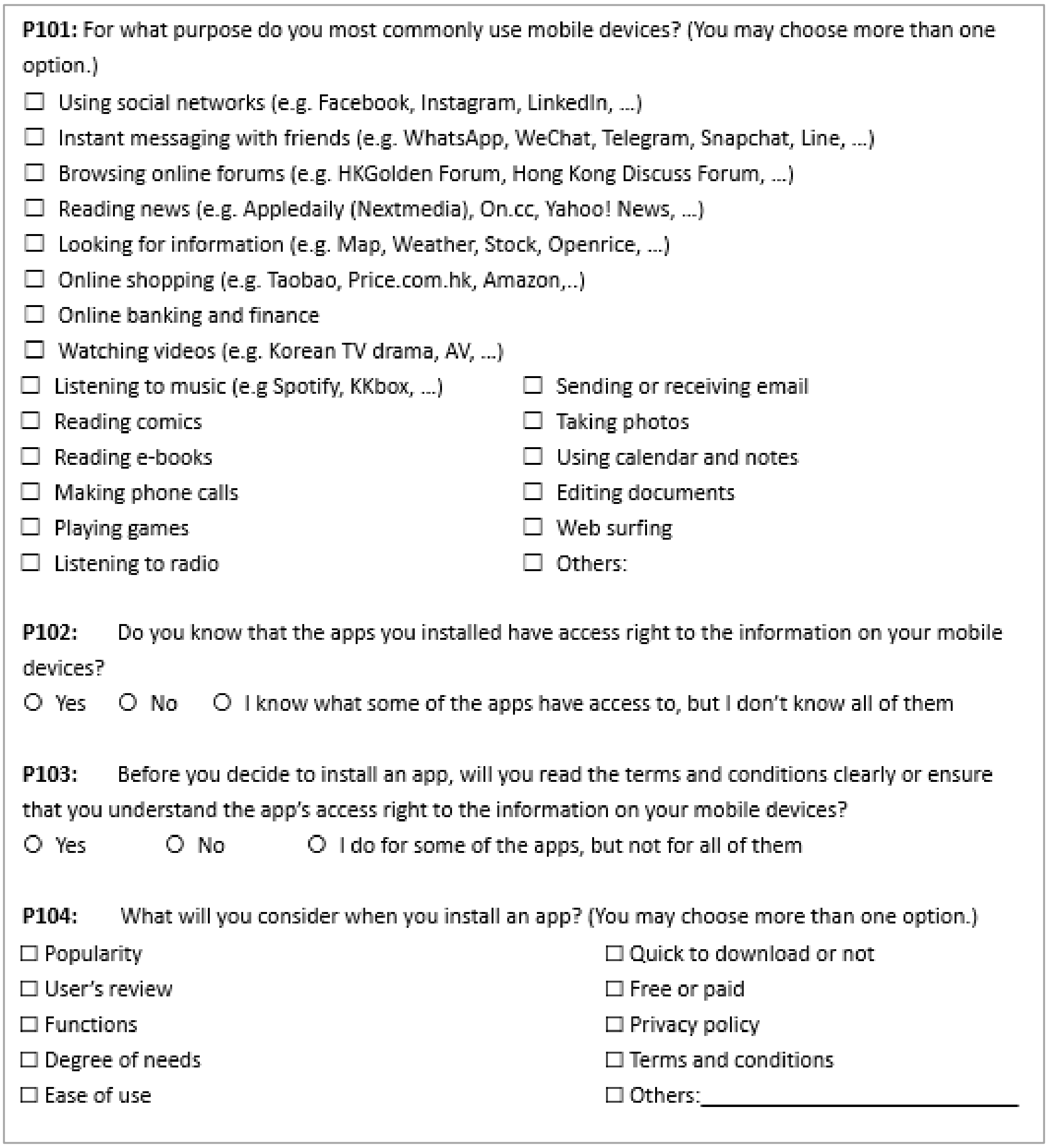
The quantitative data from Part 1 and Part 2 of the survey were used to address Research Question 1: What are HEI students' online privacy attitudes towards using mobile devices? Appendix I shows the full set of questionnaires. The survey was referred to and revised from the instruments of Fortes and Rita (2016) and Yang, Pulido and Kainan (2016).

Figure 5: Parts of the Survey that Addressed Research Question 1


Part One
• Use of Apps
Part Two
• Attitudes towards data privacy
Part Three
• Boundary rules and control of private information on mobile devices
Part Four
• Demographic information
Research Question 1
What are higher education students' online privacy attitudes of using mobile devices?

Questions in Part 1 asked students regarding the use of their mobile devices. Figures 6 and 7 show the question items.

Figure 6: Questions in Part One of the Survey (from P101 to P104)



P101: For what purpose do you most commonly use mobile devices? (You may choose more than one option.)

☐ Using social networks (e.g. Facebook, Instagram, LinkedIn, …)
☐ Instant messaging with friends (e.g. WhatsApp, WeChat, Telegram, Snapchat, Line, …)
☐ Browsing online forums (e.g. HKGolden Forum, Hong Kong Discuss Forum, …)
☐ Reading news (e.g. Appledaily (Nextmedia), On.cc, Yahoo! News, …)
☐ Looking for information (e.g. Map, Weather, Stock, Openrice, …)
☐ Online shopping (e.g. Taobao, Price.com.hk, Amazon,..)
☐ Online banking and finance
☐ Watching videos (e.g. Korean TV drama, AV, …)
☐ Listening to music (e.g Spotify, KKbox, …)
☐ Reading comics
☐ Reading e-books
☐ Making phone calls
☐ Playing games
☐ Listening to radio
☐ Sending or receiving email
☐ Taking photos
☐ Using calendar and notes
☐ Editing documents
☐ Web surfing
☐ Others:

P102: Do you know that the apps you installed have access right to the information on your mobile devices?

○ Yes ○ No ○ I know what some of the apps have access to, but I don't know all of them

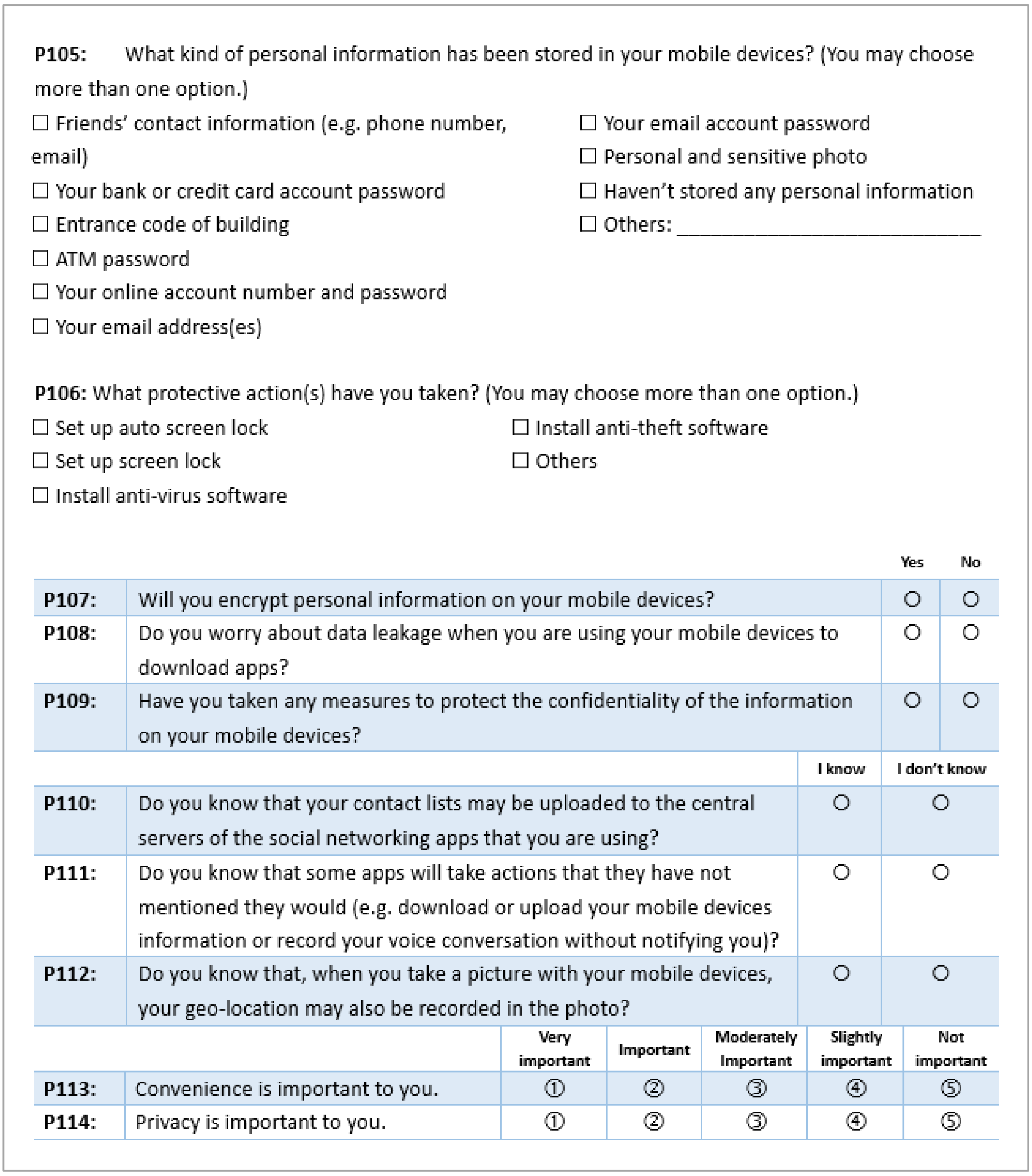
P103: Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access right to the information on your mobile devices?

○ Yes ○ No ○ I do for some of the apps, but not for all of them

P104: What will you consider when you install an app? (You may choose more than one option.)

☐ Popularity
☐ User's review
☐ Functions
☐ Degree of needs
☐ Ease of use
☐ Quick to download or not
☐ Free or paid
☐ Privacy policy
☐ Terms and conditions
☐ Others:__________________________

Figure 7: Questions in Part 1 of the Survey (from P105 to P114)



P105: What kind of personal information has been stored in your mobile devices? (You may choose more than one option.)

☐ Friends' contact information (e.g. phone number, email)
☐ Your bank or credit card account password
☐ Entrance code of building
☐ ATM password
☐ Your online account number and password
☐ Your email address(es)
☐ Your email account password
☐ Personal and sensitive photo
☐ Haven't stored any personal information
☐ Others: ____________________________

P106: What protective action(s) have you taken? (You may choose more than one option.)

☐ Set up auto screen lock
☐ Set up screen lock
☐ Install anti-virus software
☐ Install anti-theft software
☐ Others

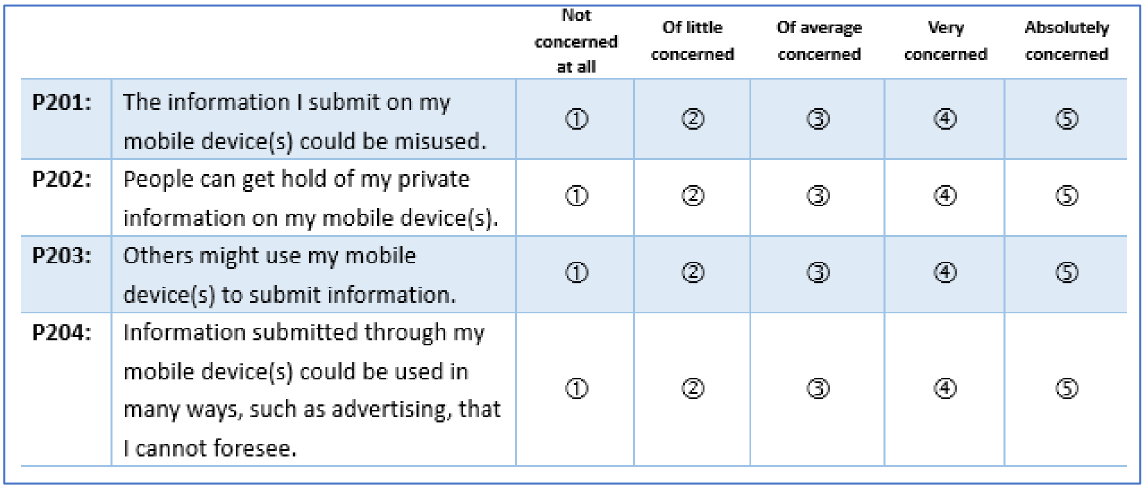
		Yes	No
P107:	Will you encrypt personal information on your mobile devices?	○	○
P108:	Do you worry about data leakage when you are using your mobile devices to download apps?	○	○
P109:	Have you taken any measures to protect the confidentiality of the information on your mobile devices?	○	○

		I know	I don't know
P110:	Do you know that your contact lists may be uploaded to the central servers of the social networking apps that you are using?	○	○
P111:	Do you know that some apps will take actions that they have not mentioned they would (e.g. download or upload your mobile devices information or record your voice conversation without notifying you)?	○	○
P112:	Do you know that, when you take a picture with your mobile devices, your geo-location may also be recorded in the photo?	○	○

		Very important	Important	Moderately Important	Slightly important	Not important
P113:	Convenience is important to you.	①	②	③	④	⑤
P114:	Privacy is important to you.	①	②	③	④	⑤

Part 2 features two major types of questions. The first type of questions (Figure 8), question codes P201, P202, P203 and P204, used a five-point Likert scale to show students' degree of concern about their private information stored in their mobile devices. The degrees of concern were 'not concerned at all', 'a little concerned', 'concerned', 'very concerned' and 'absolutely concerned'.

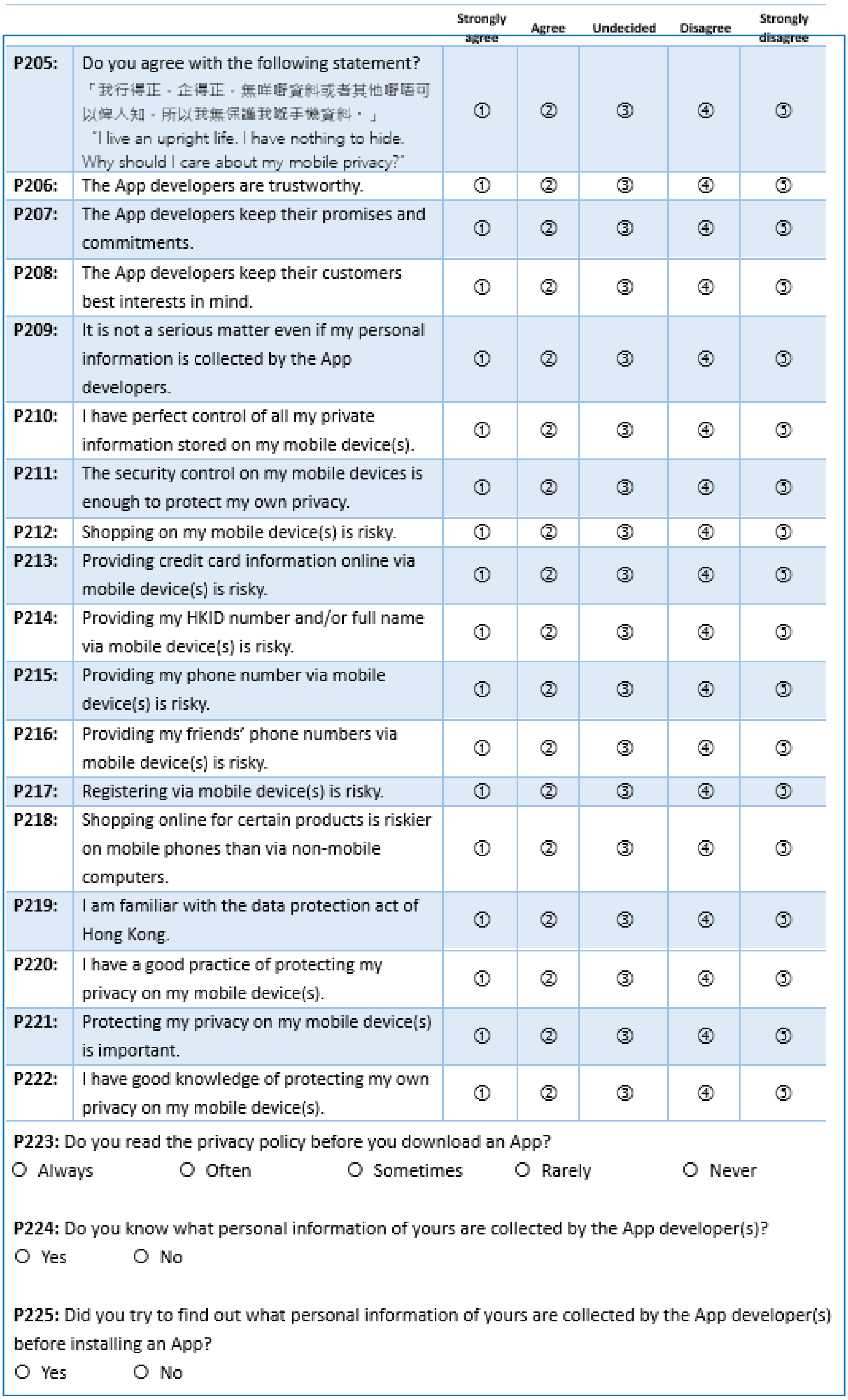
Figure 8: First Type of Questions in Part Two of the Survey (from P201 to P204)



		Not concerned at all	Of little concerned	Of average concerned	Very concerned	Absolutely concerned
P201:	The information I submit on my mobile device(s) could be misused.	①	②	③	④	⑤
P202:	People can get hold of my private information on my mobile device(s).	①	②	③	④	⑤
P203:	Others might use my mobile device(s) to submit information.	①	②	③	④	⑤
P204:	Information submitted through my mobile device(s) could be used in many ways, such as advertising, that I cannot foresee.	①	②	③	④	⑤

The second type of questions (Figure 9), question codes P205, P206, P207, P208, P209, P210 and P220, used another five-point Likert scale. Students can choose from 'strongly agree', 'agree', 'undecided', 'disagree' to 'strongly disagree' to show their attitudes towards managing their online privacy.

Figure 9: Second Type of Questions in Part Two of the Survey (from P205 to P225)



		Strongly agree	Agree	Undecided	Disagree	Strongly disagree
P205:	Do you agree with the following statement? 「我行得正，企得正，無咩嘢資料或者其他嘢唔可以俾人知，所以我無保護我嘅手機資料。」 "I live an upright life. I have nothing to hide. Why should I care about my mobile privacy?"	①	②	③	④	⑤
P206:	The App developers are trustworthy.	①	②	③	④	⑤
P207:	The App developers keep their promises and commitments.	①	②	③	④	⑤
P208:	The App developers keep their customers best interests in mind.	①	②	③	④	⑤
P209:	It is not a serious matter even if my personal information is collected by the App developers.	①	②	③	④	⑤
P210:	I have perfect control of all my private information stored on my mobile device(s).	①	②	③	④	⑤
P211:	The security control on my mobile devices is enough to protect my own privacy.	①	②	③	④	⑤
P212:	Shopping on my mobile device(s) is risky.	①	②	③	④	⑤
P213:	Providing credit card information online via mobile device(s) is risky.	①	②	③	④	⑤
P214:	Providing my HKID number and/or full name via mobile device(s) is risky.	①	②	③	④	⑤
P215:	Providing my phone number via mobile device(s) is risky.	①	②	③	④	⑤
P216:	Providing my friends' phone numbers via mobile device(s) is risky.	①	②	③	④	⑤
P217:	Registering via mobile device(s) is risky.	①	②	③	④	⑤
P218:	Shopping online for certain products is riskier on mobile phones than via non-mobile computers.	①	②	③	④	⑤
P219:	I am familiar with the data protection act of Hong Kong.	①	②	③	④	⑤
P220:	I have a good practice of protecting my privacy on my mobile device(s).	①	②	③	④	⑤
P221:	Protecting my privacy on my mobile device(s) is important.	①	②	③	④	⑤
P222:	I have good knowledge of protecting my own privacy on my mobile device(s).	①	②	③	④	⑤

P223: Do you read the privacy policy before you download an App?

○ Always ○ Often ○ Sometimes ○ Rarely ○ Never

P224: Do you know what personal information of yours are collected by the App developer(s)?

○ Yes ○ No

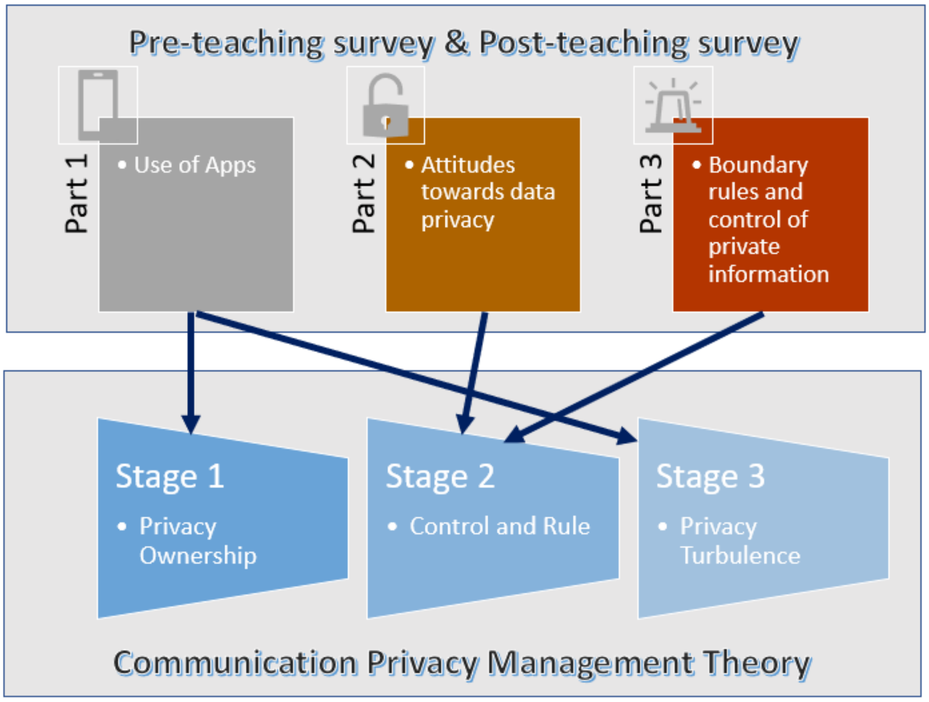
P225: Did you try to find out what personal information of yours are collected by the App developer(s) before installing an App?

○ Yes ○ No

3.5 To address Research Question 2

Three parts of the questionnaire survey are designed to answer Research Question 2: How effective is using CPM theory to improve HEI students' online privacy management strategies for their mobile devices? Figure 10 shows the survey parts employed to investigate the improvement in each of the three stage of CPM theory.

Figure 10: Parts of the Survey that Addressed Research Question 2


Pre-teaching survey & Post-teaching survey
Part 1
• Use of Apps
Part 2
• Attitudes towards data privacy
Part 3
• Boundary rules and control of private information
Stage 1
• Privacy Ownership
Stage 2
• Control and Rule
Stage 3
• Privacy Turbulence
Communication Privacy Management Theory

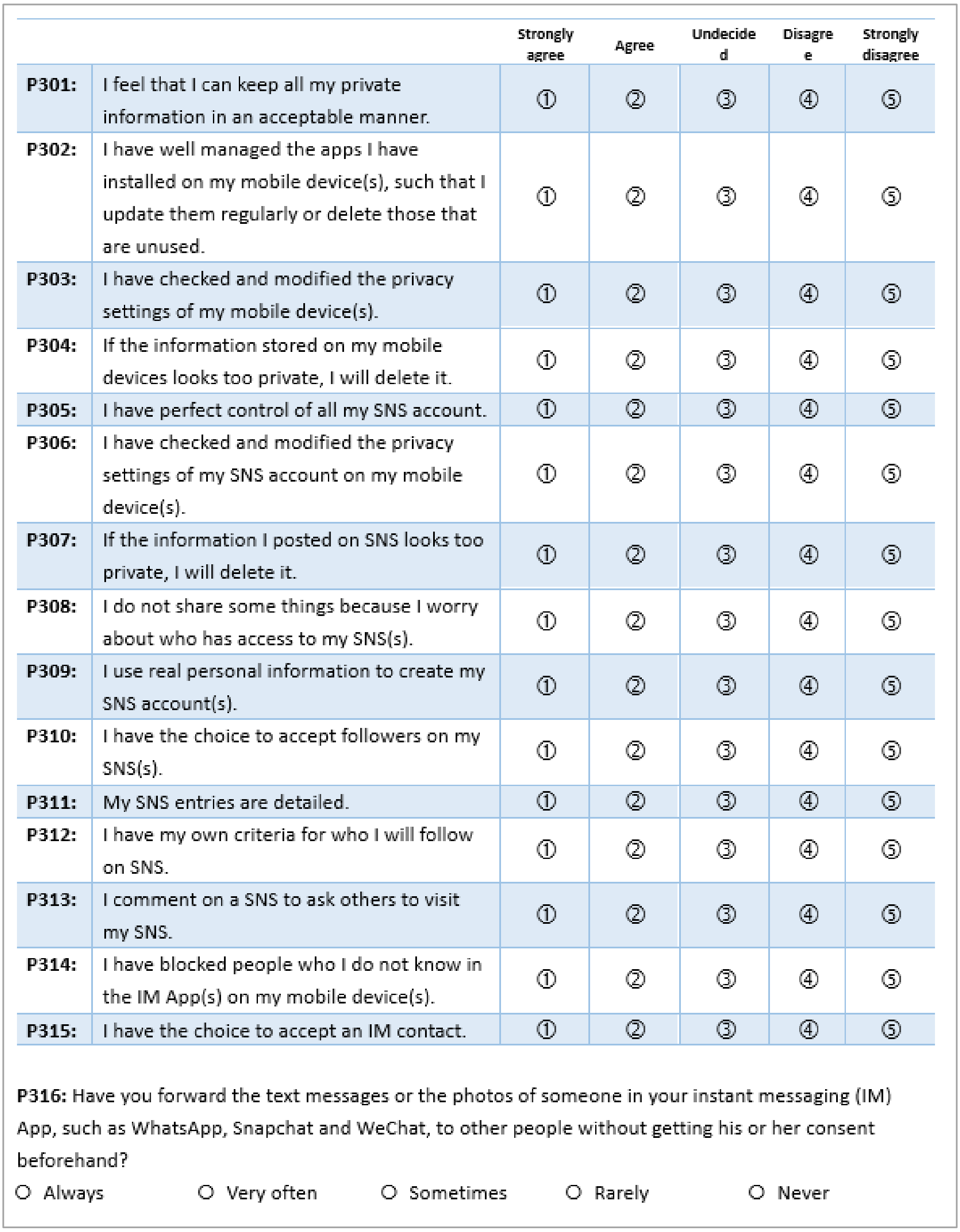
Stage 1 of CPM states the ownerships, in which people believe they own the information about themselves. Others become co-owners of people's private information. Students needed to know what kinds of personal information they owned as well as other people's personal information. Table 3 shows the questions that asked students what types of their personal information they owned as well as that of others that they kept.

Table 3: Questions Related to CPM Theory (Stage 1)

P115: What type of personal information about your friends, classmates or family members have been stored in your mobile devices? (You may choose more than one option.)	
☐ Friends' contact information (e.g. phone number, email) ☐ Entrance code of the building where you and your family live ☐ Someone's ATM password(s) ☐ Someone's online account number and password	☐ Their email addresses ☐ Their email account passwords ☐ Their personal and sensitive photos ☐ Others ☐ Haven't stored any personal information of others
P116: What types of your personal information have been stored in your mobile devices? (You may choose more than one option.)	
☐ Contact information (e.g. phone number, email address) ☐ Entrance code of the building where you and your family members live ☐ ATM password ☐ Online account ID and password	☐ Email address ☐ Email account password ☐ Personal and sensitive photos ☐ Others ☐ Haven't stored any personal information

Stage 2 refers to the control and rules that describe people's creation of boundaries to control their personal information. It mentions that people share and withhold information according to a system of rules. Figure 11 shows the questions related to Stage 2 of CPM theory, which asked students about their control and rules regarding online privacy management strategies.

Figure 11: Questions Related to CPM Theory (Stage 2)



		Strongly agree	Agree	Undecided	Disagree	Strongly disagree
P301:	I feel that I can keep all my private information in an acceptable manner.	①	②	③	④	⑤
P302:	I have well managed the apps I have installed on my mobile device(s), such that I update them regularly or delete those that are unused.	①	②	③	④	⑤
P303:	I have checked and modified the privacy settings of my mobile device(s).	①	②	③	④	⑤
P304:	If the information stored on my mobile devices looks too private, I will delete it.	①	②	③	④	⑤
P305:	I have perfect control of all my SNS account.	①	②	③	④	⑤
P306:	I have checked and modified the privacy settings of my SNS account on my mobile device(s).	①	②	③	④	⑤
P307:	If the information I posted on SNS looks too private, I will delete it.	①	②	③	④	⑤
P308:	I do not share some things because I worry about who has access to my SNS(s).	①	②	③	④	⑤
P309:	I use real personal information to create my SNS account(s).	①	②	③	④	⑤
P310:	I have the choice to accept followers on my SNS(s).	①	②	③	④	⑤
P311:	My SNS entries are detailed.	①	②	③	④	⑤
P312:	I have my own criteria for who I will follow on SNS.	①	②	③	④	⑤
P313:	I comment on a SNS to ask others to visit my SNS.	①	②	③	④	⑤
P314:	I have blocked people who I do not know in the IM App(s) on my mobile device(s).	①	②	③	④	⑤
P315:	I have the choice to accept an IM contact.	①	②	③	④	⑤

P316: Have you forward the text messages or the photos of someone in your instant messaging (IM) App, such as WhatsApp, Snapchat and WeChat, to other people without getting his or her consent beforehand?

○ Always ○ Very often ○ Sometimes ○ Rarely ○ Never

Stage 3 of CPM theory refers to privacy turbulence, which describes the scenario when the rules stated in Stage 2 are not followed and mistakes are made, thus resulting in turbulence. Questions P117 and P118 in Table 4 mention a scenario in which after students click to download a mobile app, the mobile app asks for permission to access their personal information and other people's personal information; students are asked if they would stop this download so as to prevent the turbulence.

Table 4: Questions Related to CPM Theory (Stage 3)

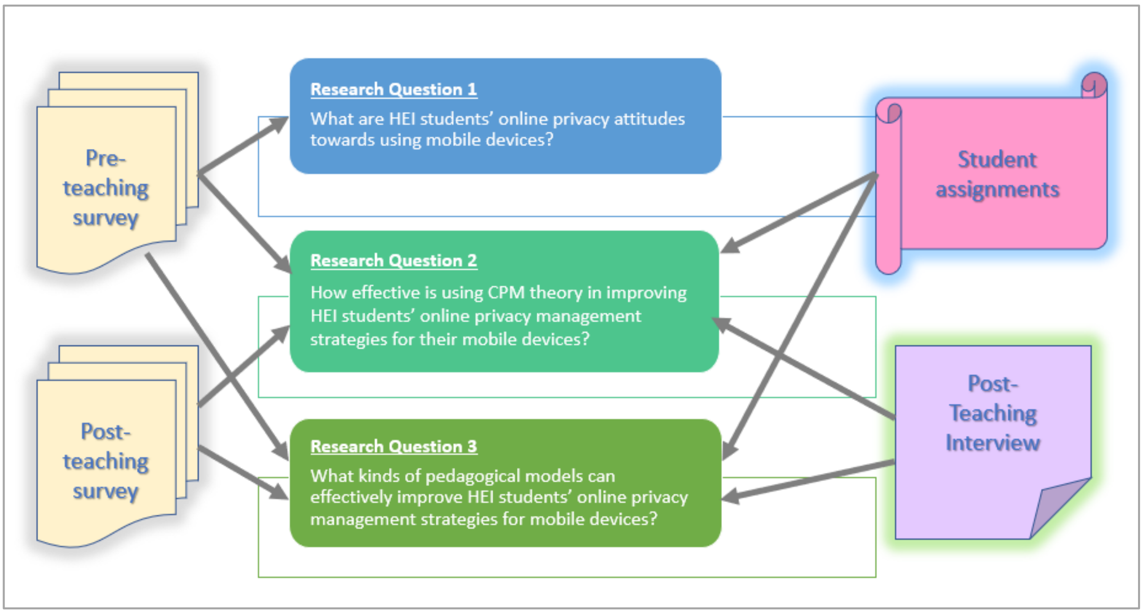
P117: Suppose that you are downloading an app on your mobile device. After you have clicked to download, the app asks access to your contacts' personal information (i.e. other people's personal information such as name and contact information) and sensitive photos about other people. If you can cancel the download, please answer the next question. If you continue with the download, state your reason below and then answer the next section.
P118: Refer to the previous question, if you will cancel the download, state your reason below.

3.6 To address Research Question 3

The results and findings of RQ1 and RQ2 are used to answer Research Question 3: What kinds of pedagogical models can effectively improve HEI students' online privacy management strategies for mobile devices?

Figure 12 shows different data sources for examining the three research questions. To address the research questions, this research collected qualitative and quantitative data. The quantitative data from the pre-teaching survey is mainly used to answer Research Question 1. Moreover, this study used a mixed method to analyse students' assignment, post-teaching interview and post-teaching survey in answering Research Questions 2 and 3.

Figure 12: Data Sources to Answer the Three Research Questions



Research Question 1
What are HEI students' online privacy attitudes towards using mobile devices?

Research Question 2
How effective is using CPM theory in improving HEI students' online privacy management strategies for their mobile devices?

Research Question 3
What kinds of pedagogical models can effectively improve HEI students' online privacy management strategies for mobile devices?

3.7 Design of the lesson

The teaching materials for online privacy management strategies were prepared according to CPM theory. The teaching activity was delivered through Moodle, a commonly used LMS in universities.

The teaching materials and Moodle activities were used in a pilot teaching to ensure that the direction and the focus of this study were correct and to improve the smoothness of future teaching sessions.

3.8 Implementation of Pedagogical Models

3.8.1 Pre-teaching survey

The pre-teaching surveys were conducted in the four target classes one month before teaching students' online privacy management strategies. The survey instrument is a closed-ended questionnaire, through which relevant data can be effectively gathered and analysed (Teddlie, 2009). If students were willing to participate in the survey, then student assistants would give them the survey. HEI students completed it anonymously, and completed survey forms were collected by student assistants. In this way, quantitative data were efficiently collected. These data were recorded in an SPSS file and analysed to provide a general prior understanding of students' knowledge and concepts of online privacy attitudes and management strategies. As the HEI students came from different academic backgrounds, this pre-teaching survey was crucial as it could provide the necessary data to enhance our pedagogical model before teaching. After the pre-teaching surveys were conducted, the gathered data were used to address RQ1.

3.8.2 Teaching

In this study, the teacher refined the designated teaching materials and LMS activities according to the results of the pre-teaching survey, and then used them to teach HEI students online privacy management strategies. Students participated in the activities on LMS, whereas the teacher observed the learning progress of students by viewing their answers on LMS and giving feedback to them after the lessons.

3.8.3 Student Assignment

An online assignment was set up on LMS and was released to students for their completion by the end of the lesson. The design of the online assignment was based on the teaching contents coming mainly from CPM theory. The purpose of this assignment is to find out students' understanding of the key points in the lesson and their improvement on their online privacy management strategies. The effectiveness of the pedagogical model can then be investigated through this assignment. To ensure the reliability of the marking of the assignments, the university invited a second marker to vet on the assignments.

3.8.4 Post-teaching survey

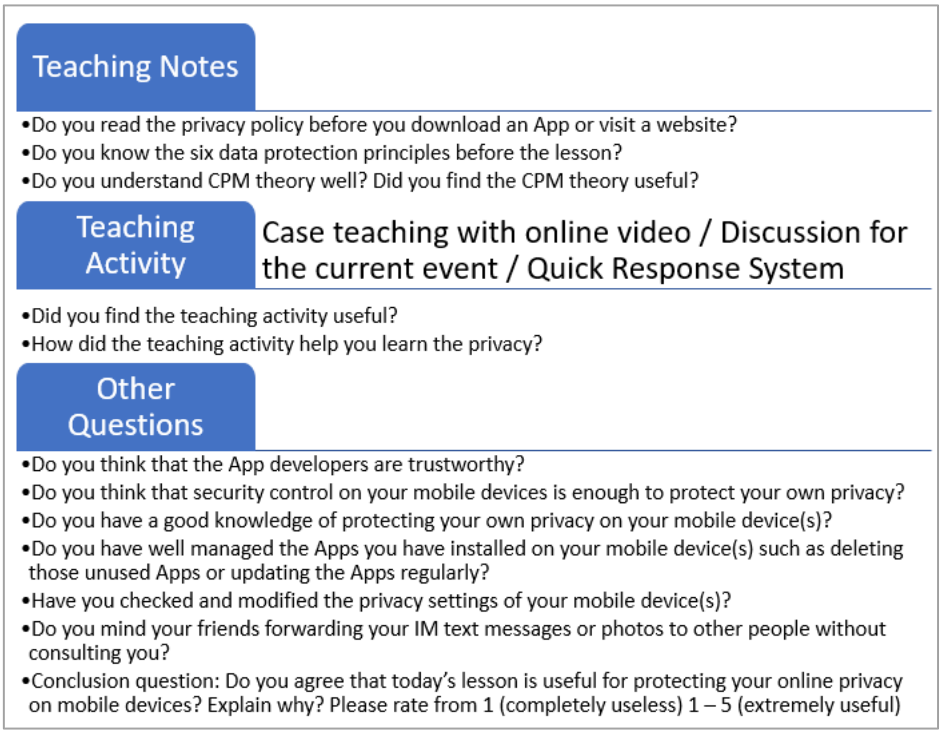
At the end of the lesson, students needed to answer the same questionnaire that they had previously answered before the lesson. This survey was intended to collect quantitative data related to students' understanding of online privacy management strategies after the lesson.

3.8.5 Post-teaching interview

A semi-structured interview was scheduled after the lesson. Two volunteer students from the taught class were invited to attend the interviews. The interviews were conducted by two student assistants separately. The identifying information of students was removed from the data and stored separately, and the link between the identifying information and the data is made through codes only. This measure ensures that the teacher would not be able to identify which set of data is collected from which interviewee. As such, interviewees were comfortable expressing their honest comments. The qualitative data from students' assignments and the post-teaching interviews underwent an in-depth analysis to examine students' understanding of the lesson, particularly the usefulness and their perception of the online privacy management strategies developed for mobile devices.

The purpose of the post-teaching interview is to find out the effectiveness of the teaching activities. The interview consisted of three parts, as shown in Figure 13.

Figure 13: Three Parts of the Post-teaching Interview



Teaching Notes

- Do you read the privacy policy before you download an App or visit a website?
- Do you know the six data protection principles before the lesson?
- Do you understand CPM theory well? Did you find the CPM theory useful?

Teaching Activity

Case teaching with online video / Discussion for the current event / Quick Response System

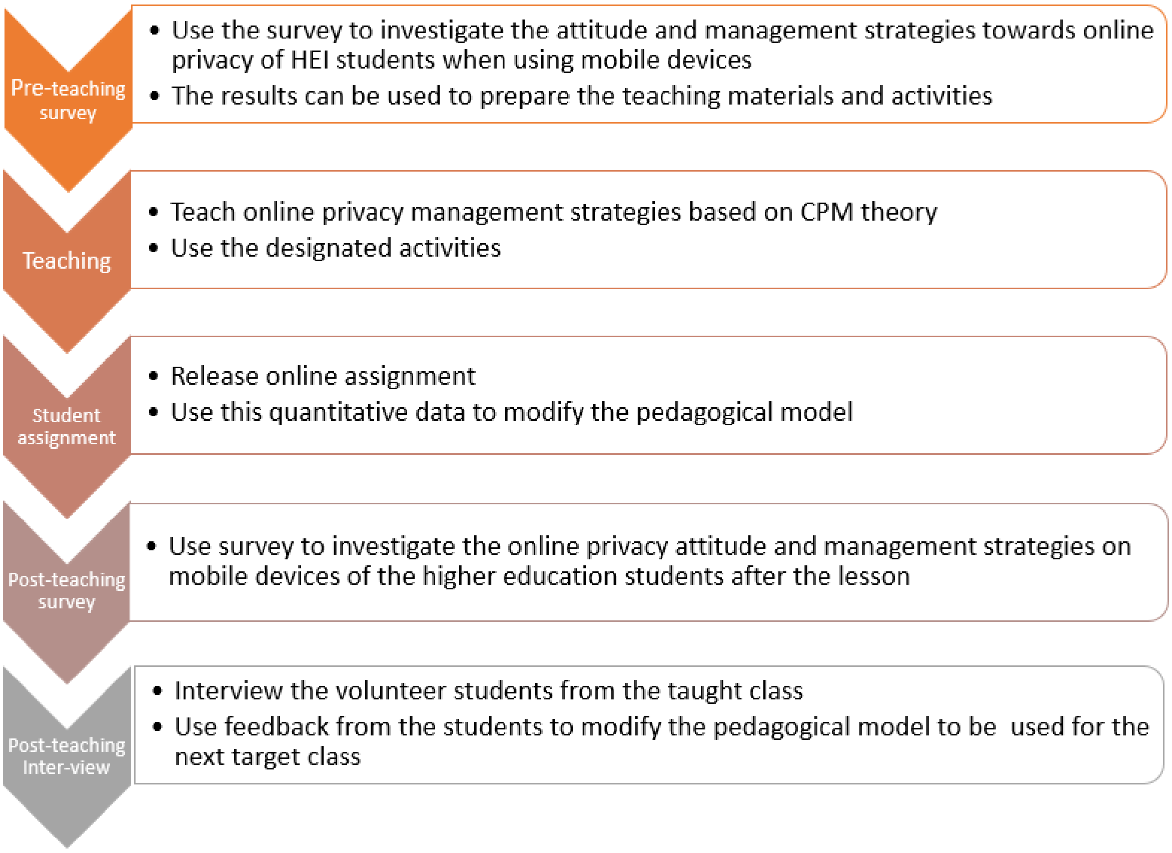
- Did you find the teaching activity useful?
- How did the teaching activity help you learn the privacy?

Other Questions

- Do you think that the App developers are trustworthy?
- Do you think that security control on your mobile devices is enough to protect your own privacy?
- Do you have a good knowledge of protecting your own privacy on your mobile device(s)?
- Do you have well managed the Apps you have installed on your mobile device(s) such as deleting those unused Apps or updating the Apps regularly?
- Have you checked and modified the privacy settings of your mobile device(s)?
- Do you mind your friends forwarding your IM text messages or photos to other people without consulting you?
- Conclusion question: Do you agree that today's lesson is useful for protecting your online privacy on mobile devices? Explain why? Please rate from 1 (completely useless) 1 – 5 (extremely useful)

Figure 14 provides a holistic picture of the implementation stage of the study. In each iteration, the pedagogical flow started with the pre-teaching survey and then teaching and assignment, and finally the post-teaching survey and the post-teaching interview were conducted.

Figure 14: Implementation of Teaching in Each Iteration



Pre-teaching survey

- Use the survey to investigate the attitude and management strategies towards online privacy of HEI students when using mobile devices
- The results can be used to prepare the teaching materials and activities

Teaching

- Teach online privacy management strategies based on CPM theory
- Use the designated activities

Student assignment

- Release online assignment
- Use this quantitative data to modify the pedagogical model

Post-teaching survey

- Use survey to investigate the online privacy attitude and management strategies on mobile devices of the higher education students after the lesson

Post-teaching Inter-view

- Interview the volunteer students from the taught class
- Use feedback from the students to modify the pedagogical model to be used for the next target class

3.9 Analysis of data collected

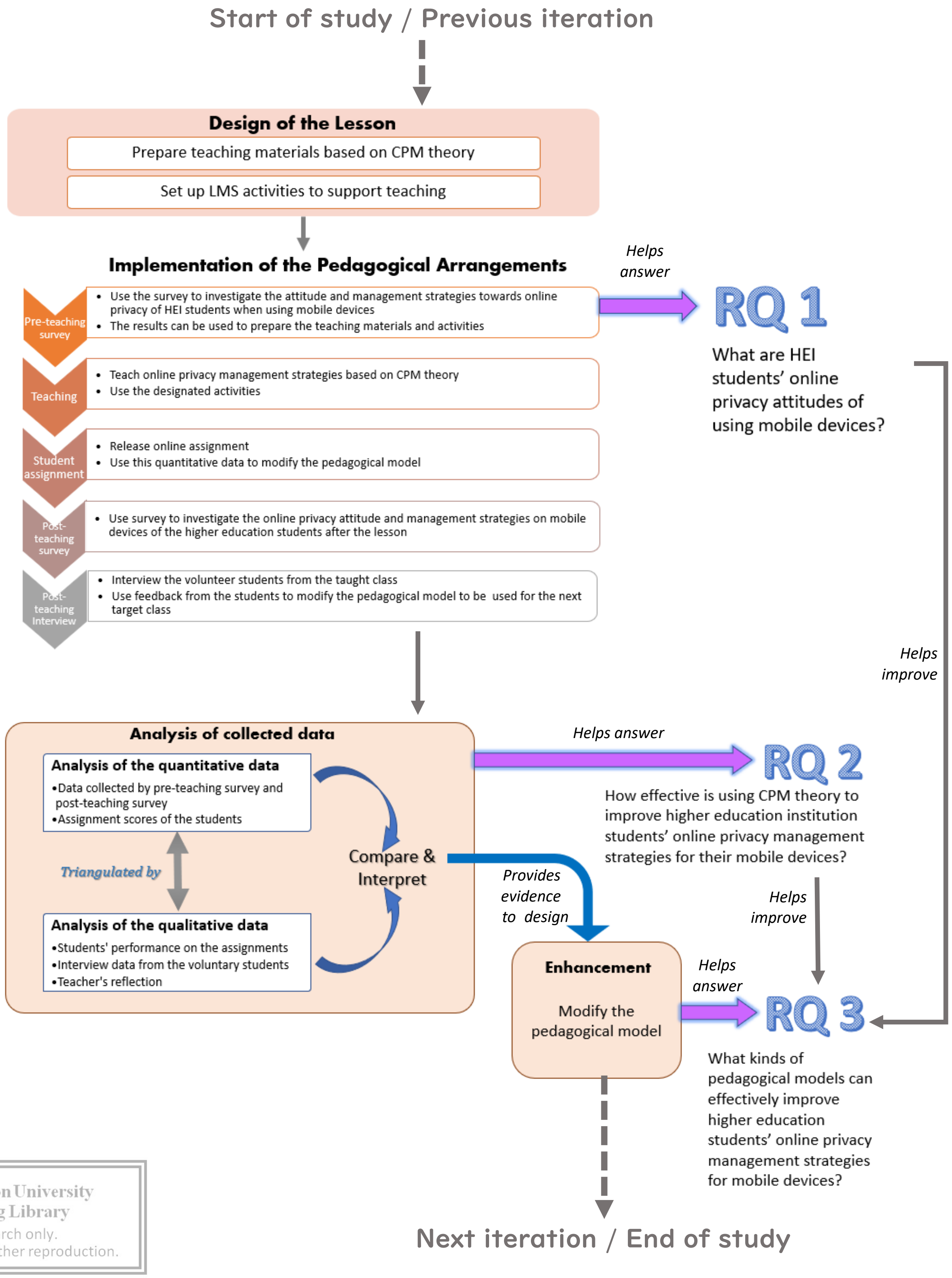
A convergent parallel mixed method was designed to compare the quantitative and qualitative data to see if the two sets of outcomes diverge or converge. The data collected from the post-teaching interview was qualitative, whereas the data collected from the pre-teaching survey, post-teaching surveys and students' assignments were quantitative. The qualitative data helped triangulate the data obtained from the survey instrument, and the results of the analysis provided answers for RQ 2. Thus, students' online privacy management strategies and the effectiveness of teaching these strategies were examined through the assessments provide information for the teacher to enhance his/her pedagogical model if necessary.

3.10 Enhancement of lesson design

After the first research iteration, the redesigned and enhanced pedagogical model was used to teach the second target class. Similarly, after the second research iteration, the pedagogical model was again modified and enhanced and used to teach the third target class. After the third research iteration, the pedagogical model was once more enhanced, and then ideally a well-designed effective pedagogical model would have been obtained and RQ 3 would have been answered.

On the basis of the literature review of different pedagogical methods in Chapter 2, case teaching with online videos will be adopted as the initial pedagogical model of this study. Figure 15 displays all stages for each research iteration in each class.

Figure 15: Stages in Each Research Iteration in Each Class


Start of study / Previous iteration
Design of the Lesson
Prepare teaching materials based on CPM theory
Set up LMS activities to support teaching
Implementation of the Pedagogical Arrangements
Pre-teaching survey
• Use the survey to investigate the attitude and management strategies towards online privacy of HEI students when using mobile devices
• The results can be used to prepare the teaching materials and activities
Teaching
• Teach online privacy management strategies based on CPM theory
• Use the designated activities
Student assignment
• Release online assignment
• Use this quantitative data to modify the pedagogical model
Post-teaching survey
• Use survey to investigate the online privacy attitude and management strategies on mobile devices of the higher education students after the lesson
Post-teaching Interview
• Interview the volunteer students from the taught class
• Use feedback from the students to modify the pedagogical model to be used for the next target class
Helps answer
RQ 1
What are HEI students' online privacy attitudes of using mobile devices?
Helps improve
Analysis of collected data
Analysis of the quantitative data
•Data collected by pre-teaching survey and post-teaching survey
•Assignment scores of the students
Triangulated by
Analysis of the qualitative data
•Students' performance on the assignments
•Interview data from the voluntary students
•Teacher's reflection
Compare & Interpret
Helps answer
RQ 2
How effective is using CPM theory to improve higher education institution students' online privacy management strategies for their mobile devices?
Provides evidence to design
Helps improve
Enhancement
Modify the pedagogical model
Helps answer
RQ 3
What kinds of pedagogical models can effectively improve higher education students' online privacy management strategies for mobile devices?
Next iteration / End of study

3.11 Ethical Concerns

Before the start of the research, four senior-year student assistants were recruited. They then attended a two-day programme to receive SPSS training and attend a workshop on interview skills. These student assistants participated in the pilot test of the survey instrument in the early stage.

At the start of the lesson on privacy, the teacher openly invited volunteer students to join the post-teaching interview. This recruitment was voluntary, as the interviews would last for 1 hour and would be conducted during students' peak season of projects/assignments/tests. Finally, only two volunteer students were successfully invited from each class. To make up for this shortcoming of insufficient volunteer students, the analysis of teachers' observation was also included as quantitative data after each iteration.

After the lessons, student assistants interviewed the volunteer students. As the volunteer interviewees may avoid making comments on the teacher directly, they could express their honest opinions. The volunteer interviewees were also told that their opinions would not affect their score in the module. The student assistants also helped input the quantitative data into SPSS files and transcribed individual interviews into qualitative data.

This study employed several methods to collect useful data from HEI students in the four target classes. The data collection procedures involving human participants and/or human-related data have gone through independent ethical review in accordance with the

Education University of Hong Kong’s Guidelines on Ethics in Research. Besides, the study has obtained the approval of the HSUHK.

For each class, approximately 30 students joined the quantitative data collection stage. Two students from each class joined the post-teaching interview, and students signed a consent form before they provided their personal information for this study. Therefore, they should understand the aims of this study and know how their personal information would be used and kept during the research activities.

Chapter 4: Results and Findings – Foundation Round of Teaching

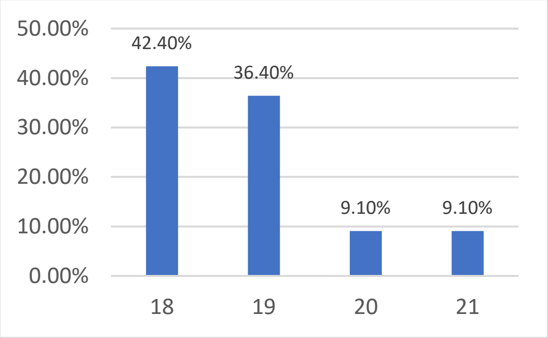
4.1 Introduction

The purpose of this chapter is to analyse the research findings of the foundation round teaching. This part is the first iteration of our DBR. Section 4.2 presents the demographic data of the first teaching class, and Section 4.3 presents the analysis of the pre-teaching survey results. On the basis of the initial analysis, Section 4.4 discusses the design of the foundation round teaching. Section 4.5 shows students' performance in the student assignment. Section 4.6 discusses students' privacy concerns regarding this teaching round. After that, Section 4.7 compares the results of the pre- and the post-teaching survey. Section 4.8 presents the results of the post-teaching interview. Section 4.9 includes the teachers' reflections. Finally, Section 4.10 presents the key findings of this teaching round. Section 4.11 summarises the findings from the foundation round.

4.2 Demographic Data of the Foundation Round Class

This section shows the demographic data of the first target class students who participated in this study. The foundation target class had a total of 33 students. Figures 16, 17, 18 and 19 listed the four categories of their demographic data, namely age, gender, study year and study major, respectively.

Figure 16: Age of Participants



Average Age: 18.84

Figure 17: Gender of Participants

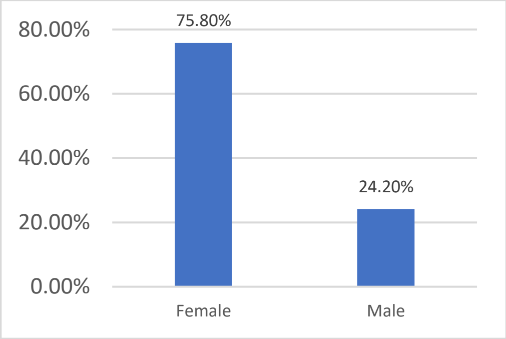
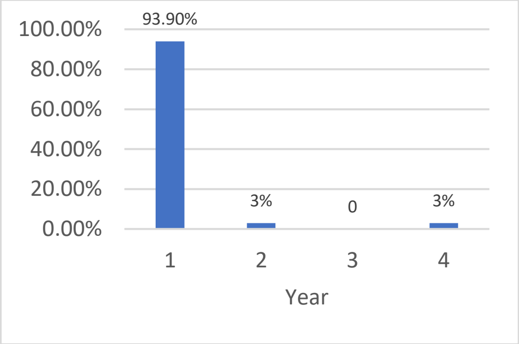
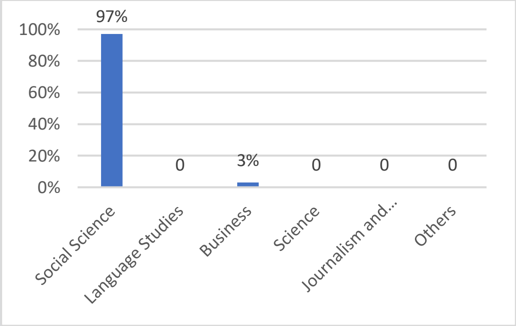


Figure 18: Year of Study



Average Year of Study: 1.12

Figure 19: Study Major



As shown in Figure 17, the average age of the first target class students was 18.84 years old. Students aged 18 comprised the biggest age group (42.4%), whereas students aged 19 comprised the smallest group (36.4%). According to Figure 18, female students comprised the majority of participants. Figure 19 shows that 93.9% of students from the first target class students were Year 1 students. Finally, Figure 20 shows that 97% of students from this class were Social Science majors.

4.3 Pre-teaching Survey Results of the Foundation Round of Teaching

The background information of students was collected through the pre-teaching survey. To understand students' background and their prior knowledge of online privacy, the pre-teaching survey questionnaires asked students two questions (i.e. A08 and J01): 'Did you take DSE ICT'? and 'Where did you learn the knowledge or skills of protecting your online privacy'? Tables 5 and 6 show the results, respectively.

Table 5: Percentage of Participants who had taken DSE ICT

		Number of participants	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	18.2	18.2	18.2
	No	27	81.8	81.8	100.0
	Total	33	100.0	100.0	

Answers to question J01 indicated that students mainly learned about online privacy from their primary (61%) and/or secondary education (88%).

Table 6: Sources of Students' Knowledge about Online Privacy

Source	Valid %
Primary education	**61%**
Secondary education	**88%**
Higher education	58%
Media such as newspapers or TV	58%
Social Networking Sites	58%
Parents	21%
Friends	39%
Others	3%

4.3.1 Part 1: Use of Mobile Devices

Part 1 included question P101 ('What is your most common purpose for using your mobile devices'?), Table 7 lists the results.

Table 7: Students' Most Common Purposes for Using their Mobile Devices

Purpose	**Valid %**	**Purpose**	**Valid %**
Browsing online forums	73%	Reading e-books	24%
Editing documents	33%	Reading news	64%
Instant messaging with friends	94%	Reading phone calls	64%
Listening to music	73%	Sending or receiving email	64%
Listening to radio	3%	Taking photos	70%
Looking for information	76%	Using calendar and notes	42%
Online banking and finance	36%	Using social networks	97%
Online shopping	73%	Watching videos	76%
Playing games	61%	Web surfing	42%
Reading comics	18%	Others	0%

Students from the first class commonly used their mobile device for social networking and for instant messaging with friends with a valid percentage of 97% and 94%, respectively.

Question P103 asked students: 'Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access rights to the information on your mobile devices?' The survey revealed that 45.5% of participants read the terms and conditions of some of their installed apps. Furthermore, Table 8 shows that 42.4% of respondents did not read the terms of conditions or ensured that they understood the app's access rights before installing it.

Table 8: Proportion of Students who Read the Terms and Conditions prior to Installing an App

	Valid %
Students who read the terms and conditions	12.1%
Students who did not read the terms and conditions	42.4%
Students who read the terms and conditions only for some of the apps	45.5%
Total	100.0%

Table 9: Students' Considerations when Deciding to Install an App

Item	Valid %
Functions	79%
Free or paid	79%
User reviews	58%
Popularity	55%
Ease of use	55%

Item	Valid %
Degree of necessity	52%
Download time	12%
Terms and conditions	9%
Privacy policy	6%
Others	0%

Question P104 asked participants: 'What do you consider when you install an app'? Table 9 shows that students considered mainly the functions and cost (free or paid) of an app before installing it. Only 9% and 6% of students of this class considered the terms and conditions and the privacy policy before installing an app. These findings showed that students did not understand the importance of protecting their online privacy while using their mobile devices. Accordingly, the teacher had considered and addressed these two issues when teaching this class.

Table 10 shows that screen lock was the most common protective measure taken by 79% of students of this class. However, only 9% and 12% of students installed anti-virus and anti-theft software, respectively. These findings indicated that students did little to protect the security of their mobile devices.

Table 10: Students' Protective Measures for their Mobile Devices

Measure	Valid %
Set up auto screen lock	79%
Set up screen lock	79%
Installed anti-theft software	12%
Installed anti-virus software	9%
Others	3%

The findings shown in Table 11 reflect that 76% of students knew that their contact lists were being uploaded to SNS servers, and 85% of students knew that their geo-location were being recorded in the pictures that they captured. However, only 58% of students knew that some apps would take actions that they were not informed beforehand.

Table 11: Students' Awareness of the Access Rights of Apps

	Item	Yes (%)	No (%)
P110:	Do you know that your contact lists may be uploaded to the central servers of the social networking apps that you are using?	76%	24%
P111:	Do you know that some apps will take actions that they have not mentioned they would?	58%	42%
P112:	Do you know that, when you take a picture with your mobile devices, your geo-location may be recorded in the photo?	85%	15%

Table 12 shows students’ perceptions of the importance of convenience and privacy. The results indicated that convenience and privacy had the same degree of importance to students. The mean five-point Likert scale result of convenience and privacy was 3.09, whereas the SD of convenience was 0.843 and that of privacy was 0.947.

Table 12: Mean and SD of Students’ Perception of Convenience and Privacy of an App

	Item	Mean*	(S.D.)
P113:	Convenience is important to you.	3.09	(0.843)
P114:	Privacy is important to you.	3.09	(0.947)

**Note: 5 = very important; 4 = important; 3 = moderately important; 2 = slightly important; 1 = not important*

Table 13: Types of the Personal Information of Friends, Classmates and Family Members that are Stored in Students’ Mobile Devices

Item	**Valid %**
Friends’ contact information	88%
Their personal and sensitive photos	58%
Their email addresses	45%
Their online account number and password	27%
Their email account passwords	21%
Entrance code of the building where you and your family members live	18%
Their ATM password(s)	12%
None	3%
Others	3%

Table 13 reveals that 88% of students stored the contact lists of their friends, classmates and family members on their mobile devices; 58% of students stored personal and sensitive photos; and 45% of students stored email addresses on their mobile devices. The findings also showed that students stored: someone’s online account IDs and passwords (27%), email account passwords (21%), entrance code of buildings (18%) and ATM passwords (12%) on their mobile devices. Although these percentages were not significantly high, the information was highly sensitive and should not be given to strangers under any circumstances.

Table 14 lists the types of personal information that students stored on their mobile devices: 82% of students saved contact information and email addresses on their mobile devices, and 61%, 58% and 58% of them saved email account passwords, online account IDs and passwords and personal and sensitive photos on their phone, respectively.

Table 14: Types of Personal Information Stored in Students' Mobile Devices

Item	**Valid %**
Contact information	82%
Email addresses	82%
Email account passwords	61%
Online account ID and password	58%
Personal and sensitive photo	58%
Entrance code of the building where you and your family members live	15%
ATM password(s)	15%
Others	9%

The findings shown in Table 13 and Table 14 reveal that students stored several private information of their own as well as that of their friends, classmates and family members on their mobile devices. However, Table 12 reports that students found their privacy important. Hence, the results shown in Table 10 and Table 12 are contradictory. On the one hand, students did not do much to protect their mobile devices. On the other hand, they consider their privacy important. Therefore, the teacher should take note of this inconsistency and address it when teaching the first target class.

A scenario was presented to students: 'Suppose that you are downloading an app on your mobile devices. After you have clicked to download, the app asks for access to your contacts' personal information (i.e. names, phone numbers) and sensitive photos'. If the student were to continue the download, then he/she may write his/her reason in Question P117; otherwise, the student is instructed to proceed to Question P118. A total of 29 respondents out of 33 gave their reasons. Tables 15 and 16 listed some of their answers.

Table 15: Sample Reasons of Students who Decided to Continue Downloading a Hypothetical App Despite Privacy Risks

P117: You continue with the download (14 responses; Valid %: 48.28%)
'Not easy for others to access personal info. Will only download popular app.'
'Not really risky; the app can really help me, and it is useful.'
'That app is what I needed to use, and no other app can be a substitute.'
'The game is popular.'
'Useful.'
'I am not afraid of my personal information getting hacked by apps.'
'I need the function of the app.'
'I think the information can make the app more convenient when using.'
'I need to use it.'
'I need the app/the app attracts me.'
'I want to use the app.'
'It is needed whenever I need to download an app.'
'Can help the app function.'
'I need the app.'

Table 16: Sample Reasons of Students who Decided not to Continue Downloading a Hypothetical App due to Privacy Risks

P118: You will cancel the download (15 responses; Valid %: 51.72%)
'I think privacy is very important to me, and I don't know how the apps will use my information.'
'Afraid of leakage of information.'
'Another app performs similar functions.'
'Don't want personal information read by the third party.'
'Hope. Because I haven't asked other people.'
'To protect my privacy.'
'To perfect my privacy.'
'It is so strange that it required me to access other people's personal information.'
'It's dangerous to give other people access to private photos.'
'I don't want my personal information sent out.'
'I don't want my personal information known by others.'
'I don't know what photo they will take and access.'
'No, it's a privacy problem.'
'I don't want to leak my personal privacy.'
'Afraid of leakage of information.'

4.3.2 Part 2: Attitudes towards Data Privacy

Table 17 shows students' attitudes towards data privacy in their mobile devices. Questions P201, P202, P203 and P204 were concerned with the possibility that students' information stored on their mobile devices may be misused by others. According to the responses, the mean five-point Likert scale scores of these questions were all over 3, ranging from 3.38 to 3.56. In the scale, 1 represents 'not concerned at all' and 5 represents 'absolutely concerned'. These scores reflected that respondents were slightly concerned about their information being misused by others through their mobile devices.

Table 17: Students' Attitudes towards Data Privacy in their Mobile Devices

	Item	Mean*	S.D.
P201:	The information I submit on my mobile device(s) could be misused.	3.41	0.837
P202:	People can get hold of my private information on my mobile device(s).	3.56	1.134
P203:	Others might use my mobile device(s) to submit information.	3.44	1.162
P204:	Information submitted through my mobile device(s) could be used in many ways, such as advertising, which I cannot foresee.	3.38	1.008

** Note: 1 = not concerned at all; 2 = a little concerned; 3 = concerned; 4 = very concerned; 5 = absolutely concerned*

The answers to Questions P206, P207, P208 and P209 displayed students' perception on app developers. As shown in Table 18, the mean five-point Likert scale scores of these questions ranged from 1.47 to 1.76. In the scale, 5 represents 'strongly agree' and 1 represents 'strongly disagree'. Overall, students slightly disagreed that app developers were trustworthy, and kept their promises and commitments.

Questions P212 to P217 indicated students' attitude towards providing information via their mobile devices. The mean five-point Likert scale scores of these questions were all below 3.80, ranging from 2.03 to 2.76. In the scale, 5 represents 'strongly agree' and 1 represents ‘strongly disagree’. These scores indicated that students agreed that providing private information such as HKID number, full name, phone number and friends’ phone numbers was risky. The mean five-point Likert scale score of Question P219 was 1.88, which revealed that respondents were not familiar with the data protection act of Hong Kong. Respondents’ practice and knowledge of protecting their privacy on their mobile devices, their mean five-point Likert scale scores of questions 28 and 30 were 2.30 and 2.18, respectively. They showed that the respondents slightly disagreed that they had a good practice and good knowledge in the issue. Finally, Table 18 lists the mean five-point scale score result of Question P221, which was 2.67, regarding the importance of protecting the respondents’ privacy on their mobile devices. This finding indicated that students slightly disagreed regarding the importance of protecting their privacy in their mobile devices.

Table 18: Students' Responses about the Importance of Protecting their Privacy in their Mobile Devices

	Item	Mean*	S.D.
P205	I live an upright life, and I have nothing to hide. Why should I care about my mobile privacy?	1.18	0.882
P206	App developers are trustworthy.	1.58	0.867
P207	App developers keep their promises and commitments.	1.76	1.001
P208	App developers keep their customers' best interests in mind.	1.58	1.062
P209	It is not a serious matter even if my personal information is collected by app developers.	1.47	0.879
P210	I have perfect control of all my private information stored on my mobile device(s).	1.73	0.839
P211	The security control on my mobile devices is enough to protect my privacy.	2.09	1.071
P212	Shopping with my mobile device(s) is risky.	2.21	0.857
P213	Providing credit card information online via mobile device(s) is risky.	2.55	1.063
P214	Providing my HKID number and/or full name via mobile device(s) is risky.	2.76	1.001
P215	Providing my phone number via mobile device(s) is risky.	2.03	1.045
P216	Providing my friends' phone numbers via mobile device(s) is risky.	2.18	1.103
P217	Registering via mobile device(s) is risky.	2.19	0.859
P218	Shopping online for certain products is riskier on mobile phones than via non-mobile computers.	2.22	0.870
P219	I am familiar with the data protection act of Hong Kong.	1.88	0.927
P220	I have a good habit of protecting my privacy on my mobile device(s).	2.30	0.770
P221	Protecting my privacy on my mobile device(s) is important.	2.67	0.816
P222	I have good knowledge of protecting my own privacy on my mobile device(s).	2.18	0.917

* *Note: 5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

4.3.3 Part 3: Boundary Rules and Control of Private Information on Mobile Devices

As shown in Table 19: , the mean five-point Likert scale scores of Questions P301, P302, P303 and P304 were all below 3. In the scale, 5 represents 'strongly agree' and 1 represents 'strongly disagree'. These findings reflected that participants admitted that they slightly did not manage and kept their private information stored on their mobile devices. The mean five-point Likert scale scores of Questions P302, P303 and P304 were respectively 2.58 (SD: 0.614), 2.27 (SD: 0.839) and 2.42 (SD: 0.830). These results showed that participants often did not delete and/or update the apps on their mobile devices, checked and modified the privacy settings of their mobile devices and would delete the information stored on mobile devices that were too private.

Table 19: Students' Habits and Attitudes towards Managing the Privacy Settings in their Mobile Devices

	Item	Mean[1]	S. D.
P301	I feel that I can keep all my private information in a way that I feel is acceptable.	2.52	0.619
P302	I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	2.58	0.614
P303	I have checked and modified the privacy settings of my mobile device(s).	2.27	0.839
P304	If the information stored on my mobile devices looks too private, then I will delete it.	2.42	0.830

This section exhibits participants' boundary rules and control of their private information stored on their SNS. Table 20: Mean Scores of Students' Boundary Rules and Control of SNS Information (Questions P305–313)lists the mean scores of the answers to Questions P305 – P313, which were all below 3 ranging, from 2.09 to 2.94. These scores suggested that participants slightly disagreed that they had enough or proper boundary rules and

[1] Note: 5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree

control of their SNS information and settings on their SNS accounts. These findings were consistent with the results of Part 2.

Table 20: Mean Scores of Students' Boundary Rules and Control of SNS Information (Questions P305–313)

	Item	Mean*	SD
P305	I have perfect control of all my SNS accounts.	2.47	0.718
P306	I have checked and modified the privacy settings of my SNS account on my mobile device(s).	2.62	0.751
P307	If the information I posted on SNS looks too private, then I will delete it.	2.78	0.792
P308	I do not share some things, because I worry about who has access to my SNS(s).	2.78	0.659
P309	I use real personal information to create my SNS account(s).	2.44	0.801
P310	I have the choice to accept followers on my SNS(s).	2.94	0.759
P311	My SNS entries are detailed.	2.09	0.928
P312	I have my own criteria for who I will follow on SNS.	2.78	0.608
P313	I comment on a SNS to ask others to check out my SNS.	2.53	0.718

** Note: 5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

This part asked respondents about their boundary rules and control of their private information on IM accounts. On the basis of the five-point Likert scale, where 5 represents 'strongly agree' and 1 represents 'strongly disagree', the mean scores of responses of Questions P314 and P315 were 2.72 (S.D. 0.888) and 2.84 (S.D. 0.628), respectively. These findings were consistent with the results of Part 2.

Table 21: Mean Scores of Students' Boundary Rules and Control of SNS Information (Questions P314–315)

	Item	Mean*	S.D.
P314	I have blocked people who I do not know in the IM app(s) on my mobile device(s).	2.72	0.888

P315	I have the choice to accept an IM contact.	2.84	0.628

** Note: 5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

Question P316 asked respondents about forwarding someone's text messages or photos to other people without seeking their consent beforehand. According to the five-point Likert scale, where 5 represents 'always' and 1 represents 'never', the mean scores of the responses was 2.19 (S.D. 0.896). This result reflected that respondents did not often forward someone's text messages and photos to others.

Table 22: Students who Forwarded the Text Messages or Photos of their Contacts in their IM App to Other People Without Getting his or her Consent Beforehand

N	**Valid**	**32**
	Missing	1
Mean[2]		2.19
Std. Deviation		0.896

The survey confirmed that the majority of students learnt about online privacy from their primary education and secondary education. They heavily utilised their mobile devices for the primary use of social networking. This result is consistent with the fact that contact information was the most common information stored in their mobile devices, and this habit led to cybersecurity threats. Their attitude towards data privacy was fair, and not much measures had been in place for security.

[2] Note: 5 = always; 4 = very often; 3 = sometimes; 2 = rarely; 1 = never

4.3.4 Key findings from the Pre-teaching survey

Table 23 lists the key findings from the foundation round pre-survey.

Table 23: Key Findings from the Foundation Round Pre-teaching Survey

Part 1: Use of Mobile Devices
1a. Foundation Round students commonly used their mobile device for social networking (97%) and instant messaging with friends (94%).
1b. When Foundation Round students decided to install an app, only 15% of them would consider the terms and conditions and privacy policy. These figures indicated that participating students did not understand the importance of protecting their online privacy while using their mobile devices. Accordingly, the teacher had considered and addressed these two issues when teaching this class.
1c. Screen lock was the most common protective measure taken by 79% of students from the Foundation Round class. However, only 9% and 12% of students installed anti-virus and anti-theft software on their mobile devices, respectively. These findings reflected that students did little to protect their mobile devices.
1d. Moreover, 76% of students knew that their contact lists were being uploaded to the SNS servers, whereas 85% of students knew that their geo-location was being recorded in the pictures that they captured. However, only 58% of students knew that some apps would take actions that they were not informed of beforehand.
1e. Students' perceptions on the importance of convenience and privacy. Convenience and privacy had the same degree (with a mean score of 3.09) of importance to students.
1f. Students stored numerous private information of their own as well as that of their friends, classmates and family members on their mobile devices. Table 12 reports that students found their privacy important. Hence, the results shown in Table 10 and Table 12 are contradictory. On the one hand, students did not do much to protect their mobile devices; on the other hand, they considered their privacy important. Therefore, the teacher should take note of this inconsistency and address it when teaching the Foundation Round class.
Part 2: Attitudes Towards Data Privacy
2a. Participating students from the Foundation Round were slightly concerned about their information being misused by others through their mobile devices.
2b. Participants slightly disagreed that app developers were trustworthy, and kept their promises and commitments. Students agreed that providing private information such as HKID number, full name and phone numbers was risky.
2c. Foundation Round students were not familiar with the data protection act of Hong Kong (with a mean score of 1.88).
2d. Foundation Round students slightly disagreed that they had a good practice and good knowledge of online privacy.
Part 3: Boundary Rules and Control of Private Information on Mobile Devices
3a. Foundation Round students found themselves well managing and maintaining their private information stored on their mobile devices.
3b. Participating students had deleted and/or updated the apps on their mobile devices

regularly, checked and modified the privacy settings of their mobile devices and would delete information stored on mobile devices that was too private.

3c. Overall, participants agreed that they had enough or proper boundary rules and control of their SNS information and settings on their SNS accounts.

3d. Foundation Round students quite often forwarded someone's text messages and photos to others.

The pedagogical model and the teaching in the Foundation Round were designed on the basis of these key findings.

4.4 Foundation Round of Teaching

Important ideas on the lesson design were generated and summarised in Table 24 according to the key findings of the pre-teaching survey shown in Table 23.

Table 24: Ideas on the Lesson Design Inspired by the Pre-teaching Survey

Students' level of understanding	**Main concepts - Items**	**Evidence (Key findings from Table 23)**	**Teaching strategy/reinforcement**
A. *Well understood*	1. Malware related to online privacy	1c	● Case study ● Student assignment ● Direct teaching should be strengthened in the class
B. *Poorly understood*	1. PCPD six data protection principles 2. Mobile apps permission details 3. Online privacy management strategies	2c 1b 3a, 3b and 3c	
C. *Overlooked*	1. Online privacy on mobile devices	1f, 2c and 2d	

Accordingly, an initial teaching plan for the first iteration was designed and shown in Table 25. The major teaching strategy used in the foundation round teaching was case video method.

Case video can also be called case, case method or case study method. A case is usually a 'description of an actual situation, commonly involving a decision, a challenge, an opportunity, a problem or an issue faced by a person or persons in an organization' (Leenders et al., 2001). Under this teaching strategy, students are required to apply what they have learnt to solve real-life cases (Gallego, Fortunato, Rossi, Korol, & Moretton, 2013). These cases are created from real-life situations and problems. Students need to exercise their critical analysis and decision-making to resolve them (Ozdilek, 2014). Although case study methods have been employed in business, law and medical education for a long time, they are only recently adopted in science education (Cameron, Trudel, Titah, & Léger, 2012), and were first used in science education in the form of science stories by James B. Conant of Harvard in 1949 (Herreid, 2006).

In this study, case study teaching was employed to motivate students to learn about online privacy management. The basic concepts of the topic were then delivered to students using presentation slides.

The findings shown in Table 13 and 14 revealed that students stored numerous private information of their own as well as that of their friends, classmates and family members on their mobile devices. However, Table 12 reports that students found their privacy important. Hence, the results shown in Table 10 and Table 12 are contradictory. On the one hand, students did not do much to protect their mobile devices; on the other hand, they considered their privacy important. Therefore, the teacher took note of this inconsistency and addressed it when teaching the first target class. Thereupon, appropriate teaching activities were developed and conducted in this iteration. Finally, as a form of reinforcement, the teacher summarised the key points to students at the end of the lesson. All these pedagogical models were adopted to foster and improve students' online privacy management strategies.

Table 25: Pedagogical Model of the First Iteration

Session	Duration (minutes)	Components
1	15	Conduct pre-teaching survey (one week before the lesson).
2	5	Introduce the topic.
3	30	Teach the basic concepts of online privacy management using presentation slides ◎ Section one: Malware related to online privacy ◎ Section two: Online privacy in mobile devices ◎ Section three: PCPD six data protection principles ◎ Section four: Mobile app permission details ◎ Section five: Online privacy management strategies – CPM theory
4	60	Case studies: online video ◎ Case one: Managing Andy's Facebook information ◎ Case two: Managing Mr. Lau's private information such as mobile phone number and medical records
5	10	Summarise the lesson contents.
6	30	Complete online assignment in the foundation round.
7	15	Conduct a post-teaching survey.
8	60	Conduct a post-teaching interview among volunteer students.

The major part of this foundation teaching round was the case teaching using an online video. Two cases were delivered in the online video, and the cases were presented as investigative stories. The first case was about 'Managing Andy's Facebook information' and the second case was the 'Managing Mr. Lau's private information such as mobile phone number and medical records'. They demonstrated how online information could be protected in different scenarios and under different security needs.

The two cases included in the video were described as follows:

Case one

- Andy gave his SNS password to his girlfriend. She logged in to Andy's SNS without Andy's knowledge. The girlfriend read his location information through his SNS.
- Finally, Andy complained to the PCPD, but he was informed that friend/family affairs

are not protected by the data protection acts.

Case two

- Mr. Lau was a CEO of an organisation. His private data, such as his smartphone number were leaked to the media, because the computer system of his daughter's school was hacked. Mr. Lau's private information were posted on a website.
- Mr. Lau's secretary used an unsecure free Wi-Fi to access Mr. Lau's email account and download his medical report. Unfortunately, this Wi-Fi network was set up by a hacker. This medical report was finally leaked to the media.

4.5 Foundation Round Assignment

After the foundation round teaching, which is the first iteration, three questions were given to participating students as an assignment. The purpose of this assignment was to gauge students' understanding of the online privacy management knowledge taught to them. The assignment was designed from an online video. Table 26 shows the questions included in the assignment.

Table 26: Student Assignment in the Foundation Round

Question	Design Rationale
1. Answer the following questions with reference to Andy's case: (a) According to CPM theory, explain briefly why Andy experienced online privacy turbulence. (b) Suggest the privacy boundary setting(s) he should adopt in the future.	Strengthen students' knowledge listed in Table 23 – B1, B3, C1
2. Answer the following questions with reference to Mr. Lau's case: (a) State the online privacy problems that Mr. Lau encountered. (b) How was Mr. Lau's medical report leaked? Suggest a way that can prevent the same problem from occurring again.	Strengthen students' knowledge listed in Table 23 – A1, B2, C1

The first question asked students to apply CPM theory in Andy's case, whereas the second question asked students to suggest a solution to the online privacy problems that Mr. Lau encountered. The full mark of the assignment was eight.

Table 27: Results of the Foundation Found Student Assignment

Average:	**5.088235**
SD:	1.524897

4.6 Students' Privacy Concerns in the Foundation Round

The study used six levels to describe students' degree of privacy concern on the basis of the mean and the SD of the teaching rounds. Students with lower mean scores were categorised as 'unconcerned', whereas those with higher mean scores were grouped under 'extremely concerned'. Table 28 shows the levels of concern of students.

Table 28: Level of the Privacy Concern of Students

Range	Level
Mean + 2 S.D. to 5	Extremely concerned
Mean + S.D. to Mean + 2 S.D.	Very concerned
Mean to Mean + S.D.	Quite concerned
Mean − S.D. to Mean	Somewhat concerned
Mean − S.D. to Mean – 2 S.D.	A little concerned
1 to Mean − 2 S.D.	Unconcerned

In addition, Figure 20 shows the number of FR students in each level.

Figure 20 Pre-teaching Survey Results on the Level of Privacy Concerns of FR Students

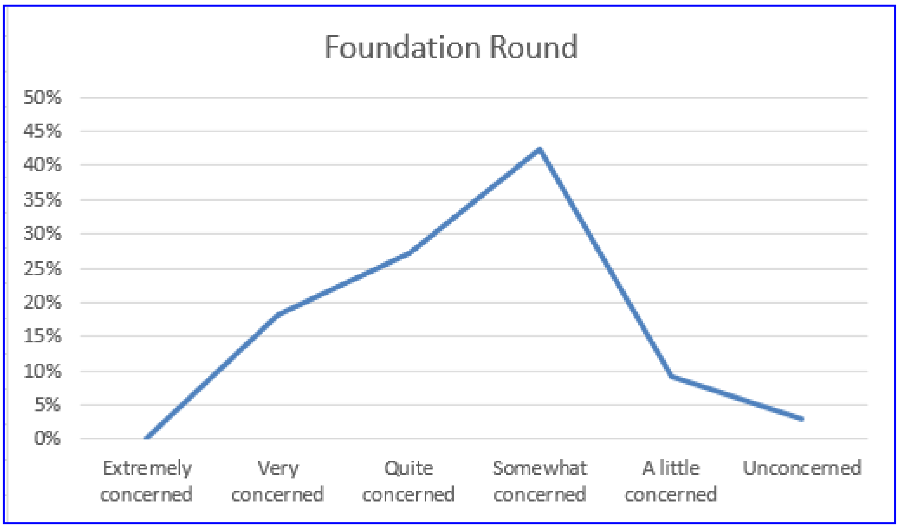


Table 29: Students' Level of Concern before the Lesson (Survey Part 2)

Level of Privacy Concerns	**Percentage of Foundation Round Students**	
Extremely concerned	0%	
Very concerned	18%	45%
Quite concerned	27%	
Somewhat concerned	42%	
A little concerned	9%	
Unconcerned	3%	

Figure 20 and Table 29 show the levels of privacy concern of FR students before the lesson. The majority of students in the FR are 'somewhat concerned' (42%) and 'quite concerned' (27%) about their online privacy. Moreover, no student was 'extremely concerned'. These results implied that FR students did not have major concerns on their own online privacy before the lesson.

4.7 Comparison of the Results of the Pre- and the Post-teaching Survey in the Foundation Round

Before and after the privacy lesson in the Foundation Round, the pre- and the post-teaching survey were distributed to participating students. The following sections included the basic statistical results and the cross-tabulation results of the foundation round.

4.7.1 Basic Statistical Results

After participating students finished their assignment, they were asked to complete the questionnaires again to identify any changes in their perceptions of online privacy.

Table 30: Comparison of Pre-teaching Survey and Post-teaching Survey Results on Students' Consideration of an App's Terms and Conditions Prior to Downloading

P103: Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access rights to the information on your mobile devices?		**Foundation Round_Pre**		**Foundation Round_Post**		**Percentage change**
		Frequency	Percentage	Frequency	Percentage	
Valid	Yes	4	12.1%	11	32.4%	+20%
	No	14	42.4%	10	29.4%	−13%
	I do for some of the apps, but not for all of them.	15	45.5%	13	38.2%	−7%
	Total	33	100.0%	34	100.0%	0%

Table 31: Comparison of Pre-teaching Survey and Post-teaching Survey Results on Students' Considerations in Downloading an App

P104: What will you consider when you install an app?	Foundation Round_Pre	Foundation Round _Post	Percentage change
Ease of use	54.5%	38.2%	−16.30%
Privacy policy	6.1%	47.1%	+41.00%
Terms and conditions	9.1%	23.5%	+14.40%

Table 32: Comparison of Pre-teaching Survey and Post-teaching Survey Results on Students' Protective Measures for their Mobile Devices

P106: What is/are the protective actions taken?	Foundation Round _Pre	Foundation Round _Post	Percentage change
Install anti-virus software	9.1%	23.5%	+14.40%

Table 33: Comparison of Pre-teaching Survey and Post-teaching Survey Results on Students' Knowledge of Apps' Undisclosed Actions on Mobile Devices

P111: Do you know that some apps will take actions that they have not mentioned they would?		Foundation Round _Pre		Foundation Round _Post		Percentage change
		Frequency	Percentage	Frequency	Percentage	
Valid	I know	19	57.6%	27	79.4%	+21.80%
	I don't know	14	42.4%	7	20.6%	−21.80%
	Total	33	100.0%	34	100.0%	0.00%

Table 34: Comparison of Pre-teaching Survey and Post-teaching Survey Results on the Importance of Convenience for Students

P113: Convenience is important to you.		**Foundation Round _Pre**		**Foundation Round _Post**		**Percentage change**
		Frequency	Percentage	Frequency	Percentage	
Valid	Very important	11	33.3%	4	11.8%	−21.50%
	Important	16	48.5%	20	58.8%	+10.30%
	Moderately important	4	12.1%	5	14.7%	+2.60%
	Slightly important	2	6.1%	4	11.8%	+5.70%
	Not important	0	0.0%	1	2.9%	+2.90%
	Total	33	100.0%	34	100.0%	0.00%

Table 35: Comparison of Pre-teaching Survey and Post-teaching Survey Results on the Importance of Privacy for Students

P114: Privacy is important to you.		**Foundation Round _Pre**		**Foundation Round _Post**		**Percentage change**
		Frequency	Percentage	Frequency	Percentage	
Valid	Very important	12	36.4%	9	26.5%	−10%
	Important	15	45.5%	15	44.1%	−1%
	Moderately important	4	12.1%	6	17.6%	+6%
	Slightly important	1	3.0%	3	8.8%	+6%
	Not important	1	3.0%	1	2.9%	0%
	Total	33	100.0%	34	100.0%	0%

Table 36: Comparison of Pre-teaching Survey and Post-teaching Survey Results of Part 2

		Foundation Round_Pre (N = 32, Missing = 1)		**Foundation Round _Post (N = 34, Missing = 1)**		**t-test**
		Mean	SD.	Mean	SD.	
P201	The information I submit on my mobile device(s) could be misused.	3.41	0.837	3.56	0.860	0.468
P202	People can get hold of my private information on my mobile device(s).	3.56	1.134	3.74	0.710	0.465
P203	Others might use my mobile device(s) to submit information.	3.44	1.162	3.76	0.819	0.194
P204	Information submitted through my mobile device(s) could be used in many ways, such as advertising, which I cannot foresee.	3.38	1.008	3.82	0.758	0.047
P205	I live an upright life, and I have nothing to hide. Why should I care about my mobile privacy?	3.82	0.882	3.71	1.060	0.639
P206	App developers are trustworthy.	3.42	0.867	3.32	0.976	0.657
P207	App developers keep their promises and commitments.	3.24	1.001	3.26	0.994	0.927
P208	App developers keep their customers' best interests in mind.	3.42	1.062	3.24	0.955	0.446
P209	It is not a serious matter even if my personal information is collected by app developers.	3.53	0.879	3.44	0.960	0.693
P210	I have perfect control of all my private information stored on my mobile device(s).	3.27	0.839	3.12	1.038	0.504
P211	The security control on my mobile devices is enough to protect my own privacy.	2.91	1.071	3.12	0.946	0.401
P212	Shopping with my mobile device(s) is risky.	2.79	0.857	2.53	0.992	0.259
P213	Providing credit card information online via mobile device(s) is risky.	2.45	1.063	2.18	0.968	0.267
P214	Providing my HKID number and/or full name via mobile device(s) is risky.	2.24	1.001	2.15	1.019	0.701

		Foundation Round_Pre (N = 32, Missing = 1)		**Foundation Round _Post (N = 34, Missing = 1)**		**t-test**
		Mean	SD.	Mean	SD.	
P215	Providing my phone number via mobile device(s) is risky.	2.97	1.045	2.44	0.991	0.037
P216	Providing my friends' phone numbers via mobile device(s) is risky.	2.82	1.103	2.50	1.052	0.231
P217	Registering via mobile device(s) is risky.	2.81	0.859	2.44	0.894	0.091
P218	Shopping online for certain products is riskier on mobile phones than via non-mobile computers.	2.78	0.870	2.18	0.626	0.002
P219	I am familiar with the data protection act of Hong Kong.	3.12	0.927	2.76	0.890	0.113
P220	I have a good habit of protecting my privacy on my mobile device(s).	2.70	0.770	2.68	0.912	0.921
P221	Protecting my privacy on my mobile device(s) is important.	2.33	0.816	2.09	0.793	0.217
P222	I have good knowledge of protecting my own privacy on my mobile device(s).	2.82	0.917	2.50	0.788	0.132

Table 37: Comparison of Pre-teaching Survey and Post-teaching Survey Results of Part 3

		Foundation Round_Pre (N = 33)		**Foundation Round_Post (N = 34)**		**t-test**
		Mean	SD.	Mean	SD.	
P301	I feel that I can keep all my private information in a way that I feel is acceptable.	2.48	0.619	2.50	0.929	0.937
P302	I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	2.42	0.614	2.71	0.871	0.131
P303	I have checked and modified the privacy settings of my mobile device(s).	2.73	0.839	2.71	1.031	0.926
P304	If the information stored on my mobile devices looks too private, then I will delete it.	2.58	0.830	2.18	0.576	0.026
P305	I have perfect control of all my SNS account.	2.53	0.718	2.59	0.925	0.937
P306	I have checked and modified the privacy settings of my SNS account on my mobile device(s).	2.38	0.751	2.59	0.857	0.131
P307	If the information I posted on my SNS looks too private, then I will delete it.	2.22	0.792	2.15	0.712	0.926
P308	I do not share some things, because I worry about who has access to my SNS(s).	2.22	0.659	2.12	0.686	0.938
P309	I use real personal information to create my SNS account(s).	2.56	0.801	2.47	0.706	0.537
P310	I have the choice to accept followers on my SNS(s).	2.06	0.759	1.85	0.500	0.000
P311	My SNS entries are detailed.	2.91	0.928	2.85	1.105	0.001
P312	I have my own criteria for who I will follow on SNS.	2.22	0.608	2.21	0.687	0.953

		Foundation Round_Pre (N = 33)		**Foundation Round_Post (N = 34)**		**t-test**
		Mean	SD.	Mean	SD.	
P313	I comment on an SNS to ask others check out my SNS.	2.47	0.718	2.44	0.786	0.014
P314	I have blocked people who I do not know in the IM app(s) on my mobile device(s).	2.28	0.888	2.21	0.902	0.000
P315	I have the choice to accept an IM contact or not.	2.16	0.628	2.03	0.626	0.000

After the lesson, students changed their behaviour and attitude towards online security. Specifically, 32.4% of respondents suggested that they will read the terms and conditions clearly or ensure that they understand an app's access rights to the information on their mobile devices. By contrast, only 12.1% of students in the pre-teaching survey would do the same. Although more students considered ease of use as a top reason for downloading a new app before the lesson, 47.1% of them became more concerned about the privacy policy and 23.5% became concerned with the terms and conditions after the lesson. The percentage of students installing an anti-virus software also grew from 9.1% to 23.5%. In Part two of the survey, the differences were minor. The differences in the mean scores of the statements were all less than 1. Some statements had a significant increase in their scores. For example, the mean score increased from 2.41 to 2.71 in P302 ('I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly'); from 2.50 to 2.17 in E27 ('I do not mind my friends forwarding my IM text messages or photos to other people without consulting me'); and from 3.38 to 3.82 in P204 ('Information submitted through my mobile device(s) could be used in many ways, such as advertising, which I cannot foresee').

4.7.2 Cross-tabulation Results

To examine the changes in students' online privacy attitudes and online privacy management strategies before and after the foundation round teaching, cross-tabulation and Pearson's chi-squared statistics were conducted using SPSS to find out the relationships between the related question items. The Pearson's chi-squared tests essentially showed whether the results of the cross-tabulation are statistically significant.

This section shows the results of the cross-tabulation and chi-square tests of questions P220, P301, P302, P303 and P304, which may significantly affect students' online privacy attitudes and privacy management strategies before and after the lesson. The reason why these five questions were selected was because essential associations were found among them.

Table 38: Question Items on Online Privacy Attitude vs. Privacy Management Strategies

Question number	**Question**	**Variable**
P220	I have a good habit of protecting my privacy on my mobile device(s).	*Online Privacy Attitude (OPA)*
P301	I feel that I can keep all my private information in a way that I feel is acceptable.	
P302	I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	*Online Privacy Management Strategy (OPMS)*
P303	I have checked and modified the privacy settings of my mobile device(s).	
P304	If the information stored on my mobile devices looks too private, then I will delete it.	

Table 39 summarises the cross-tabulation and the chi-squared test results. It displays the changes in students' online privacy attitudes and online privacy management strategies before and after the foundation round of teaching. Before the foundation round of teaching, only P220 vs. P302 and P220 vs. P304 had no correlation and were not significant. After the Foundation Round of teaching, only P301 vs. P304 had no correlation and was not significant. These results reflected that the changes in OPA vs. OPMS improved. This pedagogical model was effective in developing students' online privacy management strategies. The succeeding teaching rounds should be modified according to this model.

The contradictory attitude and behaviour in P301 ('I feel that I can keep all my private information in a way I feel okay'.) and P304 ('If the information stored on my mobile devices looks too private, I will delete it'.) displays the phenomenon of the privacy paradox. It indicated that students' privacy attitude, that is, keeping private information, was unrelated to their privacy management strategy, that is, deleting private information their mobile devices. This phenomenon will be further discussed in the qualitative findings.

Table 39: Summary Table of the Chi-squared Statistics of the Foundation Round of Teaching

Pearson’s Chi-squared Test – Asymptotic Significant (2-sided) *with p-value 0.05*					
Online Privacy Attitude (OPA)	**vs**	**Online Privacy Management Strategies (OPMS)**	**Foundation Round Pre-survey**	**Foundation Round Post-survey**	**Change**
P220: **I have a good habit of protecting my privacy on my mobile device(s).**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.255 *(Not significant)*	0.000 *(Significant)*	✓
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.043 *(Significant)*	0.001 *(Significant)*	
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.210 *(Not significant)*	0.005 *(Significant)*	✓
P301: **I feel that I can keep all my private information in a way that I feel is acceptable.**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.001 *(Significant)*	0.001 *(Significant)*	
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.002 *(Significant)*	0.005 *(Significant)*	
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.001 *(Significant)*	0.222 *(Not significant)*	✓

4.8 Foundation Round of Post-teaching interview

Overall, students did not know have sufficient knowledge about privacy policy before the lesson. Moreover, they lacked knowledge related to the six DPPs.

> *'I did not know what privacy policy was before attending the class. I did not pay attention to this issue in my daily life. However, after the lesson, I am more aware that my personal data may be collected through cookies on some websites or via my mobile devices'. (Student A)*

After the lesson, they obtained knowledge about the DPPs and CPM theory. Interviewees could even immediately tell the first two stages of theory (i.e. ownership and control and rules). They could also apply the theory in their everyday life.

> *'The lesson gave me a deeper understanding on the issue, and I am going to apply these principles to my daily life. For example, to mitigate the possibility of personal data leakage, I will check the specified collection purpose and the retention period before providing my information to the third party'.*
>
> *(Student B)*

> *'CPM Theory not only makes me realise that I am the owner of my personal information but also guides me to develop boundaries to protect my information… I set more privacy boundaries on my*

Facebook, as I can't track who can see and steal my personal information for other purposes'.
(Student B)

Respondents found the case study useful, and it compelled them to change their behaviour.

'In the past, I frequently connect to public Wi-Fi for convenience or due to insufficient mobile data. After the lesson, I only surf on trusted websites with HTTP connection. When discussing personal or sensitive information, I will only talk to others through face-to-face communication rather than through phone/IM conversations, in which my records may be kept. In the past, I gave my credit card number and password to let my friends purchase online conveniently, but I will never do that again after the lesson.' (Student A)

'Before attending the lesson, I used to store my personal information like username and passwords (e.g. email and eCampus account) on my mobile devices for convenience. Also, I didn't pay attention to website security. ... (now) I will keep updating my device's passwords regularly and will not save these personal information'. (Student A)

Significant changes were also noted regarding the impact of the privacy protection intention according to the responses of both interviewees. There were also changes in the employment of protection measures. For example, before the case study, students used fingerprint technology to log in. Now, they used anti-glancing screen protector on their mobile phone in addition to fingerprint technology to prevent others from reading their passwords.

> *'The lesson has a positive impact on me in terms of protecting my privacy. Whenever someone wants to access my personal information stored on my mobile apps, they must enter a password first'.*
>
> *(Student A)*

> *'After the class, I started paying more attention to reading the terms and conditions and stopped storing unnecessary information on my mobile phone. I will cancel the download when it asks permission for irrelevant and inessential information and access to my PC to browse the contents. These companies cannot collect my information for other purposes….I won't fill in my actual name and birthday when creating an account'.*
>
> *(Student B)*

Moreover, students mentioned that they would protect their account information when using some mobile apps.

> *'I did not store many private information on my mobile phone, such as the medical records of Mr. Lau in the case video. Also, I did not shop online. After the lesson, I realised that I was doing well in storing or providing private information to others, such as mobile app developers'. (Student A)*

> *'After the class, I believed that I started storing my personal information in my mobile phone properly. I think that my most private information was the bank account information, but that information was already given to the bank previously, so this should be no problem at all'. (Student B)*

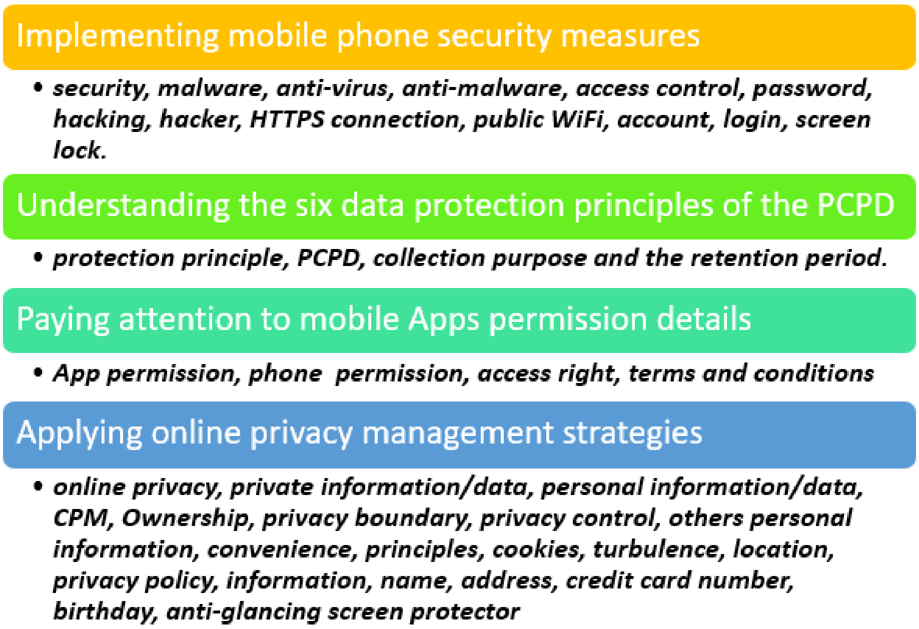
Students' responses echoed with the results shown in Table 7, which indicated that only 36% and 73% of students used their mobile devices for online banking and finance and online shopping, respectively. Hence, although students were satisfied with their online privacy management strategies, they did not really protect their mobile devices sufficiently.

As a conclusion, students found the privacy lesson very useful. Student A and B rated its usefulness at 4.5 and 5, respectively, out of 5. The lesson made them think twice before directly providing their personal information to others upon being requested.

Qualitative results of the Foundation Round Post-teaching interview

Using NVivo, the post-teaching interviews of students were coded into positive, negative and other themes. Four themes were obtained, and the percentage of students contributing to each theme was calculated. Table 40 shows the results of the Foundation Round's post-teaching interview.

Figure 21: Four Main Themes from the Post-teaching Interviews



Implementing mobile phone security measures

- *security, malware, anti-virus, anti-malware, access control, password, hacking, hacker, HTTPS connection, public WiFi, account, login, screen lock.*

Understanding the six data protection principles of the PCPD

- *protection principle, PCPD, collection purpose and the retention period.*

Paying attention to mobile Apps permission details

- *App permission, phone permission, access right, terms and conditions*

Applying online privacy management strategies

- *online privacy, private information/data, personal information/data, CPM, Ownership, privacy boundary, privacy control, others personal information, convenience, principles, cookies, turbulence, location, privacy policy, information, name, address, credit card number, birthday, anti-glancing screen protector*

Figure 22: Percentage of Students Contributing to Each Theme

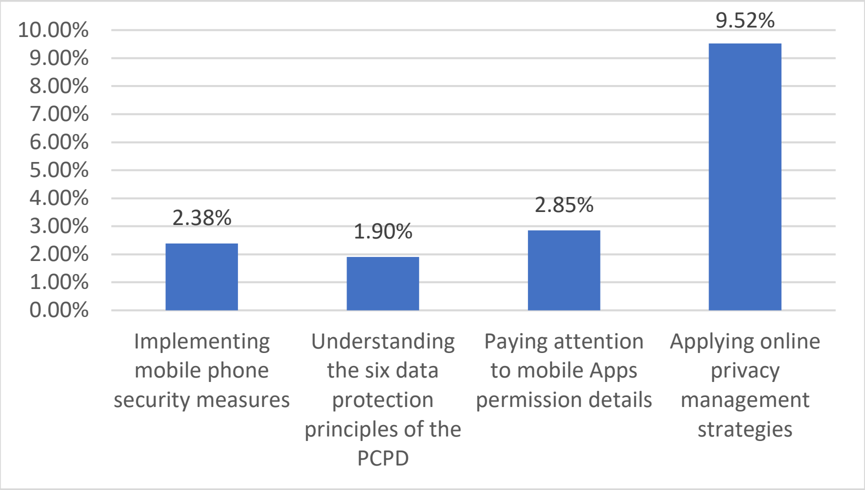


Table 40: Qualitative Results of the Foundation Round Teaching

Theme	**Interpretation**
Implementing mobile phone security measures (2.38%)	Students paid attention to their mobile phone security so as to protect the private information stored on their mobile phones.
Understanding the six data protection principles of the PCPD (1.90%)	Students initially did not know the six data protection principles of the PCPD. They learned about these principles from the lesson. However, they could not state the details of the principles.
Paying attention on mobile app permission details (2.85%)	Students were not aware of the importance of reading the mobile app permission details or terms and conditions when or after installing apps. They learned the importance of which after the lesson. Later on, they learned to read the app permission details before downloading an app.
Applying online privacy management strategies (9.52%)	Students did not apply online privacy management strategies in a systematic way. They found that CPM was useful for protecting their personal information. As a result, they can apply CPM theory in their daily life.

4.9 Teachers' reflections

After teaching the first class, teachers had the following observations and reflections:

1. The case teaching method could engage students during the lesson effectively, as students paid more attention in this method than in the direct teaching section.
2. Students actively discussed with their classmates when they were working on the assignments.
3. Students jotted down notes when they were watching the case studies video.
4. Students tackled the assignment questions well especially those related to CPM theory.
5. Some students responded that they had watched the online video during their secondary schooling.
6. The case background was quite old.
7. The initial responses of students showed that they enjoyed the lessons. They found the case studies interesting, not monotonous and relevant to their daily life.

4.10 Key Findings of the First Round of Teaching

Students from the first teaching round wear Year 1 Social Science majors. Moreover, 81% of students had not taken DSE ICT. They mainly learned online privacy knowledge from their primary and/or secondary education.

Pre-teaching Survey

- The pre-teaching survey revealed that most students learned about online privacy during their primary and secondary education.
- As students often use their mobile devices for social networking, contact information was the most common information stored in their mobile devices.
- However, their alertness towards data privacy was low, and not much security measures have been utilised for their devices. Therefore, cybersecurity threat was an issue for them.

Pre- vs. Post-teaching Survey

- After the teaching, students changed their behaviour and attitude towards online security.
  - Approximately 32.4% of respondents suggested that they will read the terms and conditions clearly or ensure that they understand apps' access rights to the information on their mobile devices before installing an app. In the pre-teaching survey, only 12.1% would do the same practice.
  - Before the lesson, more students would consider convenience in deciding to download an app. After the lesson, 47.1% of them became concerned about the privacy policy, with 23.5% specifically concerned about the terms and

conditions.

- The percentage of students installing an anti-virus software also grew from 9.1% to 23.5%.
- In Part 2 of the survey, the differences were relatively minor. The differences in the mean scores of the statements were all less than 1.
- Some statements had an significant change in their mean scores such as an increase from 2.41 to 2.71 in P302 ('I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly'.); a decrease from 2.50 to 2.17 in E27 ('I do not mind my friends forwarding my IM text messages or photos to other people without consulting me'.); and an increase from 3.38 to 3.82 in P204 ('Information submitted through my mobile device(s) could be used in many ways, such as advertising, which I cannot foresee'.).

Post-teaching interview

- Respondents found the case study useful, and it changed their behaviour. Although the online privacy items mentioned in the online video were useful, the setting of the video was slightly old.
- Significant changes were observed according to the responses of both interviewees about the impact of the privacy protection intention.
- There were also changes in the employment of protection measures. For example, before the case study, students used fingerprint technology to log in. Now, they spent extra effort and used an anti-glancing screen protector on their mobile phone to prevent others from reading their passwords.

- Students now think twice before directly providing their personal information to others upon being requested.

4.11 Summary of the Foundation Round

Accomplishments in this round

- FR students' privacy concern (OPA) increased (Part 2: +3%; +9%) with better boundary rule and control (OPMS) in using their mobile devices (Part 3: +9%; 0%).
- After the FR, among six sets of OPA and OPMS relationships, only P301 vs. P304 had no correlation and were not significant. These results reflected that the changes on OPA vs. OPMS were improved.
- As reported in the post-survey, assignment and post-teaching interview, the overall findings of this round showed positive impacts on Foundation Round students.
- FR students were attentive according to the teacher's observation.
- FR students' responses shown in the post-teaching interview had positive impression. They rated the overall lesson with 4.5/5.

Problems that need to be addressed

- The video was old but not outdated.
- The six PCPD protection principles should be highlighted in the coming rounds of teaching.

Enhancement in the next round

- As the case studies in the video was not new for FR students, the teacher should choose current news that close to daily life in the next teaching round.

Initial Responses to Research Questions

RQ 1: What are HEI students' online privacy attitudes towards using mobile devices?

Initial responses: More students in the FR were 'somewhat concerned' (42%) and 'quite concerned' (27%). Moreover, no student was 'extremely concerned'. These findings implied that FR students did not have major concerns on their own online privacy before the lesson.

RQ 2: How effective is using CPM theory in improving HEI students' online privacy management strategies for their mobile devices?

Initial responses: FR students became more concerned with their privacy (Part 2: +3%; +9%) with better boundary rule and control, which is a form of privacy management strategy, in using their mobile devices (Part 3: +9%; 0%). This result reflected that the three stages of CPM theory were useful and effective in improving students' privacy concern and privacy management strategies. In the cross-tabulation result, one set of OPA and OPMA exhibited the phenomenon of the privacy paradox. This phenomenon could be explained by the post-teaching interview result: students responded that they did not use their mobile phone to store their private information, such as bank accounts or online shopping account information. Although they know that they should protect their private information, they did not protect their private information stored on their mobile phones seriously.

RQ 3: What types of pedagogical models can effectively improve HEI students' online privacy management strategies for mobile devices?

Initial responses: These results reflected that the changes in OPA vs. OPMS were improved. This pedagogical model was effective in developing students' online privacy management strategies. Therefore, succeeding teaching rounds should be modified on the basis of this model.

Chapter 5: Results and Findings – Enhancement Rounds of Teaching

5.1 Introduction

The purpose of this chapter is to present and analyse the data collected from the three enhancement rounds of teaching. The approach is similar to that of the foundation round, starting from the pre-teaching survey, teaching, assignments and the comparison of the results of the pre- and post-teaching survey of the remaining three groups. This chapter reports the pedagogical model, teaching plan and lesson details of the remaining lessons. Finally, key findings of all remaining rounds of teaching are presented.

5.2 Demographic Data of the First to Third Enhancement Rounds of Teaching

This section shows the demographic data of students from the three target classes who participated in this study. The first, second and third enhancement rounds of target classes had 30, 33 and 28 students, respectively. Table 41 shows their age, gender, year of study and study major.

Table 41: Demographic Data of Target Class Students from the First, Second and Third Enhancement Rounds (in Percentage)

	First Enhancement Round Teaching	**Second Enhancement Round Teaching**	**Third Enhancement Round Teaching**
Number of participants	30	33	28
Age			
Age	**20.87**	**21.6**	**19.7**
17	--	--	7.1%
18	10.0%	3.3%	32.1%
19	10.0%	50.0%	32.1%
20	16.7%	36.7%	10.7%
21	30.0%	3.3%	10.7%
22	20.0%	6.7%	7.1%
23 or above	13.4%	--	--
Gender			
Female	53.3%	40.0%	71.4%
Male	46.7%	53.3%	28.6%
Missing	--	6.7%	
Study Year			
Year of Study	**2.8**	**3.97**	**1.46**
1	26.7%	--	78.6%
2	6.7%	--	--
3	26.7%	3.3%	17.9%
4	40.0%	96.7%	3.6%
Study Major			
Social Science	30.0%	--	--
Language Studies	3.3%	--	--
Business	56.7%	70%	21.5%
Science	10.0%	30%	3.6%
Journalism and Communication	--	--	60.7%
Others	--	--	3.6%
Missing	--	--	10.7%

The demographic distribution of students varied across the three enhancement rounds. In the first enhancement round, the average age of students in this class was 20.87. Students aged 21 comprised the biggest proportion (30%), followed by students aged 22 (20%). The gender percentage of female and male students was 53.3% and 46.7%, respectively. Moreover, 40% of students from the second target class were Year 4 students, and 56.7% of them studied Business.

In the second enhancement round, the average age of students from the third target class was 21.6. Students aged 19 comprised the biggest proportion (50%), followed by students aged 20 (36.7%). The gender percentage of female and male students was 40% and 53.3%, respectively, and 6.7% of them did not provide their gender. The majority (96.7%) of students from the second target class students were Year 4 students, and 70% of them studied Business.

In the third enhancement round, the average age of students from this class was 19.7. Students aged 18 and 19 comprised 64.2% of the class. The gender percentage of female and male students was 71.4% and 28.6%, respectively. Approximately 78.6% of students from the fourth target class students were Year 1 students, and 60.7% of students studied Journalism and Communication.

The four iterations had much differences in the year of study. Foundation round students were mainly Year 1 students, whereas students in the enhancement round were evenly distributed over 4 years, with 40% on Year 4. Enhancement round 2 had no Year 1 and Year 2 students. Enhancement round 3 had a similar setting as the Foundation Round.
The third enhancement round students had much differences in study major. The Foundation round mainly consisted of Social Science students, whereas enhancement round students were mainly Year 2 Business and Science students. In enhancement round 3, a significant proportion of students were Journalism and Communication majors, which was not found in the other iterations.

5.3 Pre-teaching Survey Results of the Enhancement Rounds of Teaching

The background information of students was mainly obtained by using a quantitative method, that is, the pre-teaching survey. To understand students' background and their prior knowledge of online privacy, the pre-teaching survey questionnaires asked students four questions: A08 ('Did you take DSE ICT'?), X01 ('Have your mobile device(s) been hacked by others'?), X02 ('Have your personal data stored on your mobile device(s) been misused by others'?) and J01 ('Where did you learn the knowledge or skills for protecting your online privacy'?). The results are shown in the following tables.

Table 42: Percentage of Participants in the Remaining Rounds who had taken DSE ICT (A08)

		ENHANCEMENT ROUND 1	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Valid	Yes	6.7%	23.3%	3.6%
	No	93.3%	76.7%	96.4%

The feedback from question A08 showed lack of formal ICT training among enhancement rounds participants. In enhancement round 1 and enhancement round 3, less than 10% of participants had taken DSE ICT, whereas 23.3% had taken DSE ICT in enhancement round 2.

Table 43: Participants whose Mobile Device(s) have been Hacked (X01)

		ENHANCEMENT ROUND 1	ENHANCEMENT ROUND 2	ENHANCEMENT ROUND 3
Valid	Yes	10.0%	10.0%	3.6%
	No	90.0%	90.0%	96.4%

Question X01 aims to understand if participants have experienced their mobile device being hacked. More than 90% of them have never been hacked, which is likely to affect their perception towards their cybersecurity needs.

Table 44: Participants whose Mobile Data have been Misused (X02)

		ENHANCEMENT ROUND 1	ENHANCEMENT ROUND 2	ENHANCEMENT ROUND 3
Valid	Yes	23.3%	6.7%	10.7%
	No	76.7%	93.3%	89.3%

Compared with students whose mobile devices have been hacked, more participants revealed that their mobile data have been misused previously. The highest percentage was found in enhancement round 1 participants, with a percentage of 23.3%, whereas enhancement round 2 had the lowest percentage of participants (6.7%).

Table 45: Source of Knowledge on Protecting Online Privacy (J01)

Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Primary education	40%	40%	57%
Secondary education	73%	60%	68%
Higher education	60%	57%	50%
Media such as newspapers or TV	50%	70%	46%
Social networking sites	47%	43%	50%
Parents	23%	13%	46%
Friends	37%	47%	29%
Others	3%	0%	0%

The answers to Question J01 for these three remaining rounds were similar to that in the foundation round. Most participants learned online privacy knowledge from their secondary education with the percentages 73%, 60% and 68% for the three remaining rounds, respectively.

5.3.1 Part 1: Use of Mobile devices

Part 1 included question P101 (‘What is your most common purpose for using your mobile devices’?). Table 6 shows the results.

Table 46: Students’ Most Common Purpose for using their Mobile Devices

Item	ENHANCEMENT ROUND 1	ENHANCEMENT ROUND 2	ENHANCEMENT ROUND 3
Using social networks	97%	90%	93%
Instant messaging with friends	83%	83%	89%
Browsing online forums	30%	60%	57%
Reading news	30%	47%	50%
Looking for information	57%	73%	64%
Online shopping	53%	57%	71%
Online banking and finance	23%	63%	57%
Watching videos	70%	63%	68%
Listening to music	57%	67%	71%
Reading comics	10%	20%	32%
Reading e-books	30%	17%	29%
Making phone calls	50%	53%	57%
Playing games	63%	53%	64%
Listening to radio	3%	10%	14%
Sending or receiving email	53%	63%	54%
Taking photos	53%	70%	64%
Using the calendar and notes	40%	57%	57%
Editing documents	37%	23%	39%
Web surfing	43%	43%	54%
Others	0%	0%	0%

Most students commonly used their mobile device for social networking. Approximately 97%, 90% and 93% of students in the three enhancement rounds, respectively, primarily used their mobile devices for social networking. In addition, 83%, 83% and 89% of them used their mobile devices for instant messaging with friends, respectively.

Question P103 asked students: 'Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access rights to the information on your mobile devices'? The result for enhancement round 1 and enhancement round 2 were similar; 60% and 63.3% of students answered 'no'. However, the answers in enhancement round 3 showed that 46.4% of students would read the terms and conditions before they decide to install a mobile app. In Enhancement Round 1, 30% of students would read some, but not all, of the terms and conditions during app installation.

Table 47: Proportion of Students who Read the Terms and Conditions or Understand an App's Access Rights prior to Installation

Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Yes	10.0%	16.7%	46.4%
No	60.0%	63.3%	28.6%
I do so for some of the apps, but not for all of them	30.0%	20.0%	25.0%
Total	100.0%	100.0%	100.0%

Question P104 asked participants: 'What will you consider when you install an App'? Table 48 displays that students considered mainly the function and the cost (free or paid) of an app before installing it. In enhancement round 1, only 30% of students would consider popularity when installing an app. Besides, the terms and conditions and the privacy policy were among the least concern factors. In enhancement round 2, only 3% of students would consider the terms and conditions when installing an app. These findings showed that students did not understand the importance of protecting their online privacy while using their mobile devices. Accordingly, the teacher had considered and addressed these two issues when teaching this class.

Table 48: Students' Considerations in Downloading an App

Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Popularity	30%	67%	71%
User reviews	37%	37%	57%
Functions	83%	73%	64%
Degree of needs	67%	77%	50%
Convenience	53%	47%	32%
Quick to download or not	7%	10%	14%
Free or paid	73%	73%	64%
Privacy policy	23%	17%	21%
Terms and conditions	10%	3%	7%
Others	0%	7%	0%

Table 49 shows that screen lock was the most common protective action being taken by students. Setting up the auto screen lock and using screen lock were the top two protective actions claimed by respondents in the three enhancement rounds. Compared with students in the foundation round, more students in the enhancement round had their mobile devices installed with anti-virus and anti-theft software. Enhancement round 1 had the highest proportion of students with anti-virus software installed in their phones.

Table 49: Protective Actions Taken by Students to Secure their Mobile Privacy

Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Set up auto screen lock	67%	77%	82%
Set up screen lock	50%	70%	86%
Install anti-virus software	23%	10%	18%
Install anti-theft software	13%	13%	18%
Others	0%	7%	7%

The answers to questions P110, P111 and P112, as shown in Table 50, reflected that 63.3%, 73.3% and 71.4% of students from the three enhancement rounds respectively knew that their contact lists were being uploaded to the SNS servers, whereas 70%, 80% and 71.4% of students from the three enhancement rounds, respectively, knew that their geo-location was being recorded in the pictures that they captured. Moreover, 63.3%, 63.3% and 64.3% of students from the three enhancement rounds, respectively, knew that some apps would take actions that they were not informed of beforehand.

Table 50: Percentage of Students who were Aware of Apps' Actions on Mobile Devices

	Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
		Yes	**Yes**	**Yes**
P110:	Do you know that your contact lists may be uploaded to the central servers of the social networking apps that you are using?	63.3%	73.3%	71.4%
P111:	Do you know that some apps will take actions that they have not mentioned they would?	63.3%	63.3%	64.3%
P112:	Do you know that, when you take a picture with your mobile devices, your geo-location may be recorded in the photo?	70.0%	80.0%	71.4%

Questions P113 and P114 explored students' perceptions of the importance of convenience and privacy. The results indicated that convenience and privacy had the same degree of importance to students. The mean value of Questions P113 and P114 were the highest in the enhancement round 2 group, at 1.90 and 1.70, respectively. In general, all students in the three groups believed that convenience and privacy were important issues.

Table 51: Students' Perceptions on Convenience and Privacy

	Item	**ENHANCEMENT ROUND 1**		**ENHANCEMENT ROUND 2**		**ENHANCEMENT ROUND 3**	
		Mean*	**(S.D.)**	**Mean***	**(S.D.)**	**Mean***	**(S.D.)**
P113:	Convenience is important to you.	3.23	(0.728)	3.10	(0.607)	2.74	(1.023)
P114:	Privacy is important to you.	2.93	(0.828)	3.30	(0.651)	2.70	(0.953)

**Note: 5 = very important; 4 = important; 3 = moderately important; 2 = slightly important; 1 = not important*

Table 52: Types of the Personal Information of Friends, Classmates and Family Members that are Stored in Students' Mobile Devices

Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Friends' contact information	90%	83%	79%
Entrance code of the building where you and your family members live	13%	20%	25%
ATM password(s)	10%	10%	21%
Online account number and password	17%	30%	29%
Email addresses	47%	60%	43%
Email account passwords	13%	20%	21%
Personal and sensitive photos	37%	60%	36%
Haven't stored any personal information of others	0%	0%	4%
Others	0%	0%	0%

Table 52 reveals that 90%, 83% and 79% of students from the three enhancement rounds stored the contact lists of their friends, classmates and family members on their mobile devices. Email addresses and personal and sensitive photos were the second and third most common personal information, respectively, saved in their phones. Enhancement round 2 group had the highest proportion of 60%.

Moreover, students from the last three rounds stored someone's online account IDs and passwords (17%, 30% and 29%, respectively), email account passwords (13%, 20% and 21%, respectively), entrance code of buildings (13%, 20% and 25%, respectively) and ATM passwords (10%, 10% and 21%, respectively) on their mobile devices. Although these percentages were not too high, online account IDs and passwords, email account passwords, entrance code of buildings and ATM passwords were private information that should not be shared with anyone under normal circumstances.

Table 53: Types of the Personal Information Stored in Students' Mobile Devices

Item	**ENHANCEMENT ROUND 1**	**ENHANCEMENT ROUND 2**	**ENHANCEMENT ROUND 3**
Contact information	80%	90%	75%
Entrance code of the building where you and your family members live	13%	33%	21%
ATM password(s)	20%	10%	21%
Online account ID and password	23%	37%	39%
Email addresses	83%	80%	61%
Email account passwords	47%	33%	46%
Personal and sensitive photos	57%	70%	43%
Others	3%	3%	11%
Haven't stored any personal information	0%	0%	4%

The answers to question P116 explored the types of personal information that students stored on their mobile devices. Contact information and email address were the most common personal information saved on their mobile devices. Similar to the previous result, 70% of enhancement round 2 students save personal and sensitive photos of themselves in their own mobile devices, whereas only 57% and 43% of students from enhancement round 1 and enhancement round 3, respectively, do the same.

The result from the last three rounds was contradictory again. Although students did not do much to protect their mobile devices, they considered their privacy important. Therefore, the teacher should take note of this inconsistency and address it when teaching these classes.

5.3.2 Part 2: Attitudes towards Data Privacy

Table 54 shows students' attitudes towards data privacy on their mobile devices. Questions P201, P202, P203 and P204 were concerned with the possibility of students' information stored on their mobile devices being misused by others. The mean five-point Likert scale scores of these questions were all over 3, ranging from 3.43 to 3.87, where 1 represents 'not concerned at all' and 5 represents 'absolutely concerned'. This result reflected that respondents were slightly concerned about their information stored in their mobile devices being misused by others.

Table 54: Students' Attitudes towards the Information in their Mobile Devices (remaining rounds)

	Item	**ENHANCEMENT ROUND 1**		**ENHANCEMENT ROUND 2**		**ENHANCEMENT ROUND 3**	
		Mean[#]	**S.D.**	**Mean**[#]	**S.D.**	**Mean**[#]	**S.D.**
P201:	The information I submit through my mobile device(s) could be misused.	3.43	0.679	3.50	0.731	3.18	0.612
P202:	People can get hold of my private information on my mobile device(s).	3.70	0.877	3.97	0.928	3.30	0.823
P203:	Others might use my mobile device(s) to submit information.	3.57	0.898	3.63	0.890	3.32	0.905
P204:	Information submitted through my mobile device(s) could be used in many ways, such as advertising, that I cannot foresee.	3.87	0.629	3.83	0.791	3.19	0.834

[#] *1 = not concerned at all; 2 = a little concerned; 3 = concerned; 4 = very concerned; 5 = absolutely concerned*

The answers to Questions P206, P207, P208 and P209 displayed students' perception of app developers. Table 55 shows that the mean five-point Likert scale scores of these questions ranged from 2.90 to 3.17, where 1 represents 'strongly agree' and 5 represents 'strongly disagree'. Therefore, students slightly disagreed that app developers were trustworthy and kept their promises and commitments.

Questions P212 to P217 explored students' attitude towards providing information via their mobile devices. The mean five-point Likert scale scores of these questions were all below 3, ranging from 1.63 to 2.85, where 1 represents 'strongly agree' and 5 represents 'strongly disagree'. These scores indicated that students agreed that providing private information such as HKID number, full name and phone numbers was risky. The mean five-point Likert scale score of Question P219 was 1.77, which revealed that respondents were not familiar with the data protection act of Hong Kong. Regarding respondents' practice and knowledge of protecting their privacy on their mobile devices, the last three rounds' mean five-point Likert scale scores of Questions P220 and P222 were 2.32, 1.93 and 2.21 and 2.5, 2.03 and 2.32, respectively. The scores showed that respondents agreed that they had a good habit and good knowledge of the issue. Finally, Table 55 lists the mean five-point scale score result of Question P221, which was 2.71, regarding the importance of protecting respondents' privacy on their mobile devices. This finding indicated that students considered protecting the privacy of their mobile devices important.

Table 55: Students' Perceptions Towards the Importance of Protecting the Privacy in their Mobile Phones (Remaining Rounds)

Item		ENHANCEMENT ROUND 1		ENHANCEMENT ROUND 2		ENHANCEMENT ROUND 3	
		Mean*	S.D.	Mean*	S.D.	Mean*	S.D.
P205	'I live an upright life, and I have nothing to hide. Why should I care about my mobile privacy?'	1.29	0.887	0.9	0.845	1.36	0.870
P206	App developers are trustworthy.	1.68	0.592	1.5	0.861	2.07	0.813
P207	App developers keep their promises and commitments.	1.74	0.845	1.7	0.837	2.14	0.756
P208	App developers keep their customers' best interests in mind.	1.76	0.928	1.53	0.860	2.04	0.693
P209	It is not a serious matter even if my personal information is collected by app developers.	1.56	0.837	1.27	0.691	2.07	0.813
P210	I have perfect control of all my private information stored on my mobile device(s).	1.88	0.747	1.63	0.718	1.75	0.701
P211	The security control on my mobile devices is enough to protect my own privacy.	1.88	0.828	1.77	0.935	2.11	0.737
P212	Shopping with my mobile device(s) is risky.	2.47	0.868	1.93	0.961	1.86	0.591
P213	Providing credit card information online via mobile device(s) is risky.	2.82	0.915	2.20	1.064	2.25	0.887
P214	Providing my HKID number and/or full name via mobile device(s) is risky.	2.85	1.028	2.50	0.974	2.43	0.879
P215	Providing my phone number via mobile device(s) is risky.	2.56	0.817	1.63	0.890	1.96	0.881
P216	Providing my friends' phone numbers via mobile device(s) is risky.	2.50	0.860	1.83	0.950	2.18	0.772
P217	Registering via mobile device(s) is risky.	2.56	0.865	1.93	0.828	2.14	0.891

Item		ENHANCEMENT ROUND 1		ENHANCEMENT ROUND 2		ENHANCEMENT ROUND 3	
		Mean*	S.D.	Mean*	S.D.	Mean*	S.D.
P218	Shopping online for certain products is riskier on mobile phones than via non-mobile computers.	2.82	0.850	2.10	0.960	2.11	0.832
P219	I am familiar with the data protection act of Hong Kong.	1.44	0.759	1.57	0.858	2.29	0.763
P220	I have a good habit of protecting my privacy on my mobile device(s).	2.32	0.845	1.93	0.785	2.21	0.738
P221	Protecting my privacy on my mobile device(s) is important.	2.91	0.639	2.57	0.898	2.64	0.678
P222	I have good knowledge of protecting my own privacy on my mobile device(s).	2.50	0.868	2.03	0.809	2.32	0.723

**5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

5.3.3 Part 3: Boundary Rules and Control of Private Information on Mobile Devices

As shown in Table 56, the mean five-point Likert scale scores of Questions P301, P302, P303 and P304 of the last three rounds were all below 3, where 1 represents ‘strongly agree’ and 5 represents ‘strongly disagree’, ranging from 2.00 to 2.68. These findings reflected that participants found themselves well managing and keeping their private information stored on their mobile devices. The mean five-point Likert scale scores of Questions P302, P303 and P304 in the last three rounds were all below 3. These results showed that participants delete and/or updated apps on their mobile devices regularly, check and adjust the privacy settings of their mobile devices and delete the information stored on mobile devices that were too private.

Table 56: Students’ Boundary Rules and Control of their Private Information on their Mobile Devices

	Item	**ENHANCEMENT ROUND 1**		**ENHANCEMENT ROUND 2**		**ENHANCEMENT ROUND 3**	
		Mean*	**S. D.**	**Mean***	**S. D.**	**Mean***	**S. D.**
P301	I feel that I can keep all my private information in a way that I feel is acceptable.	2.37	0.765	2.43	0.728	2.57	0.634
P302	I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	2.37	0.890	2.60	0.770	2.57	0.634
P303	I have checked and modified the privacy settings of my mobile device(s).	2.13	0.937	2.00	0.910	2.46	0.693
P304	If the information stored on my mobile devices looks too private, then I will delete it.	2.63	0.890	2.50	0.777	2.68	0.819

*5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree

Table 57 explores participants' boundary rules and control of their private information stored on their SNS. Under the five-point Likert point scale, Table 57 lists the mean scores of the responses in the three enhancement rounds, which were mostly below 3, ranging from 2.00 to 3.00. These scores suggest that participants agreed that they had sufficient or proper boundary rules and control of their SNS information and settings on their SNS accounts. These findings were consistent with the results in Part 2.

Table 57: Students' Boundary Rules and Control of their Private Information on their SNS Accounts

	Item	**ENHANCEMENT ROUND 1**		**ENHANCEMENT ROUND 2**		**ENHANCEMEN T ROUND 3**	
		Mean*	**S.D.**	**Mean***	**S.D.**	**Mean***	**S.D.**
P305	I have perfect control of all my SNS accounts.	2.33	0.711	2.69	0.660	2.38	0.571
P306	I have checked and modified the privacy settings of my SNS account on my mobile device(s).	2.47	0.900	2.43	1.040	2.52	0.714
P307	If the information I posted on my SNS looks too private, then I will delete it.	2.97	0.615	2.97	0.765	2.40	0.707
P308	I do not share some things, because I worry about who has access to my SNS(s).	3.03	0.669	3.00	0.587	2.36	0.907
P309	I use real personal information to create my SNS account(s).	2.43	0.774	2.37	0.890	2.40	0.866
P310	I have the choice to accept followers on my SNS(s).	3.13	0.571	3.27	0.691	2.64	0.952
P311	My SNS entries are detailed.	2.00	0.743	2.00	0.871	3.00	0.834
P312	I have my own criteria for who I will follow on SNS.	2.83	0.592	2.83	0.648	2.72	0.891
P313	I comment on an SNS to ask them to check out my SNS.	2.33	0.922	2.30	0.952	2.88	0.881

**5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

This part asked respondents about their boundary rules and control of their private information on IM accounts. On the basis of the five-point Likert scale, where 1 represents ‘strongly disagree’ and 5 represents ‘strongly agree’, the mean scores of responses to Questions P314 and P315 in the last three rounds were all below 3. These findings were also consistent with the results in Part 2.

Table 58: Students’ Boundary Rules and Control of their Private Information on their IM Accounts

	Item	**ENHANCEMENT ROUND 1**		**ENHANCEMENT ROUND 2**		**ENHANCEMENT ROUND 3**	
		Mean*	**S.D.**	**Mean***	**S.D.**	**Mean***	**S.D.**
P314	I block people who I do not know in the IM app(s) on my mobile device(s).	2.83	0.913	2.63	0.928	2.65	0.936
P315	I have the choice to accept an IM contact.	2.77	0.971	3.03	0.718	2.85	0.784

**5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

Question P316 asked respondents about forwarding someone's text messages or photos to other people without seeking their consents beforehand. According to the five-point Likert scale, where 1 represents 'always' and 5 represents 'never', the mean scores of the responses in the last three rounds were 3.07 (S.D. 0.828), 2.63 (S.D. 0.850) and 2.92 (S.D. 0.845), respectively. These results reflected that respondents sometimes forward someone's text messages and photos to others.

Table 59: Respondents' Attitudes towards Forwarding Someone's Messages or Photos to Other People without Prior Consent

	Item	ENHANCEMENT ROUND 1		ENHANCEMENT ROUND 2		ENHANCEMENT ROUND 3	
		Mean*	S.D.	Mean*	S.D.	Mean*	S.D.
P316	Have you ever forwarded someone's text messages or photos in your instant messaging (IM) app, such as WhatsApp, Snapchat and WeChat, to other people without getting his or her consent beforehand?	3.07	0.828	2.63	0.850	2.92	0.845

**1 = always; 2 = often; 3 = sometimes; 4 = rarely; 5 = never*

The majority of students have learned about online privacy from their primary education and secondary education. They heavily used their mobile devices primarily for social networking. This finding was consistent with the fact that contact information was the most common information that is stored in their mobile devices, which led to cybersecurity threats. Their attitude towards data privacy was fair, and not much security measures had been put in place.

5.3.4 Key findings from the Pre-teaching survey

Table 60 presents the key findings from the enhancement rounds' pre-teaching survey.

Table 60: Key Findings from the Foundation Round Pre-teaching Survey

Part 1: Use of Mobile Devices
1a. Question P101 was designed to explore students' purposes for using their mobile devices. Most students commonly used their mobile device for social networking, with a valid percentage of 97%, 90% and 93% across the three remaining rounds, followed by instant messaging with friends with a valid percentage of 83%, 83% and 89%, respectively.
1b. Question P103 asked 'whether students read the terms and conditions clearly before downloading an app'. The result for enhancement round 1 and enhancement round 2 were similar, with 60% and 63.3% of students answering 'no'. However, the answers in enhancement round 3 showed that 46.4% of students would read the terms and conditions before they decide to install an App.
1c. Question P104 asked participants: 'What will you consider when you install an App'? The functions of an app scored the highest percentage in all the remaining three rounds. Terms and conditions and the privacy policy were among the least concern factors. In enhancement round 2, only 3% of students would consider the terms and conditions when installing an app. These findings showed that students did not understand the importance of protecting their online privacy while using their mobile devices.
1d. Setting up the auto screen lock and using screen lock were the top two protective actions claimed by respondents in all the three remaining rounds. Enhancement round 1 had the highest proportion of students who have anti-virus software installed.
1e. The answers to questions P110, P111 and P112 reflected that 63.3%, 73.3% and 71.4% of students from the last three rounds, respectively, knew that their contact lists were being uploaded to SNS servers; whereas 70%, 80% and 71.4% of students from the last three rounds, respectively, knew that their geo-location was being recorded in the pictures that they captured. Moreover, 63.3%, 63.3% and

64.3% of students from the last three rounds, respectively, knew that some apps would take actions that they were not informed of beforehand.

1f. Questions P113 and P114 explored students' perceptions of the importance of convenience and privacy. The results indicated that convenience and privacy had the same degree of importance to students. The mean value of Questions P113 and P114 were the highest in the enhancement round 2 group, with 1.90 and 1.70, respectively. In general, all students in the three groups believed that convenience and privacy were important issues.

1g. The results of P115 revealed that 90%, 83% and 79% of students from the last three rounds stored the contact lists of their friends, classmates and family members on their mobile devices. Email addresses and personal and sensitive photos were the second and third, respectively, popular personal information saved in their phones. Enhancement round 2 group had the highest proportion of 60%.

1h. Students from the last three rounds stored: someone's online account IDs and passwords (17%, 30% and 29%, respectively), email account passwords (13%, 20% and 21%, respectively), entrance code of buildings (13%, 20% and 25%, respectively) and ATM passwords (10%, 10% and 21%, respectively) on their mobile devices. Although these percentages were not too high, online account IDs and passwords, email account passwords, entrance code of buildings and ATM passwords were sensitive private information that should not be shared to others under normal circumstances.

1i. The answers to Question P116 shows the types of personal information that students stored on their mobile devices. Contact information and email address were the most popular personal information saved on their mobile devices. Similar to the previous result, 70% of students in enhancement round 2 group save personal and sensitive photos of themselves in their own mobile devices, whereas only 57% and 43% of students in enhancement round 1 and enhancement round 3 groups, respectively, do the same.

Part 2: Attitudes Towards Data Privacy

2a. Questions P201, P202, P203 and P204 were concerned with the possibility of students' information stored on their mobile devices being misused by others. The mean five-point Likert scale scores of these questions were all over 3, ranging from 3.43 to 3.87. The result reflected that respondents were slightly concerned about their information stored in their mobile devices being misused by others.

2b. The answers to Questions P206, P207, P208 and P209 displayed students' perception of app developers. The mean five-point Likert scale scores ranged from 2.90 to 3.17, indicating that students slightly disagreed that app developers were trustworthy and kept their promises and commitments.

2c. The answers to Questions P212 to P217 indicated students' attitude towards providing information via their mobile devices. The mean five-point Likert scale scores of these questions were all below 3, ranging from 2.30 to 2.97. Therefore, students agreed that providing private information such as HKID number, full name and phone numbers was risky.

2d. The mean five-point Likert scale score of Question P219 was 3.10, revealing that respondents were not familiar with the data protection act of Hong Kong.

2e. Regarding the respondents' practice and knowledge of protecting their privacy on their mobile devices, the last three rounds' mean five-point Likert scale scores in Questions 28 and 30 were 3.00, 3.07 and 2.79 and 2.93, 2.97 and 2.68, respectively. Overall, respondents agreed that they had a good practice and good knowledge of the issue.

2f. The mean five-point Likert scale score of Question 29 was 2.14. This finding indicated that students considered protecting the privacy of their mobile devices important.

Part 3: Boundary Rules and Control of Private Information on Mobile Devices

3a. The means five-point Likert scale scores of Questions P301, P302, P303 and P304 in the last three rounds were all below 3, ranging from 2.37 to 2.87. Therefore, participants found themselves well managing and well keeping their private information stored on their mobile devices.

3b. The mean five-point Likert scale scores of Questions P302, P303 and P304 in the last three rounds were all below 3. Therefore, participants delete and/or update the apps on their mobile devices regularly, check and modify the privacy settings of their mobile devices and delete the information stored on mobile devices that were too private.

3c. Regarding participants' boundary rules and control of their private information stored on their SNS, the mean five-point Likert point scale scores of the response of the last three rounds were mostly below 3, ranging from 1.73 to 3.00. These scores suggest that participants agreed that they had sufficient or proper boundary rules and control of their SNS information and settings on their SNS accounts. This finding was consistent with the results in Part 2.

3d. Regarding respondents' boundary rules and control of their private information on IM accounts, the mean five-point Likert scale scores of responses to Questions P314 and P315 in the last three rounds were all below 3. This finding was consistent with the results in Part two.

3e. Question P316 asked respondents about forwarding someone's text messages or photos to other people without seeking their consent beforehand. The mean five-point Likert scale scores of the responses in the last three rounds were 3.07 (S.D. 0.828), 2.63 (S.D. 0.850) and 2.92 (S.D. 0.845), respectively. Therefore, respondents often forwarded someone's text messages and photos to others.

5.4 The Enhancement Rounds of Teaching

Table 61 shows the pedagogical models of the three enhancement rounds. According to the results from the FR and the pre-teaching survey of ER1, ER1 used a current event with the designated student assignment of ER1 as the pedagogical model. According to the results of ER1 and the pre-teaching survey of ER2, ER2 used the QRS, case video teaching and the designated student assignment of ER2. As the QRS was not effectively used, case video teaching with the designated student assignment of ER3 were used to teach ER3 class.

Table 61: Pedagogical Models of the Three Enhancement Rounds

Session	Components		
1	Conduct pre-teaching survey (one week before the privacy lesson).		
2	Introduce the topic.		
3	Teach the basic concepts of online privacy management using presentation slides ◎ Section one: Malware related to online privacy ◎ Section two: Online privacy in mobile devices ◎ Section three: Six PCPD data protection principles ◎ Section four: Mobile app permission details ◎ Section five: Online privacy management strategies – CPM theory		
	Enhancement Round 1	**Enhancement Round 2**	**Enhancement Round 3**
4	Discussion about the current event: - Latest news – Privacy leakage in WhatsApp - WhatsApp settings - WhatsApp privacy and security controls	Moodle QRS Case teaching: online video Case one: Managing Andy's Facebook information Case two: Managing Mr. Lau's private information such as mobile phone number and medical records	Case teaching: online video Case one: Managing Andy's Facebook information Case two: Managing Mr. Lau's private information such as mobile phone number and medical records
5	Summarise the teaching contents.		
6	Complete online assignment of ER1.	Complete online assignment of ER2.	Complete online assignment of ER3.
7	Conduct post-teaching survey.		
8	Conduct post-teaching interview.		

5.5 Enhancement Rounds of Assignments

After each round of teaching, an assignment was distributed to participating students. The purpose of this assignment was to gauge students' understanding of the online privacy management knowledge taught in class. The assignment was designed from an online video. The questions in the assignment are shown below.

As the teaching activities adopted in enhancement rounds varied, three sets of student assignments based on CPM theory were designed and given to participating students in different enhancement rounds.

5.5.1 The assignment in enhancement round 1 teaching

Table 62 shows the assignment question designed for enhancement round 1 teaching:

Table 62: Student Assignment in ER1

Assignment Question
Scenario: Fraudsters often 'trespass' some WhatsApp users to defraud them and their friends. Recently, some people claimed that some of their friends had their phones hacked in this way. A victim received a friend's message asking the victim to send him an SMS message with a 4-digit or 6-digit number. This number is actually the verification code of the victim's WhatsApp account. After obtaining the verification code, the fraudster re-installed the victim's WhatsApp account, and then used the victim's contact list to scam the victim's friends (e.g. asking for point cards). One of the victims claimed that the fraudsters stole her WhatsApp account and cheated her friends by using her phone book contacts. Each of her friends lost $1,280 to the fraudster.
1. Which CPM stage did the victims experience?
2. If you were a friend of the victim, suggest to him or her the new proper boundary settings of WhatsApp, so that he or she can avoid a similar incident in the future.

The first question asked students to apply CPM theory to Andy's case, whereas the second question asked students to deal with the online privacy problems that Mr. Lau encountered. The mean result of the enhancement round 1 students' assignments was 5.88 out of 8, with an S.D. of 1.76.

5.5.2 The assignment in enhancement round 2 teaching

Table 63 shows the assignment question designed for enhancement round 2 teaching. The QRS was applied. The questions focused on the understanding of facts and theory.

Table 63: Student Assignment in ER2

Assignment Question
1. Which of the following is NOT malware that records your personal information? a. Adware b. Virus c. Keystroke logger d. Spyware
2. How is the owner of personal data described in the six protection principles? a. Data user b. Data owner c. Data subject d. Data protector
3. Which of the following is/are identifiable personal information? I. Full name and HKID card number II. Mobile phone number III. Student name and mobile phone number a. I

b. II & III c. I & III d. All of the above 4. At which stage of CPM theory should you set your privacy boundary? a. Ownership b. Control and Rule c. Turbulence d. None of the above

The mean result of the enhancement round 2 students' assignment was 5.68 out of 8, with an S.D. of 1.477.

5.5.3 The assignment in enhancement round 3 teaching

Table 64 shows the assignment question designed for enhancement round 3 teaching:

Table 64: Student Assignment in ER3

Assignment Question
Scenario: Fraudsters often 'trespass' some WhatsApp users to defraud them and their friends. Recently, some people claimed that some of their friends had their phones hacked in this way. The victim received a friend's message asking the victim to send him an SMS message with a 4-digit or 6-digit number. This number is actually the verification code of the victim's WhatsApp account. After obtaining the verification code, the fraudster re-installed the victim's WhatsApp account, and then used the victim's contact list to scam the victim's friends (e.g. asking for point cards). One of the victims claimed that the fraudsters stole her WhatsApp account and cheated her

friends by using her phone book contacts. Each of her friends lost $1,280 to the fraudster.
1. Which CPM stage did the victims experience?
2. If you were a friend of the victim, suggest to him or her the new proper boundary settings of WhatsApp, so that he or she can avoid a similar incident in the future.

The first question asked students to apply CPM theory in Andy's case, whereas the second question asked students to deal with the online privacy problems that Mr. Lau encountered. The mean result of the enhancement round 3 students' assignment was 6.68 out of 8, with an S.D. of 1.749.

Among all the assignment results, enhancement round 3 group obtained the best outcome, confirming that the teaching methodology was appropriate.

5.6 Comparison of the Results from the Pre- and Post-teaching Survey of the Enhancement Rounds of Teaching

5.6.1 Basic Statistical Results

After participating students finished the assignment, they had to complete the questionnaires again to determine if their perceptions on online privacy changed.

Table 65: Comparison of Pre-teaching survey and Post-teaching survey results of Question P103 ('Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access rights to the information on your mobile devices'?)

	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% change	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Yes	3	10.0	9	29.0	+19	5	16.7	8	26.7	+10	13	46.4	7	25.0	-21.4
No	18	60.0	8	25.8	-34.2	19	63.3	10	33.3	-30	8	28.6	9	32.1	+3.5
I do for some of the apps, but not for all	9	30.0	14	45.2	+15.2	6	20.0	12	40.0	+20	7	25.0	12	42.9	+17.9
Total	30	100.0	31	100.0	0	30	100.0	30	100.0	0	28	100.0	28	100.0	0

Table 66: Comparison of Pre-teaching survey and Post-teaching survey results of Question P104

(‘What will you consider when you install an app’?)

	ER1_Pre	ER1_Post	% change	ER2_Pre	ER2_Post	% change	ER3_Pre	ER3_Post	% change
Convenience	53.3%	48.4%	-4.90%	46.7%	43.3%	-20.00%	32.1%	25%	-7.10%
Privacy policy	23.3%	22.6%	-0.70%	16.7%	26.7%	+10.00 %	21.4%	28.6%	+7.20%
Terms and conditions	10.0%	12.9%	+2.90%	3.3%	20%	+16.70 %	7.1%	17.9%	+10.80%

In all the enhancement rounds of teaching, significant changes were observed in the behaviour and attitude of students before and after the lesson. A large proportion of students have decided to read the terms and conditions clearly or ensure that they understand an app’s access rights to the information on their mobile devices when installing an app. In enhancement round 1’s students, this behaviour increased from 10% to 12.9%. In enhancement round 2’s students, it increased from 3.3% to 20%. In enhancement round 3, it also increased from 7.1% to 17.9%. In enhancement round 1 and 3, the terms and conditions was the top consideration of students when downloading an app. In enhancement round 2 and enhancement round 3, it increased from 3.3% to 20% and from 7.1% to 17.9%, respectively.

Table 67: Comparison of Pre-teaching survey and Post-teaching survey results of Question P106

('What is/are the protective actions taken'?)

	ER1_Pre	ER1_Post	% change	ER2_Pre	ER2_Post	% change	ER3_Pre	ER3_Post	% change
Install anti-virus software	54.5%	38.2%	-16.30%	10%	23.3%	+13.3%	17.95	25%	7%

Table 68: Comparison of Pre-teaching survey and Post-teaching survey results of Question P111

('Do you know that some apps will take actions that they have not mentioned they would'?)

	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% chang e	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Yes	19	63.3	25	80.6	+17.3	19	63.3	23	76.7	+13.4	18	64.3	19	67.9	+3.6
No	11	36.7	6	19.4	-17.3	11	36.7	7	23.3	-13.4	10	35.7	9	32.1	-3.6
Total	30	100.0	31	100.0	0	30	100.0	30	100.0	0	28	100.0	28	100.0	0

Table 69: Comparison of Pre-teaching survey and Post-teaching survey results of Question P113 (‘Convenience is important to you’.)

	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% change	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Very important	11	36.7	6	19.4	-17.3	7	23.3	9	30.0	+6.7	7	25.0	2	7.1	-17.9
Important	16	53.3	12	38.7	-14.6	19	63.3	10	33.3	-30	10	35.7	12	42.9	+7.2
Moderately important	2	6.7	7	22.6	+15.9	4	13.3	4	13.3	0	6	21.4	10	35.7	+14.3
Slightly important	1	3.3	6	19.4	+16.1	0	0	7	23.3	+23.3	4	14.3	4	14.3	0
Not important	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Missing	0	0	0	0	0	0	0	0	0	0	1	3.6	0	0	
Total	30	100.0	31	100.0	0	30	100.0	30	100.0	0	28	100.0	28	100.0	0

Table 70: Comparison of Pre-teaching survey and Post-teaching survey results of Question P114 (‘Privacy is important to you’.)

	ER1_Pre		ER1_Post		% Change	ER2_Pre		ER2_Post		% Change	ER3_Pre		ER3_Post		% Change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Very important	7	23.3%	10	32.3%	9.00%	12	40.0%	8	26.7%	-13.30%	6	21.4%	3	10.7%	-10.70%
Important	16	53.3%	9	29.0%	-24.30%	15	50.0%	13	43.3%	-6.70%	10	35.7%	9	32.1%	-3.60%
Moderately important	5	16.7%	7	22.6%	5.90%	3	10.0%	3	10.0%	0.00%	8	28.6%	13	46.4%	17.80%
Slightly important	2	6.7%	4	12.9%	6.20%	0	0%	4	13.3%	13.30%	3	10.7%	3	10.7%	0.00%
Not important	0	0%	1	3.2%	3.20%	0	0%	2	6.7%	6.70%	27	96.4%	0	0%	-96.40%
Missing	0	0%	0	0%	0.00%	0	0%	0	0%	0.00%	1	3.6%	0	0%	-3.60%
Total	30	100%	31	100%	0.00%	30	100%	30	100%	0.00%	28	100%	28	100%	0.00%

Enhancement round 2 and enhancement round 3 showed a significant increment change in the protective measures taken by students. In enhancement round 2, the installation rate grew from 10% to 23.3%, whereas in enhancement round 3, the installation rate grew from 17.95% to 25%. However, in enhancement round 1, the installation rate of security software dropped from 54.5% to 38.2%. All enhancement rounds have shown significant growth in the awareness of the actions taken by apps. Originally, many students considered convenience a top priority. After the lesson, this rate dropped significantly. In particular, in enhancement round 3, convenience dropped from 25% to 7.1%. Instead, privacy has become a more important consideration for students.

Table 71: Comparison of Pre-teaching Survey and Post-teaching Survey Results from Part 2

	ER1_Pre (N = 30, Missing = 0)		ER1_Post (N = 31, Missing = 0)		t-test	ER2_Pre (N = 30, Missing = 0)		ER2_Post (N = 30, Missing = 0)		t-test	ER3_Pre (N = 28, Missing = 0)		ER3_Post (N = 28, Missing = 0)		t-test
	Mean	SD.	Mean	SD.	Sig.	Mean	SD.	Mean	SD.	Sig.	Mean	SD.	Mean	SD.	Sig.
P201	3.43	0.679	3.29	0.643	0.401	3.50	0.731	3.67	0.802	0.404	3.64	0.870	3.32	1.056	0.657
P202	3.70	0.877	3.52	0.962	0.439	3.97	0.928	3.80	0.805	0.460	2.93	0.813	3.18	0.612	0.689
P203	3.57	0.898	3.68	0.909	0.634	3.63	0.890	3.87	0.681	0.259	2.86	0.756	3.00	0.770	0.919
P204	3.87	0.629	3.61	0.715	0.147	3.83	0.791	3.77	0.679	0.727	2.96	0.693	3.00	0.816	0.544
P205	1.2	0.887	1.23	0.762	0.903	0.9	0.845	1.23	0.858	0.135	2.07	0.813	1.86	0.970	0.219
P206	1.83	0.592	1.48	0.677	0.036	1.5	0.861	1.57	0.898	0.770	1.75	0.701	2.07	0.766	0.199
P207	2.1	0.845	1.65	0.709	0.026	1.7	0.837	1.8	1.157	0.703	2.11	0.737	2.00	0.816	0.487
P208	2.03	0.928	1.71	0.739	0.137	1.53	0.860	1.6	0.855	0.764	1.86	0.591	2.19	0.879	0.861
P209	1.3	0.837	1.39	0.882	0.694	1.27	0.691	1.4	0.855	0.509	2.25	0.887	2.43	0.879	0.374
P210	1.83	0.747	1.81	0.749	0.889	1.63	0.718	1.7	0.837	0.742	2.43	0.879	2.50	0.923	0.107
P211	2.07	0.828	1.74	0.815	0.128	1.77	0.935	1.7	0.794	0.767	1.96	0.881	2.29	1.013	0.608
P212	2.27	0.868	2.19	0.910	0.749	1.93	0.961	2.2	0.925	0.278	2.18	0.772	2.50	0.923	0.112
P213	2.7	0.915	2.52	0.926	0.439	2.2	1.064	2.7	1.088	0.077	2.14	0.891	2.18	0.772	0.453
P214	2.67	1.028	2.73	0.944	0.795	2.5	0.974	2.87	0.900	0.135	2.11	0.832	2.39	0.786	0.768
P215	2.23	0.817	2.03	0.875	0.358	1.63	0.890	2.5	0.900	0.000	2.21	0.738	2.39	0.737	0.211
P216	2.13	0.860	2.1	0.944	0.875	1.83	0.950	2.47	0.900	0.010	2.64	0.678	2.57	0.790	0.163
P217	2.03	0.865	1.9	0.831	0.551	1.93	0.828	2.5	0.777	0.008	2.32	0.723	2.50	0.694	0.873
P218	2.31	0.850	2.19	0.873	0.602	2.1	0.960	2.7	0.702	0.008	2.29	0.763	2.18	0.723	0.192

	ER1_Pre (N = 30, Missing = 0)		**ER1_Post** (N = 31, Missing = 0)		**t-test**	**ER2_Pre** (N = 30, Missing = 0)		**ER2_Post** (N = 30, Missing = 0)		**t-test**	**ER3_Pre** (N = 28, Missing = 0)		**ER3_Post** (N = 28, Missing = 0)		**t-test**
	Mean	SD.	Mean	SD.	Sig.	Mean	SD.	Mean	SD.	Sig.	Mean	SD.	Mean	SD.	Sig.
P220	2	0.845	1.9	0.790	0.648	1.93	0.785	2.13	0.819	0.338	1.36	0.870	1.68	1.056	0.369
P221	2.86	0.639	2.61	0.761	0.176	2.57	0.898	2.83	0.791	0.227	2.07	0.813	1.82	0.612	0.718
P222	2.07	0.868	2.06	0.772	0.992	2.03	0.809	2.4	0.814	0.085	2.14	0.756	2.00	0.770	0.350
P219	1.9	0.759	2.13	0.763	0.245	1.57	0.858	2.23	0.858	0.004	2.04	0.693	2.00	0.816	0.592

Table 72: Comparison of Pre-teaching Survey and Post-teaching Survey Results from Part 3

	ER1_Pre (N = 30, Missing = 0)		**ER1_Post** (N = 30, Missing = 0)		**t-test**	**ER2_Pre** (N = 30, Missing = 0)		**ER2_Post** (N = 29, Missing = 1)		**t-test**	**ER3_Pre** (N = 28, Missing = 0)		**ER3_Post** (N = 28, Missing = 0)		**t-test**
	Mean	SD.	Mean	SD.	Sig.	Mean	SD.	Mean	SD.	Sig.	Mean	SD.	Mean	SD.	Sig.
P301	2.37	0.765	2.71	0.643	0.062	2.43	0.728	2.33	0.802	0.615	2.57	0.634	2.54	0.693	0.841
P302	2.37	0.89	2.48	0.724	0.574	2.60	0.77	2.23	1.04	0.127	2.57	0.634	2.54	0.637	0.834
P303	2.13	0.937	2.29	0.864	0.499	2.00	0.91	2.17	0.986	0.499	2.46	0.693	2.46	0.744	1.000
P304	2.63	0.89	2.65	0.755	0.955	2.50	0.777	2.60	0.968	0.661	2.68	0.819	2.39	0.832	0.201
P305	2.33	0.711	2.17	0.95	0.065	2.69	0.66	2.10	1.047	0.413	2.62	0.571	2.31	0.618	0.068
P306	2.47	0.9	2.47	0.86	0.000	2.43	1.04	2.62	0.862	0.001	2.48	0.714	2.65	0.629	0.360
P307	2.97	0.615	2.93	0.64	0.000	2.97	0.765	2.90	0.817	0.000	2.60	0.707	2.85	0.784	0.245
P308	3.03	0.669	2.93	0.691	0.131	3.00	0.587	2.90	0.772	0.549	2.64	0.907	2.73	0.874	0.718
P309	2.43	0.774	2.67	0.661	0.436	2.37	0.89	2.52	0.911	0.523	2.60	0.866	2.46	0.647	0.520
P310	3.13	0.571	3.17	0.461	0.000	3.27	0.691	3.24	0.636	0.000	2.36	0.952	2.69	0.788	0.180
P311	2.00	0.743	2.13	0.73	0.091	2.00	0.871	2.07	0.998	0.001	2.00	0.834	2.27	0.667	0.212
P312	2.83	0.592	2.77	0.679	0.875	2.83	0.648	2.90	0.724	0.852	2.28	0.891	2.81	0.801	0.031
P313	2.33	0.922	2.27	0.868	0.002	2.30	0.952	2.52	0.911	0.003	2.12	0.881	2.42	0.643	0.166
E27	2.57	0.858	2.38	0.942	0.000	2.67	0.711	2.80	0.925	0.000	2.58	0.945	2.54	0.833	0.890
P314	2.83	0.913	2.86	0.789	0.000	2.63	0.928	2.87	0.73	0.000	2.65	0.936	2.67	0.816	0.959
P315	2.77	0.971	3.00	0.655	0.000	3.03	0.718	2.97	0.669	0.000	2.85	0.784	2.92	0.654	0.733

5.6.2 Cross-tabulation Results

The following tables show the results of the cross-tabulation and chi-square of the pre-teaching and post-teaching surveys in the three enhancement rounds.

Enhancement round 1 teaching

Table 73 summarises the cross-tabulation and the chi-squared test results in enhancement round 1. Before the ER1 of teaching, only P220 vs. P304 and P220 vs. P304 had correlation and were significant. After the ER1 of teaching, only P220 vs. P302 had a correlation and was significant. These results reflected that the changes on OPA vs. OPMS did not improve. Therefore, this pedagogical model was not effective in changing the relationship between OPA and OPMS. Succeeding teaching rounds should not be modified according to this model.

Table 73: ER1 - Results of the Cross-tabulation and Chi-squared Test

Pearson's Chi-squared Test – Asymptotic Significant (2-sided) *with p-value 0.05*

Online Privacy Attitude (OPA)	**vs**	**Online Privacy Management Strategies (OPMS)**	**Enhancement Round 1 Pre-teaching survey**	**Enhancement Round 1 Post-teaching survey**
P220: **I have a good habit of protecting my privacy on my mobile device(s).**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.255 *(Not significant)*	0.029 *(Significant)*
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.057 *(Not significant)*	0.133 *(Not significant)*
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.005 *(Significant)*	0.705 *(Not significant)*
P301: **I feel that I can keep all my private information in a way that I feel is acceptable.**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.149 *(Not significant)*	0.422 *(Not significant)*
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.654 *(Not significant)*	0.327 *(Not significant)*
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.001 *(Significant)*	0.053 *(Not significant)*

Enhancement round 2 teaching

Table 74 summarises the cross-tabulation and the chi-squared test results in enhancement round 2. Before the ER2 of teaching, only P220 vs. P302 had a correlation and was significant. After the ER2 of teaching, P220 vs. P302 and P220 vs. P303 had a correlation and were significant. These results reflected that the changes on OPA vs. OPMS had a little improvement. However, this pedagogical model was not effective in changing the relationship between OPA and OPMS. Succeeding teaching rounds should be modified according to this model.

Table 74: ER2 - Results of the Cross-tabulation and Chi-squared Test

Pearson's Chi-squared Test – Asymptotic Significant (2-sided) *with p-value 0.05*

Online Privacy Attitude (OPA)	vs	Online Privacy Management Strategies (OPMS)	Enhancement Round 2 Pre-teaching survey	Enhancement Round 2 Post-teaching survey
P220: **I have a good habit of protecting my privacy on my mobile device(s).**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.034 *(Significant)*	0.013 *(Significant)*
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.057 *(Not significant)*	0.006 *(Significant)*
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.860 *(Not significant)*	0.068 *(Not significant)*
P301: **I feel that I can keep all my private information in a way that I feel is acceptable.**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.149 *(Not significant)*	0.054 *(Not significant)*
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.654 *(Not significant)*	0.156 *(Not significant)*
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.444 *(Not significant)*	0.196 *(Not significant)*

Enhancement round 3 teaching

Table 75 summarises the cross-tabulation and the chi-squared test results in enhancement round 3. Before the ER3 of teaching, only P301 vs. P302 and P301 vs. P303 had a correlation and were significant. After the ER3 of teaching, no OPA vs. OPMS had a correlation and was significant. These results indicated that the changes in OPA vs. OPMS had no improvement.

Table 75: ER3 - Results of the Cross-tabulation and Chi-squared Test

Pearson's Chi-squared Test – Asymptotic Significant (2-sided) *with p-value 0.05*

Online Privacy Attitude (OPA)	**vs**	**Online Privacy Management Strategies (OPMS)**	**Enhancement Round 3 Pre-teaching survey**	**Enhancement Round 3 Post-teaching survey**
P220: **I have a good habit of protecting my privacy on my mobile device(s).**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.088 *(Not significant)*	0.212 *(Not significant)*
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.560 *(Not significant)*	0.232 *(Not significant)*
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.455 *(Not significant)*	0.326 *(Not significant)*
P301: **I feel that I can keep all my private information in a way that I feel is acceptable.**	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.000 *(Significant)*	0.092 *(Not significant)*
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.009 *(Significant)*	0.305 *(Not significant)*
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.228 *(Not significant)*	0.240 *(Not significant)*

5.7 The Three Enhancement Rounds of Post-teaching interview

After each lesson on privacy, a semi-structured interview was conducted on two volunteer students from the taught class. The following sections show the results of the post-teaching interviews in the three enhancement rounds.

5.7.1 Enhancement Round 1 post-teaching interview

Before attending the class, students did not know about privacy policy thoroughly and had limited knowledge. Moreover, they lacked knowledge about the six DPPs.

> *'Although I understand the importance of a privacy policy, I seldom read it seriously. I only gloss over it or completely ignore the details due to convenience concern'. (Student A)*

> *'Overall, the usefulness of the six data protection principles is so-so for me. I haven't heard of these principles, and didn't know what it was before attending the class'. (Student B)*

After the lesson, they acquired knowledge on the DPPs and CPM theory. Interviewees could even immediately identify the first two stages of the theory (i.e. ownership and control and rules). They could also apply the knowledge to their daily life.

Students voiced that they would not disclose their personal information, such as identity card and passport numbers to anybody 'since I received more knowledge regarding the leakage of personal data during the lecture' (Student B).

> *If I notice any data breach, I will modify the privacy setting as long as*

> *I can do it, and constantly monitor my data from being stolen for another purpose'. (Student B)*

The newspaper issue did not have much impact on interviewees as they were not active users of LINE or chatrooms. They voiced that such a scenario would not happen to them.

> *'If this happens to me, I will not click the link; instead, I will first ask confirmation from my friends and block the chat room immediately'. (Student B)*

> *'As an inactive user of Line, receiving a message like this is weird for me'. (Student A)*

After the lesson and after gaining more knowledge about privacy protection, students generally believed that the existing security measures of their mobile devices were insufficient.

> *'I don't think the security control on my mobile device was enough to protect my privacy, as I only set a simple password to my phone. After the class, I strengthened the privacy level, for example, I deleted personal data and stored them other than my phone'. (Student A)*

> *'I think I have enough knowledge to protect my privacy on my device. After the lesson, I learned more information, such as the notices and ways how to protect private information'. (Student A)*

> *'I rarely check and modify the privacy settings of my phone (before the lesson). I will pay more attention to the settings and the purpose of*

> *data collection after attending the lesson'. (Student B)*

5.7.2 Enhancement Round 2 Post-teaching Interview

The attitude of both interviewees towards privacy policy changed significantly after the lesson.

> *'I seldom read the privacy policy before the class. Now, I try to read the important parts instead of the whole policy before downloading an app'. (Student A)*

> *'I tended to read the policy more when browsing an accounting page but seldom did that for the download notice of an app. After the lesson, I will read them in all situations'. (Student B)*

Both interviewees agreed that the six DPP principles were important.

Principle #1: Both interviewees agreed that companies should only collect personal data of their customers legally and appropriately. Otherwise, they would not provide any personal data to any of these parties that inappropriately and illegally collected data.

Principle #2 (to provide accurate information and destroy them within the specified retention period): Both interviewees rated this principle ⅗ and pointed out that the company should delete their data within a year.

Principle #3: This principle was rated ⅘. Both interviewees agreed that they should always be wary when giving out their personal information and should refuse to provide their personal data, which were irrelevant to app developers.

Principle #4: Both interviewees agreed that this principle was relatively important in protecting their personal information.

Principle #5: Both interviewees rated this principle important. They would not hand in personal data if a company had not disclosed its purpose of data collection.
Principle #6: Both interviewees rated this principle important.

Both interviewees stated that the class did not change their behaviours at all in the three stages of CPM theory.

On ownership:

> *'Regardless of the class, I won't allow any apps to access my contacts'. (student A)*

> *'I don't mind apps accessing my data at all. Even after attending the class, my behaviour didn't change. For example, if an app asks for permission for access to my contacts, I will continue the download. It doesn't matter to me'. (student B)*

The class did not change their behaviours regarding the last two stages.

> *'In the area of data protection, I always treat everyone equally without double standards, whether they are my family, best friend or*

> *acquaintance. For example, I will not send any information from my close friends, family and even acquaintance to others easily. I don't make any exception'. (Student A)*

Interviewees were asked if they had ever forwarded information about others without their permission. Both replied: 'Yes, I did. But I tended to share information that is not sensitive, unlike credit card passwords'.

For the feedback activity, both stated that 'The content is useful for me to answer the questions because I didn't know how to answer the questions before attending the class'. They thought that the case study video presented more information about privacy. For example, they realised that they could be breaking the law and be sued in some situations.

Overall, both interviewees rated the class ⅘ (useful).

> *'The class is full of superficial knowledge. I prefer practical and in-depth information such as app recommendations which help protect the privacy in my devices'. (Student A)*

> *'I was so shocked when the lecturer announced that WeChat always records my conversations. I'm grateful to hear this useful information for a comprehensive understanding of privacy'. (Student B)*

5.7.3 Enhancement Round 3 post-teaching interview

Similar to previous rounds, students lacked knowledge on privacy policy before the class.

> *'Application portals, which require me to provide personal*

> *information like HKID and phone number, are the only platform where I know about privacy policy. I also used to believe that the company can only keep my data for its specified collection purpose, rather than selling them to other third parties'. (Student A)*

> *'I did not know what privacy policy was before attending the class. I only know that I have to keep my data (password) well'. (Student B)*

The lessons provided much information about CPM theory and its application.

> *'I've set my Instagram account to private so that only my approved followers can see my feed and photos'.*
> *(Student A)*

> *'I always ask permission patiently in a group chat via WhatsApp as long as they are the main subject of my photo. They can either type 'ok' for yes or DM me privately to object in this situation. If anyone objects, then I will not send that photo to others. After the class, I improved a lot on setting boundaries for social media and chat rooms. For example, I refuse to use Facebook frequently as I'm afraid of getting hacked by the poor security system in my company. Furthermore, I will delete sensitive information such as phone numbers, and modify the visibility of personal data (e.g. email) to 'Only Me' on the privacy setting. After I make these changes, strangers will no longer be able to see my data on Facebook in the*

> *future. At the same time, I always concentrate on protecting my information in the IM platform'.*
>
> *(Student B)*

The use of the case study during the class was a success, as the interviewees could briefly repeat the content of the activity. Both students voiced how they applied their knowledge from the case study to their real-life data protection.

> *'After the lesson, to minimise the possibility of a data breach by hackers, I avoided sending sensitive/confidential information, such as work documents, via public Wi-Fi. I will only use public Wi-Fi for non-confidential information, such as conversations with friends, in a chat room'. (Student B)*

NVivo Results of the Three Enhancement Rounds

Using NVivo, the post-teaching interviews of students were coded into positive, negative and other themes. Each theme was given a label, and the percentage of students contributing to the theme was calculated. Figure 23 shows the results of the post-teaching interview in ER1, ER2 and ER3.

Figure 23: Percentage of Each Theme in the Remaining Rounds of Teaching

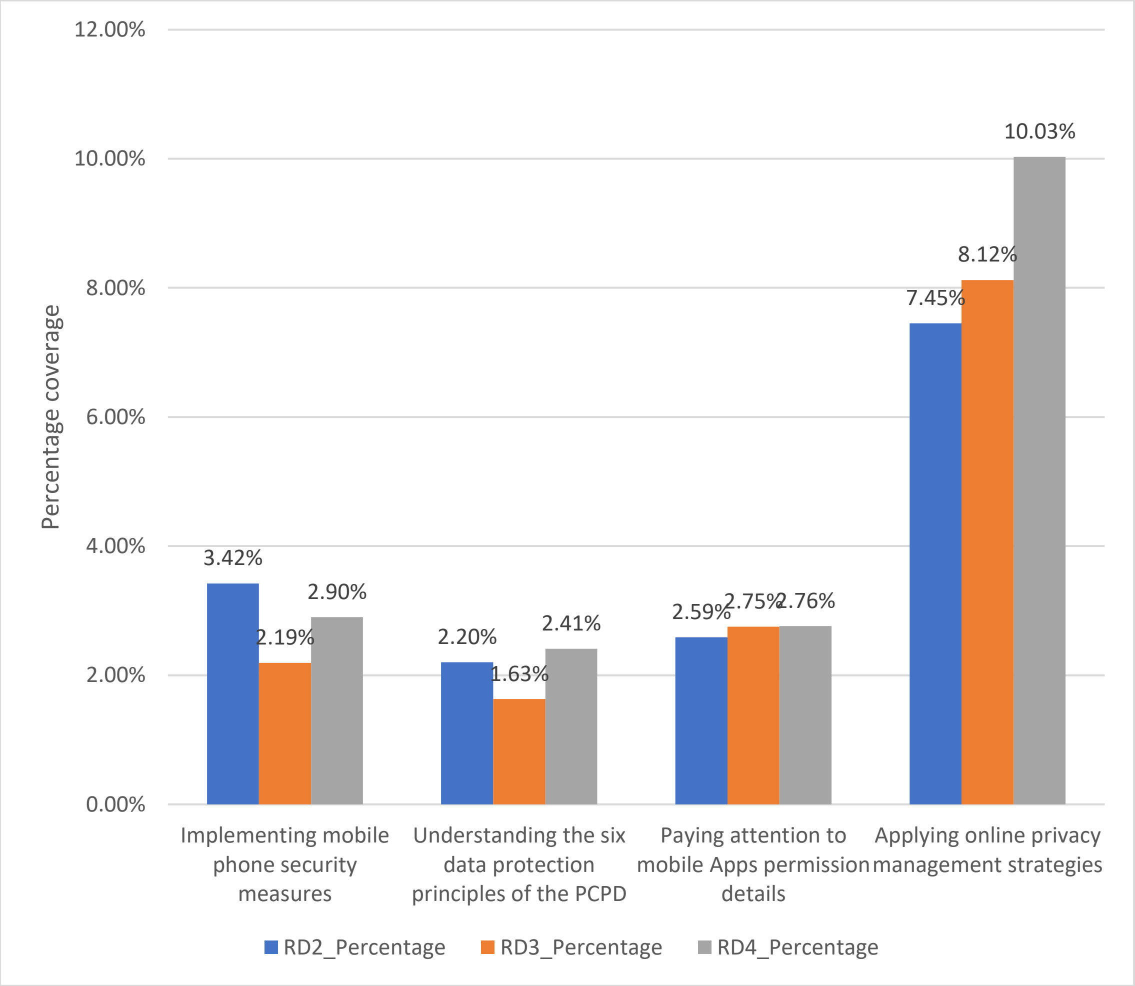


Table 76: Qualitative Result of the Lesson in the Enhancement Rounds

Theme	**Interpretation** ***(Refer to Figure 23)***
Implementing mobile phone security measures	Among the three remaining teaching classes, Enhancement Round 1 teaching class (3.42%) gave the most attention to their mobile phone security to protect the private information stored on their mobile phones. By contrast, Enhancement Round 2 teaching class have the least attention to this aspect (2.19%).
Understanding the six data protection principles of the PCPD	Overall, students initially did not know the six PCPD data protection principles. They only learned about these principles from the lesson. However, the percentage coverage of this theme among the three teaching classes ranged between 1.63% and 2.41%, indicating that they could not recall the details of the principles.
Paying attention to mobile apps' permission details	Students were not aware of the importance of reading mobile apps' permissions or terms and conditions when or after installing apps. The percentage coverage of this theme among the three teaching classes was between 2.59% and 2.76%, showing that they did not have a strong intention to read the app permission details before downloading an app.
Applying online privacy management strategies	Students did not know much about online privacy management strategies before the lesson. They found that the online privacy management strategies were useful for protecting their personal information. The percentage coverages were 7.24%, 8.12% and 10.03% in the second, third and fourth teaching classes, respectively.

5.8 Teachers' Reflection

Enhancement Round 1 Teaching

After teaching the second class, the teachers had the following observations and reflections:

1. Using current events could fairly engage students during the lesson.
2. Students did not have much discussion when they were working on the assignments.
3. Students did not jot down notes when they were watching the current event.
4. Students tackled the assignment questions well.
5. Some students pointed that they had watched the current event story before.
6. The initial responses of students showed that they did not enjoy the lessons, and the current event article did not appeal to them.

Enhancement Round 2 Teaching

After teaching the third class, the teachers had the following observations and reflections:

1. Students were supposed to finish the Moodle QRS questions after a small part of the content was taught. However, the instant teaching effects were not seen. Students did not want to follow the activity of this part.
2. Students did not have much discussion when they were working on the assignments.
3. Students jotted down notes when they were watching the case studies videos.
4. Students tackled the assignment questions well.
5. The teachers found that the Moodle QRS was not effectively used during the lesson. Students could not catch up with the teaching pace in this part, that is, direct teaching with Moodle QRS.

Enhancement Round 3 Teaching

After teaching the fourth class, the teachers had the following observations and reflections:

1. The case teaching method could engage students during the lesson. Students paid more attention under this method than in the direct teaching section.
2. Students were willing to discuss with their classmates when they were working on the assignments.
3. Students jotted down notes when they were watching the case studies video.
4. Students tackled the assignment questions well.
5. The case background was old.
6. The initial responses of students showed that they enjoyed the lessons. The case studies were interesting, not monotonous and relevant to their daily life.
7. Although most students were willing to complete the post-teaching survey, some did not do it seriously. For example, some of them returned the completed survey in only five minutes.

5.9 Key findings from the Three Enhancement Rounds

Pre-teaching Survey

- Most students have learned about online privacy from their primary and secondary schooling.
- Participants depended heavily on their mobile devices for the primary use of social networking. Therefore, contact information was the most common information stored in their mobile devices.
- Students' attitude towards data privacy was fairly positive, and not much measures had been put to protect their online privacy.

Pre- vs. Post-teaching Survey

- In all the remaining rounds of teaching, the behaviour and attitude of students had significant changes before and after the lesson. More students would read the terms and conditions clearly or ensure that they understand an app's access rights to the information on their mobile devices when installing an app. In Enhancement Round 1 students, this behaviour increased from 10% to 29%. In Enhancement Round 2 students, it increased from 16.7% to 26.7%. However, in Enhancement Round 3, it decreased from 46.4% to 25%.
- The terms and conditions became a more important concern among students. Significant changes could be observed from Enhancement Round 2 and Enhancement Round 3, in which this consideration increased from 3.3% to 20% and from 7.1% to 17.9%, respectively.
- Enhancement Round 2 and Enhancement Round 3 showed a significant incremental change in the protective measures taken by students. In Enhancement Round 2, the

installation rate of security software grew from 10% to 23.3%, whereas in Enhancement Round 3, the installation rate grew from 17.95% to 25%. However, in Enhancement Round 1, the rate dropped from 54.5% to 38.2%.

- Originally, many students believed that convenience was very important for them. After the teaching, this rate dropped significantly. In Enhancement Round 3, it dropped from 25% to 7.1%. By contrast, privacy became a more important consideration for students.

Post-teaching Interview

- Before attending the classes, students did not know about privacy policy thoroughly, and they had limited knowledge. Similarly, interviewees were lacking knowledge in the six DPPs.
- After the lesson, they acquired knowledge about the six DPPs and CPM theory. Interviewees could even immediately state the first two stages of the theory (i.e. ownership and control and rules). They could also apply it in real life.
- Students voiced that they would not disclose their personal information, such as identity card and passport numbers, to anybody, because of their new knowledge about the possibility of leakage of personal data.

- Enhancement Round 1
  - The newspaper issue did not have much impact on interviewees, as they were not active users of LINE or chatrooms. They said that the incident would not happen to them.
  - After the teaching, students believed that the existing security measures of their mobile devices were insufficient, as they gained new knowledge about privacy protection.
- Enhancement Round 2
  - In all the three stages of CPM theory, both interviewees stated that the class did not change their behaviours. This finding reflected that CPM theory was not effective in improving students' privacy management strategies.
  - For the feedback activity, both stated that 'the content is useful for me to answer the questions because I didn't know how to answer the questions before attending the class'. By contrast, the case study video presented more information about privacy to them. For example, they realised that they could be breaking the law and be sued in some situations.
  - Overall, both interviewees rated the class ⅘ (useful).
- Enhancement Round 3
  - Similar to the previous rounds, students lacked the knowledge on privacy policy before the class.
  - The lessons provided much information about CPM theory and its application.
  - The use of the case study during the class was a success, as the interviewees could briefly repeat the content of the activity. Both students voiced how they were able to apply the case study knowledge to their real-life data protection.

5.10 Summary of the Three Enhancement Rounds

This section shows the achievements, problems that still needed to be solved and how to tackle the problems in next round in the three enhancement rounds.

Enhancement Round 1

Achievement of ER1

- The chosen current event could not attract students' attention.
- In the post-teaching interview, students showed that they did not learn much in the current news. They felt that they would not make the similar mistakes featured in the current event news.

Problems that still needed to be solved

- The news could not motivate students effectively, and they did not enjoy this activity.

How to tackle these problems in next round

- As the current news could not motivate ER1 students effectively, the teacher decided to modify the FR's pedagogical model. Besides, QRS was incorporated to improve students' learning process.

Enhancement Round 2

Achievement of ER2

- The QRS was not very effective, whereas the case studies could attract students' attention.
- In the post-teaching interview, students showed that the QRS was not very useful in learning the privacy concepts, and they had difficulty follow the teaching pace through the QRS questions. By contrast, they felt that the case study video was more useful in learning about privacy issues in their daily life.

Problems that still needed to be solved

- The QRS was not effectively used.

How to tackle these problems in next round

- The QRS was not effectively used in reviewing the privacy knowledge, whereas the case study video was an excellent teaching aid in assisting students to learn the concepts of privacy.

Enhancement Round 3

Achievement of ER3

- Students could learn from the video effectively and attentively. The average of their assignment scores was the highest among all teaching rounds.
- In the post-teaching interview, students found the video useful, as it featured several privacy cases that they could learn from.

Conclusion

- The pedagogical model of the FR was repeated in ER3. The result was clear and encouraging. Students' privacy concern and boundary rule and control were improved.
- However, the analysis of the results of the cross-tabulation of the three enhancement rounds showed that the relationship between OPA and OPMS was unrelated as well. This result indicated that OPA did not significantly affect OPMA. The privacy paradox occurred again.
- Stages 1 and 2 of CPM theory were effective in enhancing students' privacy ownership and privacy management strategies in ER1 and ER3. However, all stages of CPM theory were not useful in ER2.

Chapter 6 Overall Analysis of All Teaching Rounds

6.1 Key Findings from the Answers in RQ1 (privacy attitude)

This section summarised the key findings in the four teaching rounds as reported in Chapter 4 to Chapter 5. As mentioned in Chapter 3, Parts 1 and 2 of the pre-teaching survey were designed to answer Research Question 1: What are higher education students' online privacy attitudes towards using mobile devices? This section presents the key findings of Parts 1 and 2.

Part 1: Use of Mobile devices

Question P103 asked students: 'Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access rights to the information on your mobile devices?' Less than 20% of students in the first 3 teaching rounds would read the terms and conditions before they decide to install some apps. In ER3, 46% of students would read them.

Table 77: Students' Consideration of an App's Terms and Conditions and Access Rights Prior to Downloading (all teaching rounds)

Item	Foundation Round (FR)	Enhancement Round 1 (ER1)	Enhancement Round 2 (ER2)	Enhancement Round 3 (ER3)
Yes	12%	10%	17%	46%
No	42%	60%	63%	29%
I do so for some of the apps, but not for all.	46%	30%	20%	25%
Total	100%	100%	100%	100%

Question P104 asked participants: 'What will you consider when you install an app'? Table 78 shows that students in all teaching rounds considered mainly the functions and the cost (free or paid) of an app before installing it. The terms and conditions and the privacy policy were among the least concern factors. These findings showed that most students did not understand the importance of protecting their online privacy while using their mobile devices.

Table 78: Students' Considerations when Deciding to Install an App (all teaching rounds)

Item	Foundation Round (FR)	Enhancement Round 1 (ER1)	Enhancement Round 2 (ER2)	Enhancement Round 3 (ER3)
Popularity	55%	30%	67%	71%
User reviews	58%	37%	37%	57%
Functions	79%	83%	73%	64%
Degree of needs	52%	67%	77%	50%
Convenience	55%	53%	47%	32%
Quick to download or not	12%	7%	10%	14%
Free or paid	79%	73%	73%	64%
Privacy policy	6%	23%	17%	21%
Terms and conditions	9%	10%	3%	7%
Others	0%	0%	7%	0%

Table 79 shows that screen lock was the most common protective action taken by students. In particular, over 50% of respondents set up an auto screen lock and use it for their mobile devices.

Table 79: Protective Actions Taken by Students to Secure their Mobile Privacy (all teaching rounds)

Item	**Foundation Round (FR)**	**Enhancement Round 1 (ER1)**	**Enhancement Round 2 (ER2)**	**Enhancement Round 3 (ER3)**
Set up auto screen lock	79%	67%	77%	82%
Set up screen lock	79%	50%	70%	86%
Install anti-virus software	9%	23%	10%	18%
Install anti-theft software	12%	13%	13%	18%
Others	3%	0%	7%	7%

Table 80 displays the results of questions P110, P111 and P112. More than half of students in each teaching round knew that their contact lists may be uploaded to the servers of apps, some apps may take undisclosed actions and that their geo-location information was recorded in the photo that they take.

Table 80: Percentage of Students who were Aware of Apps' Actions on Mobile Devices (all teaching rounds)

	Item	**Foundation Round**	**Enhancement Round 1**	**Enhancement Round 2**	**Enhancement Round 3**
		Yes	**Yes**	**Yes**	**Yes**
P110:	Do you know that your contact lists may be uploaded to the central servers of the SNS apps that you are using?	76%	63%	73%	71%
P111:	Do you know that some apps will take actions that they have not mentioned they would?	58%	63%	63%	64%
P112:	Do you know that, when you take a picture with your mobile devices, your geo-location may be recorded in the photo?	85%	70%	80%	71%

The results from Questions P113 and P114 displayed students' perceptions of the importance of convenience and privacy. Both attributes had the same degree of importance to students with a mean of approximately 3 and a standard deviation of approximately 0.8. In general, all groups believed that convenience and privacy were important issues.

Table 81: Mean and SD of Students' Perception of Convenience and Privacy of an App (all teaching rounds)

Item		**Foundation Round (FR)**		**Enhancement Round 1 (ER1)**		**Enhancement Round 2 (ER2)**		**Enhancement Round 3 (ER3)**	
		Mean*	**S.D.**	**Mean***	**S.D.**	**Mean***	**S.D.**	**Mean***	**S.D.**
P113:	Convenience is important to you.	3.09	0.843	3.23	0.728	3.09	0.607	2.74	1.023
P114:	Privacy is important to you.	3.09	0.947	2.93	0.828	3.30	0.651	2.70	0.953

**Note: 5 = very important; 4 = important; 3 = moderately important; 2 = slightly important; 1 = not important*

Contact information of their friends, classmates and family members was the most popular personal information stored in their mobile devices. Email addresses and personal and sensitive photos were the second and third, respectively, popular personal information saved in their mobile phones.

Moreover, students from the FR to ER3 stored someone's online account IDs and passwords, email account passwords, entrance code of buildings and ATM passwords on their mobile devices. Although these percentages were not too high, these data are private information that should not be shared to anyone under normal circumstances.

Table 82: Types of the Personal Information of Friends, Classmates and Family Members that are Stored in Students' Mobile Devices (all teaching rounds)

Item	**Foundation Round (FR)**	**Enhancement Round 1 (ER1)**	**Enhancement Round 2 (ER2)**	**Enhancement Round 3 (ER3)**
Contact information	88%	90%	83%	79%
Entrance code of the building where you and your family members live	18%	13%	20%	25%
ATM password(s)	12%	10%	10%	21%
Online account number and password	27%	17%	30%	29%
Email addresses	46%	47%	60%	43%
Email account passwords	21%	13%	20%	21%
Personal and sensitive photo	58%	37%	60%	36%
Haven't stored any personal information of others	3%	0%	0%	4%
Others	3%	0%	0%	0%

Table 83 exhibits the personal information that students stored on their mobile devices. Contact information and email address were the most popular personal information saved on their mobile devices. Similar to the result of the previous question, 70% of ER2 students save their personal and sensitive photo in their mobile devices, whereas 43% to 57% of Foundation Round, ER1 and ER3 groups did the same.

The results from all the four teaching rounds were consistent but contradiction emerged again. Although, they considered their privacy important, they did not do much to protect their mobile devices.

Table 83: Types of the Personal Information that are Stored in Students' Mobile Devices (all teaching rounds)

Item	**Foundation Round (FR)**	**Enhancement Round 1 (ER1)**	**Enhancement Round 2 (ER2)**	**Enhancement Round 3 (ER3)**
Contact information	82%	80%	90%	75%
Entrance code of the building where you and your family members live	15%	13%	33%	21%
ATM password(s)	15%	20%	10%	21%
Online account ID and password	58%	23%	37%	39%
Email addresses	82%	83%	80%	61%
Email account passwords	61%	47%	33%	46%
Personal and sensitive photos	58%	57%	70%	43%
Others	9%	3%	3%	11%
Haven't stored any personal information	0%	0%	0%	4%

Summary of Survey Part 1's Findings [To Answer RQ1]

Based on the above findings, Table 84 summarises participating students' responses in the teaching survey – part 1.

Table 84: Summary of Survey Part 1 Findings from the Answers to RQ1

Item	Table	Purpose	Findings
P103	101	To know whether students read the terms and conditions before installing an app	Not more than 20% of the FR, ER1 and ER2 students may read the terms and conditions before installing an app. Moreover, 46% of the ER3 students would read them before installation of the Apps. ER3 students had a higher level of privacy concern.
P104	102	To know students' considerations when they install an app	More than 60% of students in all teaching rounds considered 'functionality' and 'free or not' when they install an app. Not more than 23% of students of all teaching rounds considered 'privacy policy' and 'terms and conditions'. These results were consistent with question P103.
P106	103	To know the protective actions taken by students for their mobile devices	All teaching round classes used similar protective actions on their mobile devices, which were setting up auto screen lock and screen lock. This result reflected that students choose the most convenient ways to protect their devices.
P110	104	To know whether students are aware that their contact lists are being uploaded to SNS apps' servers	More than half of students in each teaching round knew that their contact lists may be uploaded to the servers of apps, some apps may take undisclosed actions, and geo-location information was recorded in the photo they take. All teaching round classes had good knowledge that their information is kept by others.
P111	104	To know whether students are aware of app developers' actions	
P112	104	To know that whether students are aware that their geo-location is being recorded in the photos they take	

P113	105	To know students' perception of the importance of convenience	The ratings of all teaching rounds, except ER3, were higher than 3 out of 5, where 5 was 'very important'. The rating of ER3 was 2.74 out of 5, which reflected that ER3 students found convenience less important.
P114	105	To know students' perception of the importance of privacy	The ratings of FR and ER2 were higher than 3 out of 5, where 5 was 'Very important'. The ratings of ER1 and ER3 were 2.93 and 2.70 out of 5 respectively, these reflected that the ER1 and ER3 students found privacy less important.
P115	106	To know what types of private information of others were kept on their mobile devices	All teaching round students mainly kept their friends' contact information, their personal and sensitive photos and their email addresses on their mobile devices.
P116	106	To know what types of personal private information were kept on their mobile devices	All teaching round students mainly kept their contact information, their personal and sensitive photos and their email addresses on their mobile devices.

Part 2: Attitudes towards Data Privacy

Table 85 shows students' attitudes towards data privacy on their mobile devices. Questions P201, P202, P203 and P204 were concerned with the possibility of students' information stored on their mobile devices being misused by others. The mean five-point Likert scale scores of these questions were all over 3, ranging from 3.18 to 3.97, where 1 represents 'not concerned at all' and 5 represents 'absolutely concerned'. This result reflected that respondents were slightly concerned about their information stored in their mobile devices being misused by others. For FR, the S.D. of P202, P203 and P204 were over 1.000, which reflected that the results may have irregularities.

Table 85: Students' Attitudes towards Data Privacy in their Mobile Devices (four teaching rounds)

Item		Foundation Round (FR)		Enhancement Round 1 (ER1)		Enhancement Round 2 (ER2)		Enhancement Round 3 (ER3)	
		Mean*	S.D.	Mean*	S.D.	Mean*	S.D.	Mean*	S.D.
P201:	The information I submit on my mobile device(s) could be misused.	3.41	0.837	3.43	0.679	3.50	0.731	3.18	0.612
P202:	People can get hold of my private information on my mobile device(s).	3.56	1.134	3.70	0.877	3.97	0.928	3.30	0.823
P203:	Others might use my mobile device(s) to submit information.	3.44	1.162	3.57	0.898	3.63	0.89	3.32	0.905
P204:	Information submitted through my mobile device(s) could be used in many ways, such as advertising, which I cannot foresee.	3.38	1.008	3.87	0.629	3.83	0.791	3.19	0.834

**1 = not concerned at all; 2 = a little concerned; 3 = concerned; 4 = very concerned; 5 = absolutely concerned*

The results of Questions P206, P207, P208 and P209 displayed students' perception of app developers. As shown in Table 110, the mean five-point Likert scale scores of these questions ranged from 2.10 to 1.47, where 5 represents 'strongly agree' and 1 represents 'strongly disagree'. Thus, students slightly disagreed that app developers were trustworthy and kept their promises and commitments.

Questions P212 to P217 indicated students' attitude towards providing information via their mobile devices. The mean five-point Likert scale scores of these questions were all below 3 in the FR and ER1 rounds, ranging from 2.03 to 2.76; whereas, they were approximately 2 in the ER2 and ER3 teaching rounds, ranging from 1.63 to 2.5. In the scale, 5 represents 'strongly agree' and 1 represents 'strongly disagree'. These scores indicated that students agreed that providing private information such as HKID number, full name and phone numbers was risky. The mean five-point Likert scale score of Question P219 of FR to ER3 were 1.88, 1.90, 1.57 and 2.29. These results revealed that respondents were not familiar with the data protection act of Hong Kong. Regarding respondents' practice and knowledge of protecting their privacy on their mobile devices, the mean five-point Likert scale scores of Questions P220 and P222 of FR to ER3 were 2.30, 2.00, 1.93, 2.21 and 2.18, 2.07, 2.03, 2.32, respectively. The scores showed that respondents agreed that they had a fair practice and fair knowledge of the issue. Finally, regarding the importance of protecting respondents' privacy on their mobile devices, the mean five-point scale score result of Question P221 listed Table 86 were all above 2.50. This finding indicated that students considered protecting their privacy on their mobile devices important.

Table 86: Students' Perceptions towards the Importance of Protecting the Privacy in their Mobile Phones (Four teaching rounds)

Item		Foundation Round		Enhancement Round 1		Enhancement Round 2		Enhancement Round 3	
		Mean*	S.D.	Mean*	S.D.	Mean*	S.D.	Mean*	S.D.
P205	'I live an upright life, and I have nothing to hide. Why should I care about my mobile privacy?'	1.18	0.882	1.20	0.887	0.90	0.845	1.36	0.870
P206	App developers are trustworthy.	1.58	0.867	1.83	0.592	1.50	0.861	2.07	0.813
P207	App developers keep their promises and commitments.	1.76	1.001	2.10	0.845	1.70	0.837	2.14	0.756
P208	App developers keep their customers' best interests in mind.	1.58	1.062	2.03	0.928	1.53	0.860	2.04	0.693
P209	It is not a serious matter even if my personal information is collected by app developers.	1.47	0.879	1.30	0.837	1.27	0.691	2.07	0.813
P210	I have perfect control of all my private information stored on my mobile device(s).	1.73	0.839	1.83	0.747	1.63	0.718	1.75	0.701
P211	The security control on my mobile devices is enough to protect my own privacy.	2.09	1.071	2.07	0.828	1.77	0.935	2.11	0.737
P212	Shopping with my mobile device(s) is risky.	2.21	0.857	2.27	0.868	1.93	0.961	1.86	0.591
P213	Providing credit card information online via mobile device(s) is risky.	2.55	1.063	2.70	0.915	2.20	1.064	2.25	0.887
P214	Providing my HKID number and/or full name via mobile device(s) is risky.	2.76	1.001	2.67	1.028	2.50	0.974	2.43	0.879
P215	Providing my phone number via mobile device(s) is risky.	2.03	1.045	2.23	0.817	1.63	0.890	1.96	0.881
P216	Providing my friends' phone numbers via mobile device(s) is risky.	2.18	1.103	2.13	0.860	1.83	0.950	2.18	0.772
P217	Registering via mobile device(s) is risky.	2.19	0.859	2.03	0.865	1.93	0.828	2.14	0.891
P218	Shopping online for certain products is riskier on mobile phones than via non-mobile computers.	2.22	0.870	2.31	0.850	2.10	0.960	2.11	0.832

Item		Foundation Round		Enhancement Round 1		Enhancement Round 2		Enhancement Round 3	
		Mean*	S.D.	Mean*	S.D.	Mean*	S.D.	Mean*	S.D.
P220	I have a good habit of protecting my privacy on my mobile device(s).	2.3	0.770	2.00	0.845	1.93	0.785	2.21	0.738
P221	Protecting my privacy on my mobile device(s) is important.	2.67	0.816	2.86	0.639	2.57	0.898	2.64	0.678
P222	I have good knowledge of protecting my own privacy on my mobile device(s).	2.18	0.917	2.07	0.868	2.03	0.809	2.32	0.723
P219	I am familiar with the data protection act of Hong Kong.	1.88	0.927	1.90	0.759	1.57	0.858	2.29	0.763

**5 = strongly agree; 4 = agree; 3 = undecided; 2 = disagree; 1 = strongly disagree*

Summary of Survey Part 2's Findings [To Answer RQ1]

To show the levels of privacy concern of students, the study classified the six groups according to the mean and S.D. of the teaching rounds. Students with lower mean scores were categorised as 'unconcerned', whereas those with higher mean scores were grouped under 'extremely concerned'. Table 87 shows the levels of the privacy concern of students.

Table 87: Levels of the Privacy Concern of Students

Range	Level
Mean + 2 S.D. to **5**	Extremely concerned
Mean + S.D. to Mean + 2 S.D.	Very concerned
Mean to Mean + S.D.	Quite concerned
Mean – S.D. to Mean	Somewhat concerned
Mean – S.D. to Mean – 2 S.D.	A little concerned
1 to Mean - 2 S.D.	Unconcerned

Figure 24 to 27 show the number of students in each level of concern.

Figure 24. FR students - Pre-teaching Survey Results of the Level of Privacy Concern

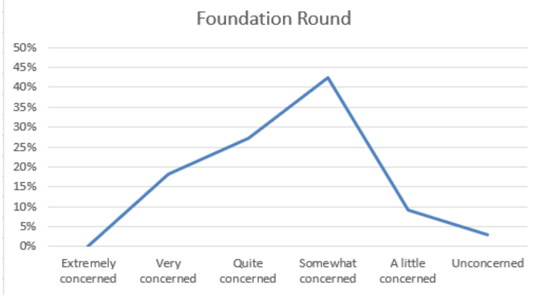


Figure 25. ER1 students - Pre-teaching Survey Results of the Level of Privacy Concern

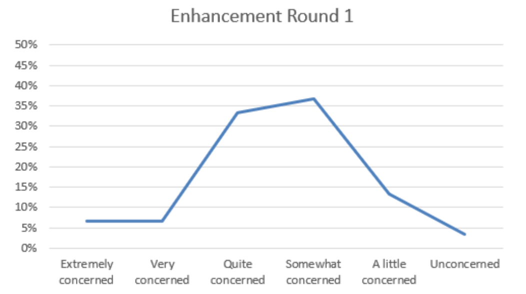


Figure 26 ER2 students - Pre-teaching Survey Results of the Level of Privacy Concern

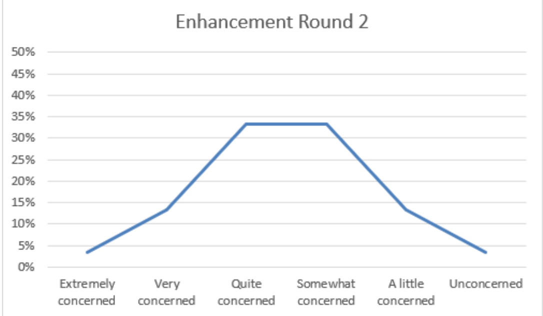


Figure 27 ER3 students - Pre-teaching Survey Results of the Level of Privacy Concern

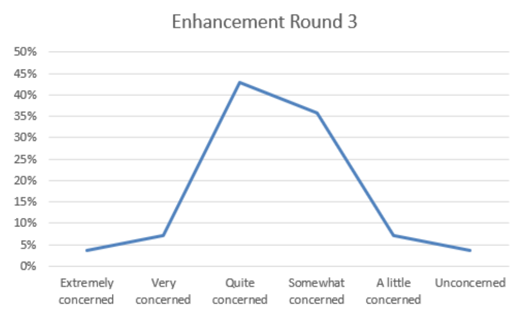


Table 88: Levels of Privacy Concern Before the Lesson [Survey Part 2]

Level	**Foundation Round**		**Enhancement Round 1**		**Enhancement Round 2**		**Enhancement Round 3**	
Extremely concerned	0%		7%		3%		4%	
Very concerned	18%	45%	7%	47%	13%	49%	7%	55%
Quite concerned	27%		33%		33%		43%	
Somewhat concerned	42%		37%		33%		36%	
A little concerned	9%		13%		13%		7%	
Unconcerned	3%		3%		3%		4%	

The above figures and table show the levels of privacy concern of students in all teaching rounds before the lessons. More students in ER3 were ‘extremely concerned’ (4%), ‘very concerned’ (7%) and ‘quite concerned’ (43%), which account for a total of 59%. This result implied that ER3 students had a higher degree of privacy concern before the lesson. These findings were consistent with Survey Part 1’s findings; ER3 students had a higher degree of privacy concern in many items in Part 1.

6.2 Key Findings from the Answers to RQ2 (CPM theory improves students' privacy management strategies)

How effective is using CPM theory to improve HEI students' online privacy management strategies for their mobile devices? CPM theory consists of three stages. In stage 1 (privacy management), Question P116 asked: What types of your personal information are stored in your mobile devices? This question was the key item for this stage.

Table 89: Key Items for Stage 1 - Privacy Ownership

Item	**FR**	**ER1**	**ER2**	**ER3**
Friends' contact information	82%	90%	83%	79%
Entrance code of building where you and your family members live	15%	13%	20%	25%
Someone's ATM password(s)	15%	10%	10%	21%
Someone's online account number and password	58%	17%	30%	29%
Their email addresses	82%	47%	60%	43%
Their email account passwords	61%	13%	20%	21%
Their personal and sensitive photo	58%	37%	60%	36%
Haven't stored any personal information of others	0%	0%	0%	4%
Others	9%	0%	0%	0%

Results from the Pre- and Post-teaching Survey on Students' Perception

After the lesson, students had to complete the questionnaire again to determine any changes in their perceptions on online privacy.

Table 90 shows the comparison between the pre-teaching survey and post-teaching survey results of Question P103 ('Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access rights to the information on your mobile devices'?).

Across the four teaching rounds significant changes were observed in the behaviour and attitude of students before and after the lesson. Table 91 indicates that more students would read the terms and conditions clearly or ensure that they understand an app's access rights to the information on their mobile devices when installing an app. For ER1 students, the behaviour increased from 10% to 29%. For ER2 students, it increased from 16.7% to 26.7%. However, for ER3, it decreased from 46.4% to 25%. Regarding the considerations before installing an app, the terms and conditions attracted students' appeal more. Significant changes could be observed from ER2 and ER3, where it increased from 3.3% to 20% and from 7.1% to 17.9%, respectively.

Table 92 shows a significant incremental change ER2 and ER3. In ER2, the installation rate of security software grew from 10% to 23.3%, while in ER3, the installation rate grew from 17.95% to 25%. However, in ER1, the rate dropped from 54.5% to 38.2%. As shown in Table 93, all remaining rounds have shown a significant growth in the knowledge of the actions taken by apps. Originally, many students believed that convenience was very important for them. After the lesson, this rate dropped significantly.

In particular, in ER3, it dropped from 25% to 7.1%. By contrast, privacy became a more important consideration for students, as shown in Table 94.

Table 90: P103 - Changes in the Attitude of Students in the Four Iterations

	FR_Pre		FR_Post		% change	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% change	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Yes	4	12.1	11	32.4	+20	3	10.0	9	29.0	+19	5	16.7	8	26.7	+10	13	46.4	7	25.0	-21.4
No	14	42.4	10	29.4	-13	18	60.0	8	25.8	-34.2	19	63.3	10	33.3	-30	8	28.6	9	32.1	+3.5
I do for some of the apps, but not for all.	15	45.5	13	38.2	-7	9	30.0	14	45.2	+15.2	6	20.0	12	40.0	+20	7	25.0	12	42.9	+17.9
Total	33	100.0	34	100.0	0	30	100.0	31	100.0	0	30	100.0	30	100.0	0	28	100.0	28	100.0	0

Table 91: Comparison of the Pre-teaching Survey and Post-teaching survey results of Question P104 ('What will you consider when you install an app'?)

	FR_Pre	FR_Post	% change	ER1_Pre	ER1_Post	% change	ER2_Pre	ER2_Post	% change	ER3_Pre	ER3_Post	% change
Convenience	54.5%	38.2%	-16.30%	53.3%	48.4%	-4.90%	46.7%	43.3%	-20.00%	32.1%	25%	-7.10%
Privacy policy	6.1%	47.1%	+41.00%	23.3%	22.6%	-0.70%	16.7%	26.7%	+3.30%	21.4%	28.6%	+7.20%
Terms and conditions	9.1%	23.5%	+14.40%	10.0%	12.9%	+2.90%	3.3%	20%	-3.30%	7.1%	17.9%	+10.80%

Table 92: Comparison of the Pre-teaching Survey and Post-teaching Survey Results of Question P106

(‘What is/are the protective actions taken’?)

	FR_Pre	FR_Post	% change	ER1_Pre	ER1_Post	% change	ER2_Pre	ER2_Post	% change	ER3_Pre	ER3_Post	% change
Install anti-virus software	9.1%	23.5%	+14.40%	54.5%	38.2%	-16.30%	10%	23.3%	+13.3%	17.95	25%	+7%

Table 93: Comparison of the Pre-teaching Survey and Post-teaching Survey results of Question P111

(‘Do you know that some apps will take actions that they have not mentioned they would’?)

	FR_Pre		FR_Post		% change	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% change	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Yes	19	57.6	27	79.4	+21.80%	19	63.3	25	80.6	+17.3	19	63.3	23	76.7	+13.4	18	64.3	19	67.9	+3.6

Table 94: Comparison of the Pre-teaching Survey and Post-teaching Survey Results of Question P113 (‘Convenience is important to you’.)

	FR_Pre		FR_Post		% change	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% change	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Very important	11	33.3	4	11.8	-21.50	11	36.7	6	19.4	-17.3	7	23.3	9	30.0	+6.7	7	25.0	2	7.1	-17.9
Important	16	48.5	20	58.8	+10.30	16	53.3	12	38.7	-14.6	19	63.3	10	33.3	-30	10	35.7	12	42.9	+7.2
Moderately important	4	12.1	5	14.7	+2.60	2	6.7	7	22.6	+15.9	4	13.3	4	13.3	0	6	21.4	10	35.7	+14.3
Slightly important	2	6.1	4	11.8	+5.70	1	3.3	6	19.4	+16.1			7	23.3	+23.3	4	14.3	4	14.3	0
Not important	0	0.0	1	2.9	+2.90					0					0					
Missing	33	100.0	34	100.0	0.00					0					0	1	100			
Total	11	33.3	4	11.8	-21.50	30	100.0	31	100.0	0	30	100.0	30	100.0	0	28	100.0	28	100.0	0

Table 95: Comparison of the Pre-teaching Survey and Post-teaching Survey Results of Question P114 (‘Privacy is important to you’.)

	FR_Pre		FR_Post		% change	ER1_Pre		ER1_Post		% change	ER2_Pre		ER2_Post		% change	ER3_Pre		ER3_Post		% change
	Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%		Freq.	%	Freq.	%	
Very important	12	36.4	9	26.5	-10	7	23.3	10	32.3	+9.00	12	40.0	8	26.7	-13.30	6	21.4	3	10.7	-10.70
Important	15	45.5	15	44.1	-1	16	53.3	9	29.0	-24.30	15	50.0	13	43.3	-6.70	10	35.7	9	32.1	-3.60
Moderately important	4	12.1	6	17.6	+6	5	16.7	7	22.6	+5.90	3	10.0	3	10.0	0.00	8	28.6	13	46.4	+17.80
Slightly important	1	3.0	3	8.8	+6	2	6.7	4	12.9	+6.20			4	13.3	+13.30	3	10.7	3	10.7	0.00
Not important	1	3.0	1	2.9	0			1	3.2	+3.20			2	6.7	+6.70					0
Missing	33	100.0	34	100.0												1	3.6			
Total	12	36.4	9	26.5	-10	30	100	31	100	0.00	30	100	30	100	0.00	28	100	28	100	0.00

Table 96 exhibits students' attitudes towards data privacy on their mobile devices. Questions P201, P202, P203 and P204 were concerned with the possibility of students' information stored on their mobile devices being misused by others. For the Foundation Round pre-teaching survey, the mean five-point Likert scale scores of these questions were all below 1.6, ranging from 1.44 to 1.59, where 5 represents 'not concerned at all' and 1 represents 'absolutely concerned'; whereas that of the post-teaching survey were all below 1.5, ranging from 1.18 to 1.44. This finding indicated that the foundation round students' concerns about their information being misused by others slightly increased after the foundation round. As for ER1, ER2 and ER3, no significant difference between the mean five-point Likert scale scores of these questions of the pre- and post-teaching surveys was observed.

The results of Questions P206, P207, D09 and P209 reflected students' perception of app developers. In the Foundation Round, Enhancement Round 1 and Enhancement Round 3 pre-teaching surveys, the mean five-point Likert scale scores of these questions ranged from 1.30 to 2.10, where 5 represents 'strongly agree' and 1 represents 'strongly disagree', whereas that of the post-teaching surveys ranged from 1.39 to 1.80. This finding indicated that students from the Foundation Round to Enhancement Round 3 did not show significant change in their perception of app developers after the lesson. However, in Enhancement Round 3, the mean five-point Likert scale scores of P206 and P208, which asked students whether they trust to app developers, decreased (P206: mean pre-teaching survey score: 1.75 with S.D. 0.701; mean post-teaching survey score: 2.07 with S.D. 0.766; P208: mean pre-teaching survey score: 1.86 with S.D. 0.887; mean post-teaching survey score: 2.19 with S.D. 0.879.) These figures reflected that ER3 students slightly agreed that app developers were trustworthy and keep their customers' best interests in mind.

The results of Questions P212 to P217 reflected students' attitude towards providing information such as HKID number, full name and phone numbers via their mobile devices. In the Foundation Round and Enhancement Round 2 pre-teaching surveys, the mean five-point Likert scale scores of these questions ranged from 1.63 to 2.76, where 5 represents 'strongly agree' and 1 represents 'strongly disagree', whereas that of the post-teaching surveys ranged from 2.19 to 2.87. This finding indicated that Foundation Round and Enhancement Round 3 students slightly changed their attitude towards providing information after the lesson. However, in Foundation Round and Enhancement Round 3, the mean five-point Likert scale scores of these questions ranged from 2.03 to 2.70, whereas that of the post-teaching surveys ranged from 1.90 to 2.73. This finding indicated that Foundation Round and Enhancement Round 3 students had no significant change in their attitude on providing information after the lesson.

The results of Questions P220, P221 and P222 exhibited students' practice and knowledge of protecting their privacy on their mobile devices. For the Foundation Round and Enhancement Round 2 pre-teaching surveys, the mean five-point Likert scale scores of these questions ranged from 1.93 to 2.67, where 5 represents 'strongly agree' and 1 represents 'strongly disagree', whereas that of the post-teaching surveys ranged from 2.13 to 2.91. This finding indicated that in Foundation Round and Enhancement Round 2, students showed a slight change in their practice and knowledge of protecting their privacy. However, in Foundation Round and Enhancement Round 3, the mean five-point

Likert scale scores of these questions of the pre-teaching surveys ranged from 1.36 to 2.86, whereas that of the post-teaching surveys ranged from 1.68 to 2.61. This finding indicated that students in the Foundation Round and Enhancement Round 3 did not have significant changes in their attitude towards providing information after the lesson.

Table 96: Comparison of the Pre-teaching Survey and Post-teaching Survey Result of Part 2

	FR_Pre (N = 32, Missing = 1)		**FR_Post** (N = 34, Missing = 1)		**t-test**	**ER1_Pre** (N = 30, Missing = 0)		**ER1_Post** (N = 31, Missing = 0)		**t-test**	**ER2_Pre** (N = 30, Missing = 0)		**ER2_Post** (N = 30, Missing = 0)		**t-test**	**ER3_Pre** (N = 28, Missing = 0)		**ER3_Post** (N = 28, Missing = 0)		**t-test**
	Mean	SD.	Mean	SD.	Sig.*	Mean	SD.	Mean	SD.	Sig. *	Mean	SD.	Mean	SD.	Sig. *	Mean	SD.	Mean	SD.	Sig. *
P201	1.59	0.837	1.44	0.860	0.468	1.57	0.679	1.71	0.643	0.401	1.50	0.731	1.33	0.802	0.404	1.36	0.870	1.68	1.056	0.657
P202	1.44	1.134	1.26	0.710	0.465	1.30	0.877	1.48	0.962	0.439	1.03	0.928	1.2	0.805	0.460	2.07	0.813	1.82	0.612	0.689
P203	1.56	1.162	1.24	0.819	0.194	1.43	0.898	1.32	0.909	0.634	1.37	0.890	1.13	0.681	0.259	2.14	0.756	2.00	0.770	0.919
P204	1.62	1.008	1.18	0.758	**0.047**	1.13	0.629	1.39	0.715	0.147	1.17	0.791	1.23	0.679	0.727	2.04	0.693	2.00	0.816	0.544
P205	1.18	0.882	1.29	1.06	0.639	1.20	0.887	1.23	0.762	0.903	0.90	0.845	1.23	0.858	0.135	2.07	0.813	1.86	0.970	0.219
P206	1.58	0.867	1.68	0.976	0.657	1.83	0.592	1.48	0.677	**0.036**	1.50	0.861	1.57	0.898	0.770	1.75	0.701	2.07	0.766	0.199
P207	1.76	1.001	1.74	0.994	0.927	2.10	0.845	1.65	0.709	**0.026**	1.70	0.837	1.80	1.157	0.703	2.11	0.737	2.00	0.816	0.487
P208	1.58	1.062	1.76	0.955	0.446	2.03	0.928	1.71	0.739	0.137	1.53	0.86	1.60	0.855	0.764	1.86	0.591	2.19	0.879	0.861
P209	1.47	0.879	1.56	0.960	0.693	1.30	0.837	1.39	0.882	0.694	1.27	0.691	1.40	0.855	0.509	2.25	0.887	2.43	0.879	0.374
P210	1.73	0.839	1.88	1.038	0.504	1.83	0.747	1.81	0.749	0.889	1.63	0.718	1.70	0.837	0.742	2.43	0.879	2.50	0.923	0.107
P211	2.09	1.071	1.88	0.946	0.401	2.07	0.828	1.74	0.815	0.128	1.77	0.935	1.70	0.794	0.767	1.96	0.881	2.29	1.013	0.608
P212	2.21	0.857	2.47	0.992	0.259	2.27	0.868	2.19	0.910	0.749	1.93	0.961	2.20	0.925	0.278	2.18	0.772	2.50	0.923	0.112
P213	2.55	1.063	2.82	0.968	0.267	2.70	0.915	2.52	0.926	0.439	2.20	1.064	2.70	1.088	0.077	2.14	0.891	2.18	0.772	0.453
P214	2.76	1.001	2.85	1.019	0.701	2.67	1.028	2.73	0.944	0.795	2.50	0.974	2.87	0.900	0.135	2.11	0.832	2.39	0.786	0.768
P215	2.03	1.045	2.56	0.991	**0.037**	2.23	0.817	2.03	0.875	0.358	1.63	0.890	2.50	0.900	**0.000**	2.21	0.738	2.39	0.737	0.211
P216	2.18	1.103	2.50	1.052	0.231	2.13	0.860	2.10	0.944	0.875	1.83	0.950	2.47	0.900	**0.010**	2.64	0.678	2.57	0.790	0.163
P217	2.19	0.859	2.56	0.894	0.091	2.03	0.865	1.90	0.831	0.551	1.93	0.828	2.50	0.777	**0.008**	2.32	0.723	2.50	0.694	0.873
P218	2.22	0.870	2.82	0.626	**0.002**	2.31	0.850	2.19	0.873	0.602	2.10	0.96	2.70	0.702	**0.008**	2.29	0.763	2.18	0.723	0.192

	FR_Pre (N = 32, Missing = 1)		**FR_Post** (N = 34, Missing = 1)		**t-test**	**ER1_Pre** (N = 30, Missing = 0)		**ER1_Post** (N = 31, Missing = 0)		**t-test**	**ER2_Pre** (N = 30, Missing = 0)		**ER2_Post** (N = 30, Missing = 0)		**t-test**	**ER3_Pre** (N = 28, Missing = 0)		**ER3_Post** (N = 28, Missing = 0)		**t-test**
	Mean	SD.	Mean	SD.	Sig.*	Mean	SD.	Mean	SD.	Sig. *	Mean	SD.	Mean	SD.	Sig. *	Mean	SD.	Mean	SD.	Sig. *
P220	2.3	0.770	2.32	0.912	0.921	2.00	0.845	1.90	0.79	0.648	1.93	0.785	2.13	0.819	0.338	1.36	0.870	1.68	1.056	0.369
P221	2.67	0.816	2.91	0.793	0.217	2.86	0.639	2.61	0.761	0.176	2.57	0.898	2.83	0.791	0.227	2.07	0.813	1.82	0.612	0.718
P222	2.18	0.917	2.50	0.788	0.132	2.07	0.868	2.06	0.772	0.992	2.03	0.809	2.40	0.814	0.085	2.14	0.756	2.00	0.770	0.350
P219	1.88	0.927	1.44	0.890	0.113	1.90	0.759	1.71	0.763	0.245	1.50	0.858	1.33	0.858	**0.004**	1.36	0.693	1.68	0.816	0.592

$p < 0.05$

Summary of Survey Part 2's Findings [To Answer RQ2]

To show the level of privacy concern of students, the study classified the six groups according to the mean and S.D. of the teaching rounds. Students with lower mean scores were categorised as 'unconcerned', whereas those with higher mean scores were grouped under 'extremely concerned'. Table 87 shows the levels of the privacy concern of students. Figure 28, 29, 30 and 31 display the percentage of students in each level of privacy concern. Figures 28 to 31 reflect that the percentage of privacy concern level increased.

Figure 28 FR students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 2]

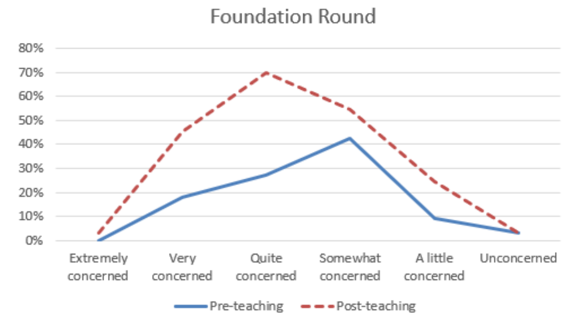


Figure 29 ER1 students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 2]

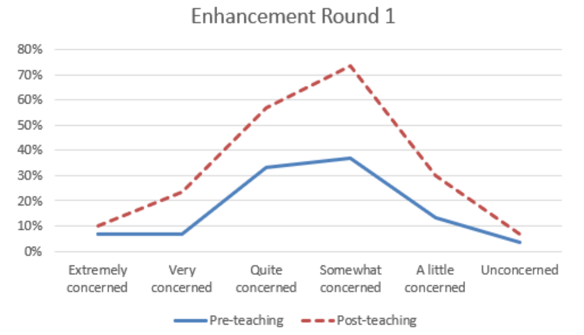


Figure 30 ER2 students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 2]

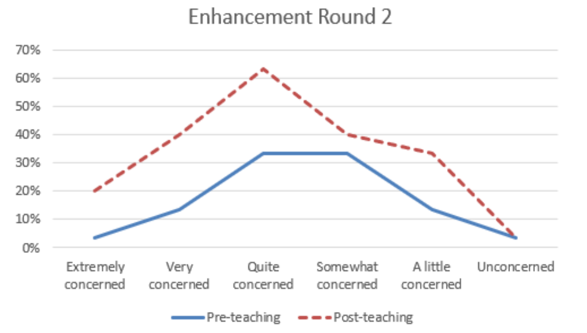


Figure 31 ER3 students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 2]

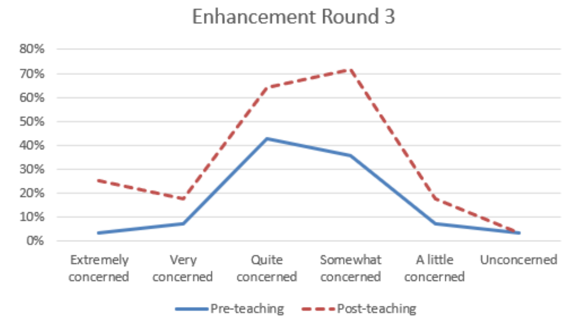


Table 97: Students' Level of Privacy Concern Before and After the Lesson [Survey Part 2]

Level of Privacy Concern	Foundation Round			Enhancement Round 1			Enhancement Round 2			Enhancement Round 3		
	Pre-teaching	Post-teaching	**Diff.**	Pre-teaching	Post-teaching	**Diff.**	Pre-teaching	Post-teaching	**Diff.**	Pre-teaching	Post-teaching	**Diff.**
Extremely concerned	0%	3%	**+3%**	7%	3%	**-3%**	3%	17%	**+13%**	4%	21%	**+18%**
Very concerned	18%	27%	**+9%**	7%	17%	**+10%**	13%	27%	**+13%**	7%	11%	**+4%**
Quite concerned	27%	42%	**+15%**	33%	23%	**-10%**	33%	30%	**-3%**	43%	21%	**-21%**
Somewhat concerned	42%	12%	**-30%**	37%	37%	**0%**	33%	7%	**-27%**	36%	36%	**0%**
A little concerned	9%	15%	**+6%**	13%	17%	**+3%**	13%	20%	**+7%**	7%	11%	**+4%**
Unconcerned	3%	0%	**-3%**	3%	3%	**0%**	3%	0%	**-3%**	4%	0%	**-4%**

The above figures and table show the levels of privacy concern of students in all teaching rounds before and after the lesson. After the privacy lessons, all teaching rounds except Enhancement Round 1 had positive effects in terms of privacy concern, and Foundation Round shows the most prominent improvement. More students in Foundation Round were 'extremely concerned' (+3%), 'very concerned' (+9%) and 'quite concerned' (+15%), which account for a total of +27%. This result implied that Foundation Round students had a higher degree of privacy concern after the privacy lesson. However, ER1 had a negative improvement ('extremely concerned' (−3%), 'very concerned' (+10%) and 'quite concerned' (−10%), which account for a total of −3% after teaching. In conclusion, on the basis of survey part 2's result, the privacy lesson had a positive impact in all teaching rounds except in Enhancement Round 1. The Foundation Round class showed a significant improvement in terms of OPA.

Table 98 shows the results of the OPMS of students in all teaching rounds. In Table 98, the results of Questions P301, P302, P303 and P304 from the pre- and post-teaching surveys exhibited students' perceptions of their boundary rules and control of private information on their mobile devices. In the pre-teaching surveys of all teaching rounds, the mean five-point Likert scale scores of these questions ranged from 2.13 to 2.68, where 5 represents 'strongly agree' and 1 represents 'strongly disagree', whereas that in the post-teaching surveys ranged from 2.29 to 2.82. This finding indicated that Foundation Round to Enhancement Round 3 students agreed slightly more with the boundary rules and control of private information after the lesson.

The results of Questions P305 to P313 in the pre- and post-teaching surveys indicated students' boundary rules and control of their private information stored on their SNS. In the pre-teaching surveys of all teaching round, the mean scores of these questions ranged from 2.09 to 2.78 in the Foundation Round, from 2.00 to 3.13 in ER1, from 2.37 to 3.27 in ER2 and from 2.12 to 2.62 in ER3. By comparison, that in the post-teaching surveys ranged from 2.15 to 3.15 in the Foundation Round, from 2.17 to 3.17 in ER1, from 2.07 to 3.24 in ER2 and from 2.27 to 2.85 in ER3. This finding indicated that Foundation Round to Enhancement Round 3 students agreed slightly more with the boundary rules and control of private information stored on their SNS after the lesson.

The results of Questions P314 and P315 in the pre- and post-teaching surveys indicated students' boundary rules and control of their private information on their IM accounts. In the pre-teaching surveys of all teaching round, the mean scores of these questions ranged from 2.50 to 2.84 in Foundation Round, from 2.57 to 2.83 in ER1, from 2.63 to 3.03 in

ER2 and from 2.58 to 2.85 in ER3. By comparison, that in the post-teaching surveys ranged from 2.79 to 2.97 in the Foundation Round, from 2.39 to 3.00 in ER1, from 2.80 to 2.97 in ER2 and from 2.54 to 2.92 in ER3. This finding indicated that Foundation Round to Enhancement Round 3 students agreed slightly more with the boundary rules and control of private information stored on their IM accounts after the lesson.

After the privacy lessons of Foundation Round to Enhancement Round 3, students agreed slightly more with the boundary rules and control of private information, which represented stage 2 of CPM theory. Therefore, Stage 2 of CPM theory effectively improved students' OPMS in all teaching rounds.

Table 98: Comparison of the Pre-teaching Survey and Post-teaching Survey Result in Part 3

	FR_Pre (N = 32, Missing = 1)		FR _Post (N = 34, Missing = 1)		t-test	ER1_Pre (N = 30, Missing = 0)		ER1_Post (N = 30, Missing = 0)		t-test	ER2_Pre (N = 30, Missing = 0)		ER2_Post (N = 29, Missing = 1)		t-test	ER3_Pre (N = 28, Missing = 0)		ER3_Post (N = 28, Missing = 0)		t-test
	Mean	SD.	Mean	SD.	Sig.*	Mean	SD.	Mean	SD.	Sig.*	Mean	SD.	Mean	SD.	Sig.*	Mean	SD.	Mean	SD.	Sig.*
P301	2.52	0.619	2.50	0.929	0.937	2.37	0.765	2.71	0.643	0.062	2.43	0.728	2.33	0.802	0.615	2.57	0.634	2.54	0.693	0.841
P302	2.58	0.614	2.29	0.871	0.131	2.37	0.89	2.48	0.724	0.574	2.60	0.77	2.23	1.04	0.127	2.57	0.634	2.54	0.637	0.834
P303	2.27	0.839	2.29	1.031	0.926	2.13	0.937	2.29	0.864	0.499	2.00	0.91	2.17	0.986	0.499	2.46	0.693	2.46	0.744	1.000
P304	2.42	0.830	2.82	0.576	0.026	2.63	0.89	2.65	0.755	0.955	2.50	0.777	2.60	0.968	0.661	2.68	0.819	2.39	0.832	0.201
P305	2.47	0.718	2.41	0.925	0.731	2.33	0.711	2.17	0.95	0.065	2.69	0.66	2.10	1.047	0.413	2.62	0.571	2.31	0.618	0.068
P306	2.62	0.751	2.41	0.857	0.002	2.47	0.9	2.47	0.86	0.000	2.43	1.04	2.62	0.862	0.001	2.48	0.714	2.65	0.629	0.360
P307	2.78	0.792	2.85	0.712	0.009	2.97	0.615	2.93	0.64	0.000	2.97	0.765	2.90	0.817	0.000	2.60	0.707	2.85	0.784	0.245
P308	2.78	0.659	2.88	0.686	0.938	3.03	0.669	2.93	0.691	0.131	3.00	0.587	2.90	0.772	0.549	2.64	0.907	2.73	0.874	0.718
P309	2.44	0.801	2.53	0.706	0.537	2.43	0.774	2.67	0.661	0.436	2.37	0.89	2.52	0.911	0.523	2.60	0.866	2.46	0.647	0.520
P310	2.94	0.759	3.15	0.500	0.000	3.13	0.571	3.17	0.461	0.000	3.27	0.691	3.24	0.636	0.000	2.36	0.952	2.69	0.788	0.180
P311	2.09	0.928	2.15	1.105	0.001	2.00	0.743	2.13	0.73	0.091	2.00	0.871	2.07	0.998	0.001	2.00	0.834	2.27	0.667	0.212
P312	2.78	0.608	2.79	0.687	0.953	2.83	0.592	2.77	0.679	0.875	2.83	0.648	2.90	0.724	0.852	2.28	0.891	2.81	0.801	0.031
P313	2.53	0.718	2.56	0.786	0.014	2.33	0.922	2.27	0.868	0.002	2.30	0.952	2.52	0.911	0.003	2.12	0.881	2.42	0.643	0.166
P314	2.72	0.888	2.79	0.902	0.000	2.83	0.913	2.86	0.789	0.000	2.63	0.928	2.87	0.73	0.000	2.65	0.936	2.67	0.816	0.959
P315	2.84	0.628	2.97	0.626	0.000	2.77	0.971	3.00	0.655	0.000	3.03	0.718	2.97	0.669	0.000	2.85	0.784	2.92	0.654	0.733

$p < 0.05$

In Table 98, the P-values for the two-tail analysis, which are lower than our alpha level of significance ($P<0.05$), are highlighted. Therefore, we rejected the null hypothesis due to differences in the pre- and post-teaching surveys. Students' boundary rules and control of private information on mobile devices demonstrated changes in the Foundation Round, Enhancement Round 1 and Enhancement Round 2.

Table 99: Cross-tabulation Analysis Summary of the Answers for RQ2

			Pre-teaching survey				**Post-teaching survey**			
Online Privacy Attitude (OPA)	**vs**	**Online Privacy Management Strategies (OPMS)**	FR	ER1	ER2	ER3	FR	ER1	ER2	ER3
			(33)	(31)	(33)	(28)	(34)	(32)	(34)	(28)
P220: I have a good habit of protecting my privacy on my mobile device(s).	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.255	0.255	0.034	0.088	0.000	0.029	0.013	0.212
			N	N	S	N	S	S	S	N
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.043	0.057	0.057	0.560	0.001	0.133	0.006	0.232
			S	N	N	N	S	N	S	N
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.210	0.005	0.86	0.455	0.005	0.705	0.068	0.326
			N	S	N	N	S	N	N	N
P301: I feel that I can keep all my private information in a way that I feel is acceptable.	vs	**P302:** I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly.	0.001	0.149	0.149	0.000	0.001	0.422	0.054	0.092
			S	N	N	S	S	N	N	N
	vs	**P303:** I have checked and modified the privacy settings of my mobile device(s).	0.002	0.654	0.654	0.009	0.005	0.327	0.156	0.305
			S	N	N	S	S	N	N	N
	vs	**P304:** If the information stored on my mobile devices looks too private, then I will delete it.	0.001	0.001	0.444	0.228	0.222	0.053	0.196	0.24
			S	S	N	N	N	N	N	N

**$p < 0.05$

* S – ‘significant change’, N – ‘no significant change’

In Table 99, two OPAs (P220, P301) vs. three OPMS (P302, P303, P304), for a total of six cross-tabulation combinations, were under study in the four teaching rounds, comparing the pre-teaching and post-teaching surveys. Table 99 shows the results, where S represents 'significant change' and N represents 'no significant change'.

The post-teaching survey indicated three significant changes in the three teachings in the Foundation Round, the Enhancement Round 1 and the Enhancement Round 2 in the combination of P220 ('I have a good habit of protecting my privacy on my mobile device[s]'.) vs. P302 ('I have well managed the apps that I have installed on my mobile device(s), such as deleting unused apps or updating them regularly'.). The result suggested that students had significant change in OPA vs. OPMS.

However, no significant changes were observed in all teaching sessions in the post-teaching survey on crosstab P301 ('I feel that I can keep all my private information in a way that I feel is acceptable'.) vs. P304 ('If the information stored on my mobile devices looks too private, then I will delete it'.).

Overall, the findings indicated four clear improvements from no significant change to significant change in P220 vs. P302 in the Foundation Round and Enhancement Round 1, in P220 vs. P303 ('I have checked and modified the privacy settings of my mobile device[s]'.) in Enhancement Round 1 and in P220 vs. P304 ('If the information stored on my mobile devices looks too private, then I will delete it.) in the Foundation Round.

Therefore, the Foundation Round had obvious improvement in the OPA vs. OPMS, whereas the three enhancement rounds did not. The privacy paradox could explain the cross-tabulation results of the three enhancement rounds. This finding exhibited that OPA did not affect OPMS especially in the enhancement rounds.

Summary of Survey Part 3's Findings [To Answer RQ2]

In survey part 3, the questions asked participating students about their boundary rules and control of private information on their mobile devices. This part presented the change in students' OPMS. The comparison between the pre-teaching survey and post-teaching survey results from part 3 is shown in the following figures and table. Students with lower mean scores were categorised as 'unconcerned' whereas those with higher mean scores were categorised as 'extremely concerned'. Table 87 shows the levels of the privacy concern of students. Figures 32, 33, 34 and 35 display the percentage of students in each level of privacy concern for survey part 3. The figures reflect that students' level of privacy concern increased.

Figure 32 FR students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 3]

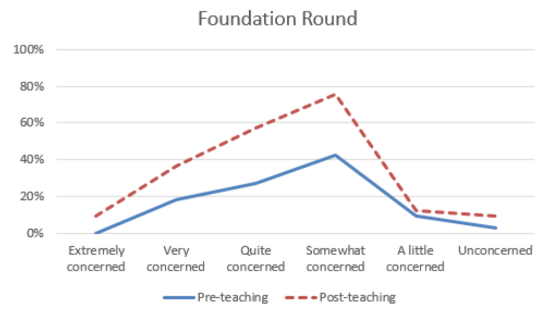


Figure 33 ER1 students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 3]

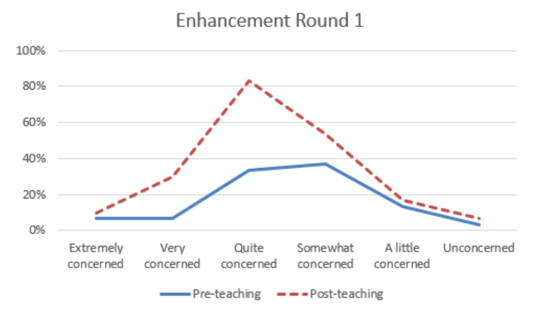


Figure 34 ER2 students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 3]

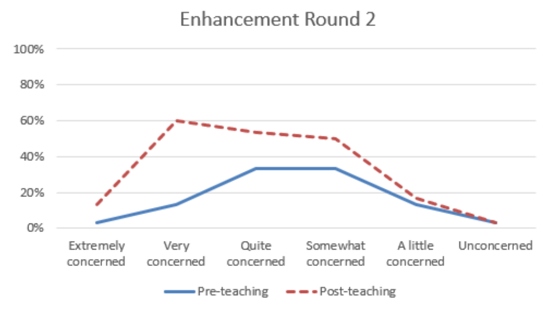


Figure 35 ER3 students - Pre- and Post-teaching Survey Results of Privacy Concern Levels [Survey Part 3]

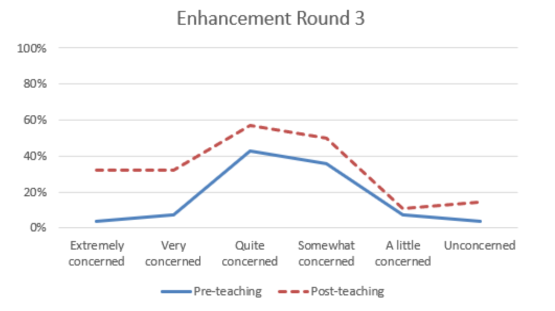


Table 100: Students' Level of Privacy Concern Before and After the Lessons

[Survey Part 3]

Level of Privacy Concern	Foundation Round			Enhancement Round 1			Enhancement Round 2			Enhancement Round 3		
	Pre-teaching	Post-teaching	**Diff.**	Pre-teaching	Post-teaching	**Diff.**	Pre-teaching	Post-teaching	**Diff.**	Pre-teaching	Post-teaching	**Diff.**
Extremely concerned	0%	9%	**+9%**	7%	3%	**-4%**	3%	10%	**+7%**	4%	30%	**+26%**
Very concerned	18%	18%	**0%**	7%	23%	**+16%**	13%	47%	**+34%**	7%	26%	**+19%**
Quite concerned	27%	30%	**+3%**	33%	50%	**+17%**	33%	20%	**-13%**	43%	17%	**-26%**
Somewhat concerned	42%	33%	**-9%**	37%	17%	**-20%**	33%	17%	**-16%**	36%	16%	**-20%**
A little concerned	9%	3%	**-6%**	13%	3%	**-7%**	13%	3%	**-10%**	7%	7%	**0%**
Unconcerned	3%	6%	**-3%**	3%	3%	**0%**	3%	0%	**-3%**	4%	4%	**0%**

After the lessons, all teaching rounds except Enhancement Round 1 had obvious effects in 'extremely concerned' (FR: +9%; ER2: +7%; ER3: +26.6%), and Enhancement Round 3 showed the most prominent effect. Survey part 3 comparison results were consistent with those of survey part 2.

After combining the two sets of results, Foundation Round and Enhancement Round 3 had a greater improvement after the privacy lesson. Their OPA and OPMS increased significantly.

6.3 Key Findings to Answer RQ3 (Pedagogical Model)

The pedagogical model has been modified in each iteration according to the result of the student assignments, the pre- and post-teaching survey, the post-teaching interview and the teacher's observations.

Online assignments were given to students at the end of the lesson. The instructor and the second marker marked all student assignments of the four classes. Table 101 shows a comparison of the results of the assignments.

Table 101: Comparison of the Student Assignment Results

	Foundation Round	**Enhancement Round 1**	**Enhancement Round 2**	**Enhancement Round 3**
Mean	5.09	5.88	5.68	6.68
Standard Deviation	1.520	1.760	1.477	1.749

Enhancement Round 3 has a particularly high mean, which could be explained by the fact that the teacher had experienced the foundation round model (which shares the same approach); hence, the teacher conducted the lesson in a more effective way.

After each teaching round, the teacher had the following observations.

Table 102: Observations and Inspirations from All Teaching Rounds

Foundation Round	
Pedagogy	Case video
Student engagement	◎ The case teaching method could engage students during the lesson effectively, as students paid more attention in this method than in the direct teaching section. ◎ Students jotted down notes when they were watching the case study video.
Student discussion	Students actively discussed with their classmates when they were working on the assignments.
Student assessment	Students tackled the assignment questions well especially CPM-theory-related questions.
Instant student feedback	Some students responded that they had watched the online video during their secondary schooling. The case background was quite old.
Overall observation	◎ The instant responses of students showed that they enjoyed the lessons. The case studies were interesting, not monotonous and relevant to their daily life. ◎ Survey findings: FR Students became more concerned with privacy (Part 2: +3%; +9%) with better boundary rule and control in using their mobile devices (Part 3: +9%; 0%). ◎ Cross-tabulation findings: Obvious significant changes were found in OPA vs. OPMS.
Inspiration	Case video teaching was an exciting teaching method. It used two stories to discuss many useful privacy and security issues, which were closely related to the daily needs of students. This method could be hardly replaced by other methods. However, students reflected that the case background was quite old (5–6 years ago), and this impression may affect students' learning outcomes in other rounds.
Enhancement Round 1	
Pedagogy	Current Event
Student engagement	◎ Using current event could fairly engage students during the lesson. ◎ Students did not jot down notes when they were watching the current event.
Student discussion	Students did not have much discussion when they were working on the assignments.
Student assessment	Students tackled the assignment questions well.
Instant student feedback	Some students pointed that they had watched the current event article before.

Overall observation	◎ The instant responses of students showed that they did not enjoy the lessons, and the current event article did not appeal to them. ◎ Survey findings: Students’ privacy concern increased, but it was not better than in FR (Part 2: −3%; +10% and Part 3: −4%; +16%). ◎ Cross-tabulation findings: No obvious significant changes were found in OPA vs. OPMS.
Inspiration	Using current event teaching was not effective in this round. Although the current event about WhatsApp was new and close to the daily use of mobile device, this case did not appeal to students. Compared with the case video teaching in FR, this teaching method was unable to motivate students to learn. According to the findings of 6.2, ER1 students had no significant improvement on privacy attitude and positive effect on boundary rules and control of their private information on mobile devices. In the coming round, the case video teaching would be adopted again. The QRS was added to enhance their privacy concepts.
Enhancement Round 2	
Pedagogy	Case video teaching and QRS
Student engagement	◎ Students were supposed to finish the QRS questions after a small part of the content was taught. However, the instant teaching effects were not seen. Students did not want to follow this part of the activity. ◎ Students jotted down notes when they were watching the case studies videos.
Student discussion	Students did not have much discussion when they were working on the assignments.
Student assessment	Students tackled the assignment questions well.
Instant student feedback	Students thought that they could finish the QRS questions by the end of the lesson, so they did not follow the pace of the teacher.
Overall observation	◎ The teacher found that the Moodle QRS was not effectively used during the lesson. Students could not keep up with the teaching pace in this part, that is, direct teaching with Moodle QRS. ◎ Survey findings: Students’ privacy concern increased (Part 2: +13%; +13% & Part 3: +7%; +34%). ◎ Cross-tabulation findings: No obvious significant changes were found in OPA vs. OPMS.
Inspiration	Again, case video teaching was properly used, but Moodle QRS could not achieve the previous aims. According to the findings of 6.2, Enhancement Round 2 students had improvement on privacy attitude and positive

	effect on boundary rules and control of their private information on mobile devices.
Enhancement Round 3	
Pedagogy	Case video teaching
Student engagement	The case teaching method could engage students during the lesson in general, as students paid more attention in this method than in the direct teaching section. Students jotted down notes when they were watching the case studies video.
Student discussion	Students were willing to discuss with their classmates when they were working on the assignments.
Student assessment	Students tackled the assignment questions well. Students in this teaching round obtained the highest scores among the four classes.
Instant student feedback	Students found that the case video was useful, and they liked the artists in the video.
Overall observation	◎ The instant responses of students showed that they enjoyed the lessons. The case studies were interesting, not monotonous and relevant to their daily life. ◎ Survey findings: Students' privacy concerned increased significantly (Part 2: +18%; +4% & Part 3: +26%; +19%). ◎ Cross-tabulation findings: No obvious significant changes were found in OPA vs. OPMS.
Inspiration	The case video teaching was confirmed as the best teaching method, but the key to success was choosing an appropriate and quality video that was close to the daily needs of students.

Table 103 displays the achievements, problems that still needed to be solve and suggested solutions in each teaching round.

Table 103: Achievements, problems that still needed to be solved and suggested solutions in the four iterations

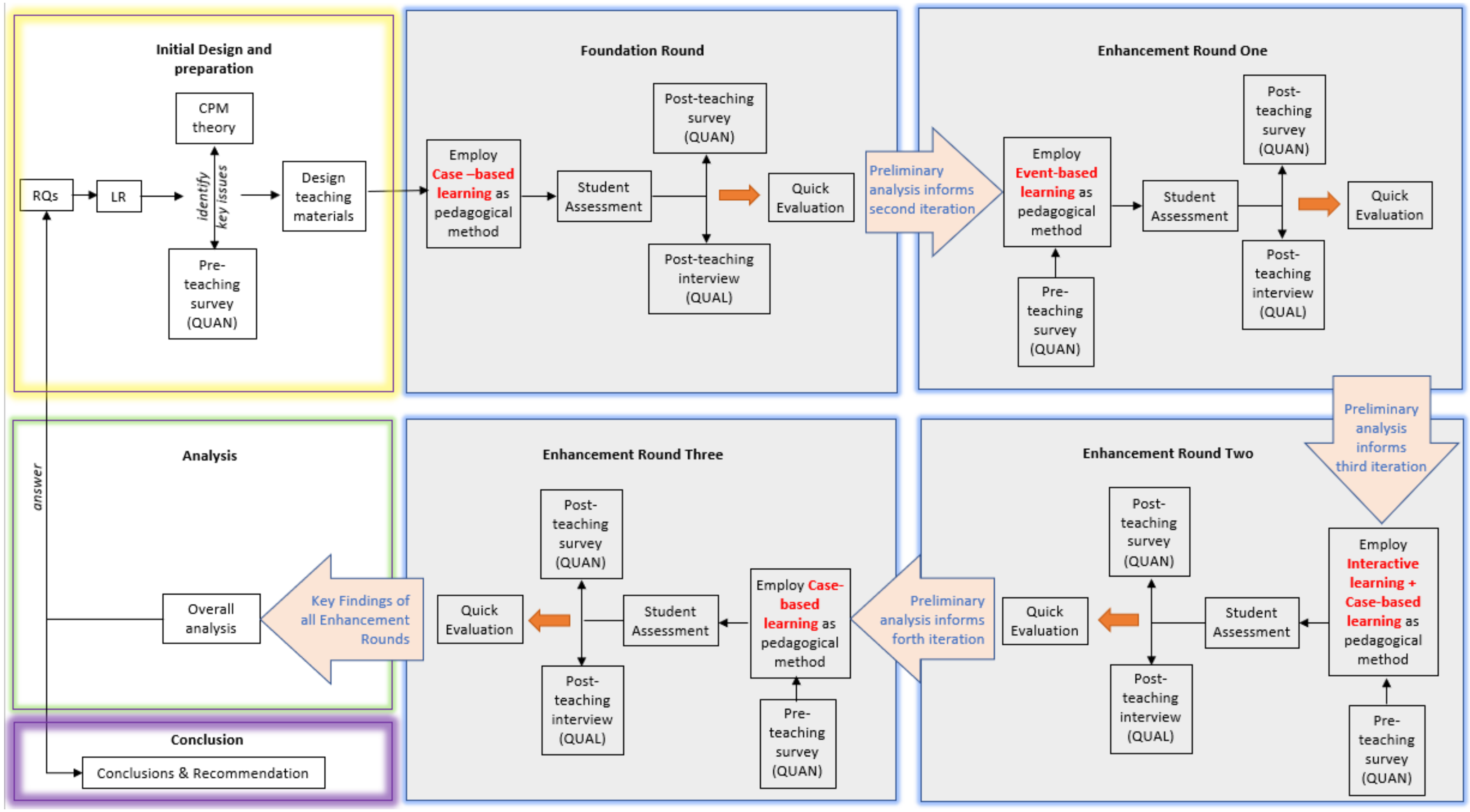
Foundation Round	Enhancement Round 1	Enhancement Round 2	Enhancement Round 3
Achievement ● FR Students became more concerned with privacy (Part 2: +3%; +9%) with better boundary rule and control in using their mobile devices (Part 3: +9%; 0%). ● FR students were attentive. ● FR students' responses shown in the post-teaching interview had positive impression. They rated the overall lesson. ● Obvious significant changes were observed in the OPA vs. OPMS cross-tab findings.	Achievement ● Students' privacy concerned became higher, but not better than in FR. (Part 2: -3%; +10% & Part 3: -4%; +16%) ● Teacher found that the current event chosen could not attract students' attention. ● In the post-teaching interview, students displayed they were not learned much in the current news, they felt that they would not make the mistakes found in the current event news.	Achievement ● Students' privacy concerned became higher (Part 2: +13%; +13% & Part 3: +7%; +34%). ● Teacher found that QRS was not very effectively used, while the case studies could attract students' attention. ● In the post-teaching interview, students showed that QRS was not very useful in learning the privacy concepts, they may not be able to follow the teaching pace of using QRS questions. However, they felt that the case studies video was useful to know more privacy issues of their daily life.	Achievement ● Students' privacy concerned increased significantly (Part 2: +18%; +4% & Part 3: +26%; +19%) ● Teacher found that they could learn from the video effectively and attentively. The average of their assignment scores was highest among all teaching rounds. ● In the post-teaching interview, they found the video was useful as several privacy cases that they could learn from them.
Problems that still needed to be solved ● Video was old but not outdated.	Problems that still needed to be solved ● As the current news could not motivate students effectively, teacher decided to modify the FR's pedagogical model. Therefore, the teacher added Quick Response Systems to improve students' learning process.	Problems that still needed to be solved ● QRS was not effectively used.	Conclusion ● The pedagogical model of FR was repeated in ER3, the result was obvious and encouraging. Students' privacy concern and boundary rule and control were improved.
How to tackle these problems in next round ● As the case study video was not new to FR students, the teacher selected current news for next teaching round. The news was recent and realistic.	How to tackle these problems in next round ● As the current news could not motivate the ER1 students effectively, teacher decided to modify the FR's pedagogical model, so as to add QRS to improve students' learning process.	How to tackle these problems in next round ● QRS was not effectively used, while case studies video was good enough for students to learn the concepts of privacy.	

Table 104: Pedagogical models for 4 teaching rounds

Session	Pedagogical Model			
1	Conduct pre-teaching survey (one week before the privacy lesson).			
2	Introduce the topic.			
3	Teach the basic concepts of online privacy management using presentation slides ◎ Section one: Malware related to online privacy ◎ Section two: Online privacy on mobile devices ◎ Section three: Six PCPD data protection principles ◎ Section four: Mobile apps permission details ◎ Section five: Online privacy management strategies – CPM theory			
	Foundation Round	**Enhancement Round 1**	**Enhancement Round 2**	**Enhancement Round 3**
4	**Case-based learning with online video** - Case one: Managing Andy's Facebook information - Case two: Managing Mr. Lau's private information, such as mobile phone number and medical records	**Event-based learning** - Latest news – Security breach in WhatsApp - WhatsApp settings - WhatsApp security controls	**Interactive classroom with QRS** Case-based learning with online video - Case one: Managing Andy's Facebook information - Case two: Managing Mr. Lau's private information such as mobile phone number and medical records	**Case-based learning with online video** - Case one: Managing Andy's Facebook information - Case two: Managing Mr. Lau's private information such as mobile phone number and medical records
5	Summarise the teaching contents.			
6	Complete online assignment of FR	Complete online assignment of ER1	Complete online assignment of ER2	Complete online assignment of ER3
7	Conduct post-teaching survey.			
8	Conduct post-teaching interview (volunteer students).			

As shown in Table 104, two cases were used in the foundation round. Enhancement Round 1 teaching adopted the discussion of ‘latest news – security breach in WhatsApp’. As in the Foundation Round, Enhancement Round 2 teaching adopted case studies, but it also included Moodle QRS. This inclusion aimed at confirming whether students learned effectively after the direct teaching part. Same as the foundation round, the last round adopted the relatively effective pedagogical model.

Figure 36: Flow of the Four Teaching Rounds (Four Iterations)


Initial Design and preparation
CPM theory
RQs
LR
identify key issues
Design teaching materials
Pre-teaching survey (QUAN)
Foundation Round
Employ Case –based learning as pedagogical method
Student Assessment
Post-teaching survey (QUAN)
Post-teaching interview (QUAL)
Quick Evaluation
Preliminary analysis informs second iteration
Enhancement Round One
Employ Event-based learning as pedagogical method
Pre-teaching survey (QUAN)
Student Assessment
Post-teaching survey (QUAN)
Post-teaching interview (QUAL)
Quick Evaluation
Preliminary analysis informs third iteration
Enhancement Round Two
Employ Interactive learning + Case-based learning as pedagogical method
Pre-teaching survey (QUAN)
Student Assessment
Post-teaching survey (QUAN)
Post-teaching interview (QUAL)
Quick Evaluation
Preliminary analysis informs forth iteration
Enhancement Round Three
Employ Case-based learning as pedagogical method
Pre-teaching survey (QUAN)
Student Assessment
Post-teaching survey (QUAN)
Post-teaching interview (QUAL)
Quick Evaluation
Key Findings of all Enhancement Rounds
Analysis
Overall analysis
answer
Conclusion
Conclusions & Recommendation

Chapter 7 Conclusion, Discussion and Recommendations

This chapter first recapitulates the aims, design and methodology of this study, and then encapsulates the research findings and implications and highlights the research contributions and recommendations. It also includes a discussion of the research limitations and future studies.

7.1 Recapitulation of the Research Aims, Research Questions and Research Approach

7.1.1 Research Aims

This research aimed to investigate the online privacy practice of Hong Kong higher education students when using their mobile devices and to develop their OPMS. It focused on investigating how they manage their private information as well as the personal information of other people when using their mobile devices. Growing up in an information age and a digital world, students of this generation are active users of mobile devices. Given that the online privacy concerns of students about the security of their mobile devices were low (PCPD, 2012), this research explored an effective pedagogical model to improve higher education students' OPMS of using mobile devices.

7.1.2 Research questions

This study aimed at exploring an effective pedagogical model of developing and improving higher education students' online privacy management strategies of mobile devices by using CPM theory. It was designed to inquire the online privacy practice of Hong Kong higher education students when using their mobile devices and to develop their OPMS. Besides, it focused on investigating how they manage their private information and the personal information of others. With reference to the purpose of this study and the literature review, the following research questions (RQ) were generated:

RQ 1: What are HEI students' online privacy attitudes of using mobile devices?

RQ 2: How effective is using CPM theory in improving HEI students' online privacy management strategies for their mobile devices?

RQ 3: What kinds of pedagogical models can effectively improve HEI students' online privacy management strategies for mobile devices?

7.1.3 Research Approach

In this study, DBR, which could effectively bridge the chasm between research and practice in formal education (Anderson & Terry, 2012; Alghamdi & Li, 2013), is used as a practical research methodology. DBR Collective (2003) argues that DBR, which combines empirical educational research with the theory-driven design of learning environments, is an important methodology for understanding how, when and why educational innovations work in practice. It cited Brown (1992) and Collins (1992) and reported that DBR is for the study of learning in context through the systematic design and study of instructional strategies and tools. It also argued that DBR helps develop knowledge regarding creating, enacting and supporting innovative learning environments. Besides, DBR is a popular paradigm used in education research (Anderson & Shattuck, 2012; Schmitz, Klemke, Walhout, & Specht, 2015).

Given that the mixed methods approach is able to maximise the validity and at the same time increase the objectivity and reliability of the current research, most DBR literature agree that the mixed methods approach is appropriate for collecting and analysing data (Alghamdi & Li, 2013; Bell, 2004; Design-Based Research Collective, 2003; Wang & Hannafin, 2005). Therefore, in the DBR methodology, qualitative and quantitative research methods were adopted to address the research questions (Bogdan & Biklen, 2006; Li & Chu, 2018; MacDonald, 2008).

This study adopted a mixed method research approach to collect qualitative and quantitative data, so as to triangulate the findings. Significant advantages were obtained by applying multiple methods to the study, such as the diminution of inappropriate certainty, in spite of an increased time cost (Robson, 1993).

In this study, quantitative and qualitative data were collected at the same time and then merged for comparison. Finally, the results were interpreted or explained for any discrepancy. The convergent parallel mixed methods design was employed.

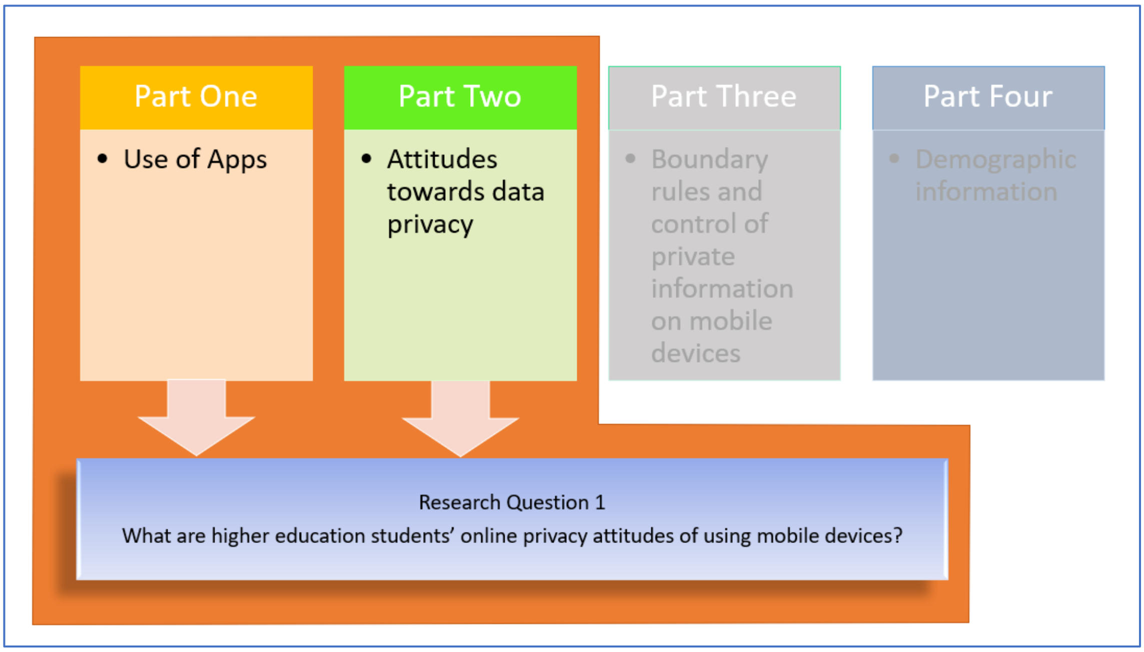
The present study conducted four research iterations. Each iteration involved one class and the collection of quantitative data from pre-teaching survey, post-teaching survey and the assignment and qualitative data from the interview of volunteer students. The quantitative data were analysed using the cross-tabulation, descriptive statistics and t-test functions of SPSS. The qualitative data were coded into positive, negative and other themes. Each theme was given a label, and the percentage of students contributing to the theme was calculated using NVIVO. The quantitative and qualitative data were compared and used to investigate the perception of students and the effectiveness of the teaching approach. According to these findings, the pedagogical model was adjusted and enhanced and then used in the second research iteration. The four stages of the research iteration were repeated, and so forth, following the steps shown in Figure 16.

7.2 Encapsulation the research findings and implications

7.2.1 Research question 1

The quantitative data from Part 1 were used to address Research Question 1: What are HEI students' online privacy attitudes of using mobile devices?

Figure 6. Relationship between the Survey and RQ 1


Part One
Use of Apps
Part Two
Attitudes towards data privacy
Part Three
Boundary rules and control of private information on mobile devices
Part Four
Demographic information
Research Question 1
What are higher education students' online privacy attitudes of using mobile devices?

The above figure shows the approach for addressing research question 1. Two parts of the pre-teaching survey were applied to investigate the issue in research question 1 regarding students' attitudes towards using mobile devices.

The first part of the pre-teaching survey was about the use of mobile devices. The pre-teaching survey was conducted in all four iterations. According to Table 83, students mainly used their mobile device for social networking and IM. Students in all teaching rounds used their mobile devices for similar purposes. Question P104 asked: What are your top considerations when deciding to install an app? However, students' responses in the four teaching rounds have high divergence. Moreover, privacy policy and the terms and conditions were not given much consideration. *'Functionality' and the 'Free or not' aspects of an app were more important considerations. This finding showed a consistency with the literature. Students in all teaching rounds had a similar level of knowledge about their information kept by others.*

The second part of the pre-teaching survey investigated students attitudes towards data privacy. Table 84 shows the result of this part; respondents were slightly concerned about their information stored in their mobile devices being misused by others. Students slightly disagreed that app developers were trustworthy and kept their promises and commitments. Moreover, students agreed that providing private information such as HKID number, full name and phone numbers was risky. Students thought that they had a good practice and good knowledge of the issue. *The findings in this table indicated that students considered protecting their privacy on their mobile devices important.*

According to Figures 24–27 and Table 88, students who were 'extremely concerned', 'very concerned' and 'quite concerned' with their online privacy were less than 50% in the first three teaching rounds. However, the total percentage of these three privacy concern categories was 55% in enhancement round 3. In general, enhancement round 3 students had a higher level of privacy concern when installing a mobile app.

In conclusion, mobile devices were heavily used in daily lives. Although HEI students thought they have a good habit of protecting their online privacy in their mobile devices, they did not possess a high sense of online privacy concern before the privacy lesson. *The following list summarises HEI students' online privacy attitude towards using mobile devices.*

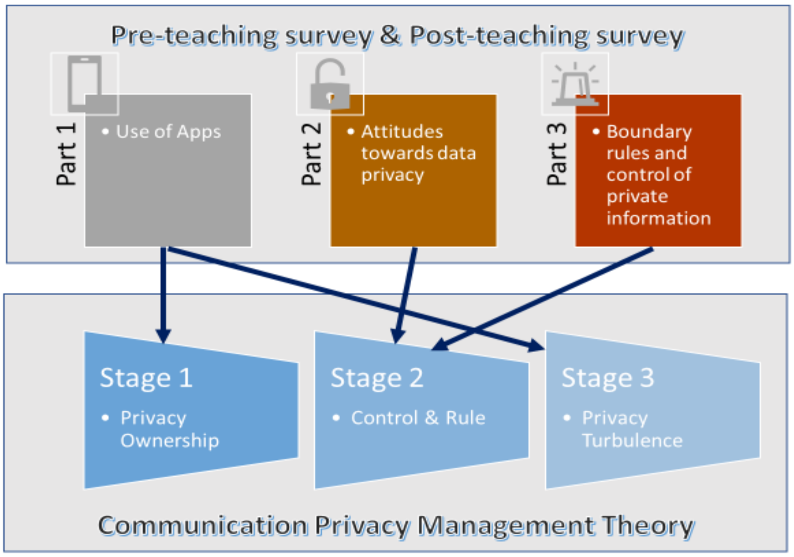
- *'Functionality' and 'free or not' were the more important aspects of a mobile app.*
- *HEI students had a good knowledge about their information kept by others.*
- *Protective measures, namely setting up auto screen lock and screen lock, were used by HEI students on their mobile devices. This practice reflected that students select the most convenient ways to protect their devices.*
- *The findings of all teaching rounds were consistent, yet contradictory. HEI students did not do much to protect their mobile devices, but at the same time, they admitted that their privacy is important. Research articles revealed the privacy paradox, and found that participants may claim that they are concerned about their privacy, but they were willing to sacrifice some of it in view of the convenience gained from Internet-connected devices such as mobile devices (Aleisa, Renaud, & Bongiovann, 2020; Barnes, 2006; Barth & de Jong, 2017). This confirms our previous findings and can explain this contradiction.*

7.2.2 Research question 2

Research Question 2 asked: How effective is using CPM theory in improving HEI students' OPMS for their mobile devices? The teaching materials were designed with reference to CPM theory. The results from the pre-teaching survey and the post-teaching survey were compared to answer this question.

CPM theory was composed of three stages. Stage 1 of CPM mentioned ownerships, in which people believed that they owned the information about themselves. Others became co-owners of people's private information. Students need to know what kinds of personal information, as well as what kinds of other people's personal information, they owned. Stage 2 refers to as 'Control and Rules', which describe that people develop boundaries to control their personal information. It mentioned that people share and withhold information according to a system of rules. Stage 3 of CPM theory referred to privacy turbulence, which describes when the rules stated in Stage 2 were not followed, mistakes were made, thus resulting in turbulence. The following diagram recaps the structure in addressing Research Question 2.

Figure 6: Survey Parts of Research Question 2


Pre-teaching survey & Post-teaching survey
Part 1
• Use of Apps
Part 2
• Attitudes towards data privacy
Part 3
• Boundary rules and control of private information
Stage 1
• Privacy Ownership
Stage 2
• Control & Rule
Stage 3
• Privacy Turbulence
Communication Privacy Management Theory

In Stage 1, privacy ownership, the findings are shown in Tables 82 and 83. With a low sense of privacy protection, HEI students stored numerous private information of their own as well as that of their friends, classmates and family members on their mobile devices. However, different groups exhibited, through different behaviour, the different types of information stored in their mobile devices. For example, foundation round students had a higher proportion of saving email addresses in their mobile devices, whereas enhancement round 1 students had a few personal and sensitive photos stored in their phones.

Stage 2 describes people developing boundaries so as to control their personal information. It mentions that people share and withhold information according to a system of rules. According to the findings of section 6.2, participants found themselves well managing and well keeping their private information stored on their mobile devices.

This finding indicated that all students in the four teaching rounds agreed slightly more with the boundary rules and control of private information after the lesson. Besides, students agreed slightly more with the boundary rules and control of private information stored on their SNS after the lesson. Finally, students in the Foundation Round to Enhancement Round 3 agreed slightly more with the boundary rules and control of private information stored on their IM accounts after the lesson.

In Table 99, the cross-tabulation analysis summary reflects a significant correlation between OPA and OPMS in the Foundation Round. However, no significant correlation was found between OPA and OPMS in the three enhancement rounds. Similar to the prior research articles, these contradictory findings confirmed that OPA was unrelated to OPMS.

According to the section 'Summary of Survey Part 2's Findings [To Answer RQ2]', Figure 28–31 and Table 97 display that all teaching classes except ER1 had positive effects in terms of privacy concern level, and Foundation Round students showed better improvement in their privacy attitude. In survey Part 3, based on the section 'Summary of Survey Part 3's Findings [To Answer RQ2]', the questions asked students about their boundary rules and control of their personal information on mobile devices, Figure 32–35 and Table 100 reflect that all teaching rounds except Enhancement Round 1 had significant effects in privacy concern level, and that in Enhancement Round 3 was evident. After merging survey Part 2 and Part 3 findings, Foundation Round and Enhancement

Round 3 showed significant improvement after the lesson. Privacy concern in developing boundaries so as to control their personal information increased significantly. Thus, students' OPMS were enhanced significantly.

Stage 3 focused on the privacy turbulence, which can be traced back to Part 1 of this survey regarding the use of apps. To address this stage, a scenario was given to students. 'Suppose that you are downloading an app on your mobile devices. After you have clicked to download, the app asks for access to your contacts' personal information (i.e. other people's personal information such as phone numbers) and sensitive photos'. The result was mixed.

The key reasons of students to continue downloading included: 'not easy for others to access personal info' and 'will only download popular app'. Some responses implied a low level of perceived risk, such as 'not really risky'. The utility of the app contributed a critical factor, such as 'useful' and 'the game is popular'. Those who cancelled the download considered privacy a higher cause of concern. Participating students responded that they found stage 3's idea not very useful in their daily life. As the overall result was mixed, HEI students had many considerations when downloading an app. Although privacy was a consideration, it was not the most important.

In conclusion, only Stage 1 and Stage 2 of CPM theory were effectively adopted to develop

HEI students' online privacy management strategies. For Stage 3 of CPM theory, the skills of handling HEI students' online privacy during privacy turbulence was not improved significantly. As such, CPM theory was partially effective on improving HEI students' online privacy management strategies for their mobile devices.

7.2.3 Research question 3

The last research question was: What kinds of pedagogical models can effectively improve higher education students' online privacy management strategies for mobile devices? This research question was tackled by comparing the pre- and post-teaching survey, student assignments, teacher's observation and the post-teaching interview.

As shown in Table 104, case video teaching was employed in the Foundation Round. Subsequently, Enhancement Round 1 adopted the discussion of 'latest news – security breach in WhatsApp'. However, similar to the Foundation Round, Enhancement Round 2 teaching adopted case video teaching with the addition of Moodle QRS. This modification reduced the time allotted to the part on case studies. Finally, the last round also adopted the relatively effective pedagogical model.

Student assignments were provided to students, and the results were compared in Table 101. Among the first three teaching rounds, Enhancement Round 3 had a high mean, which could be explained by the fact that the teacher (researcher) had experienced the foundation round model (which shares the same approach) and therefore conducted the lesson in a more effective way.

After the lesson, according to the section 6.2's findings, students changed their behaviour and attitude. Approximately 32.4% of respondents suggested that they would read the terms and conditions clearly or ensure that they understood the app's access rights to the information on their mobile devices. The increase was significant as compared with only 12.1% in the pre-teaching survey. Although more students would consider whether the app was convenient to use or not when engaging with new App, 47.1% of them are now concerned about the privacy policy, with 23.5% specifically concerned about the terms and conditions. The percentage of students installing anti-virus software also grew from 9.1% to 23.5%.

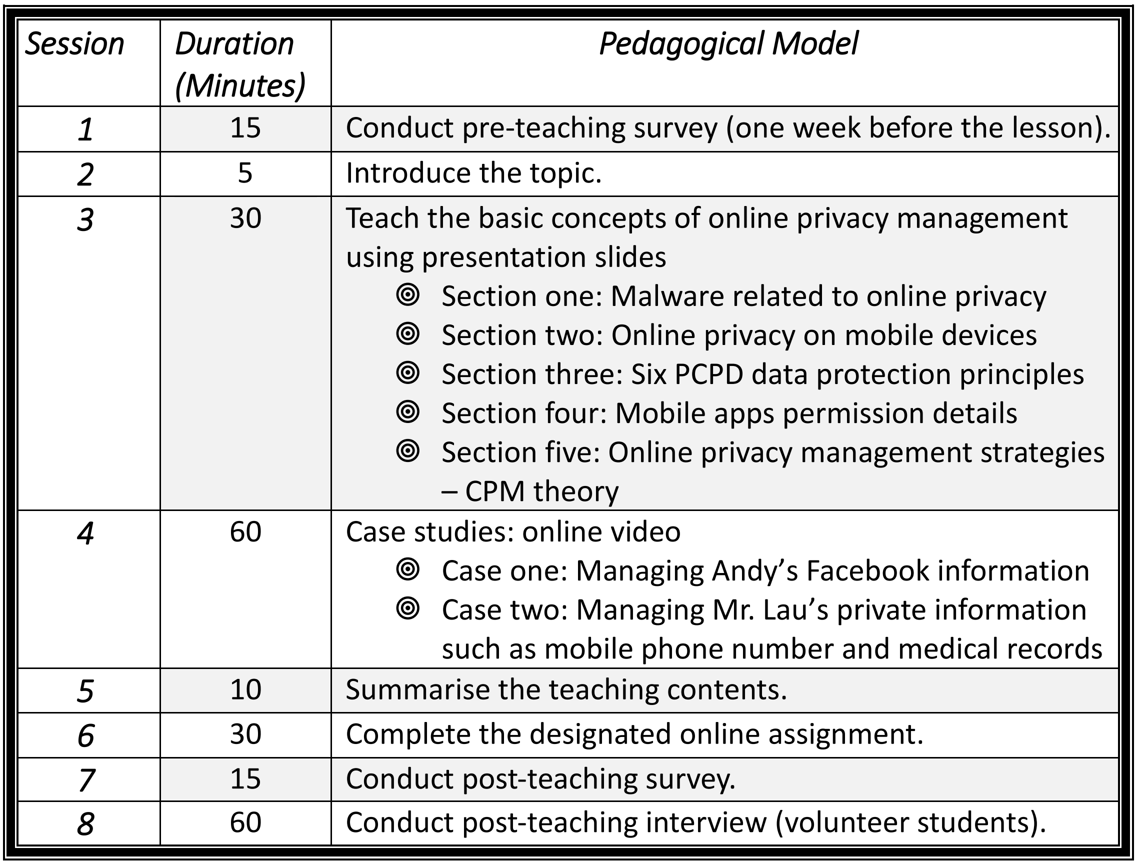
Table 103 shows the achievements, the problems that needed to be solved and how to tackle the problems in each teaching round. After four iterations, Enhancement Round 3 students' privacy concerned increased prominently. This finding could be seen from the results of the Teaching Survey Part 2 and Part 3 (Part 2 - online privacy attitude, OPA: +18% for 'extremely concerned' & +4% for 'very concerned'; Part 3 – online privacy management strategies, OPMS: +26% for 'extremely concerned' & +19% for 'very concerned'). In Table 102, the observation showed that Enhancement Round 3 students could learn from the case video effectively and attentively. Besides, the result of their assignment scores was the highest among all teaching rounds. In the post-teaching interview, students responded that the video was useful and would make use of those privacy skills learned from the video cases. This result once again confirmed that the pedagogical model in Enhancement Round 3 was relatively effective.

By combing the cross-tabulation results of this study and prior research articles (Joinson, Reips, Buchanan, & Paine Schofield, 2010; Krasnova, Spiekermann, Koroleva, &

Hildebrand, 2010; Mohamed & Ahmad, 2012), it was observed that if students' OPA was weak before the lessons, like the online privacy concerned level of students in the foundation round, their OPMS were improved significantly at end of the lessons. Thus, the adoption of the materials developed by using CPM theory and case-based learning to enhance the OPMS of students with low OPA is legitimate. However, privacy paradox emerged in the results of the three enhancement rounds. This result can be explained by the fact that if students' OPA was not weak, then no significant relationship exists between OPA and OPMA.

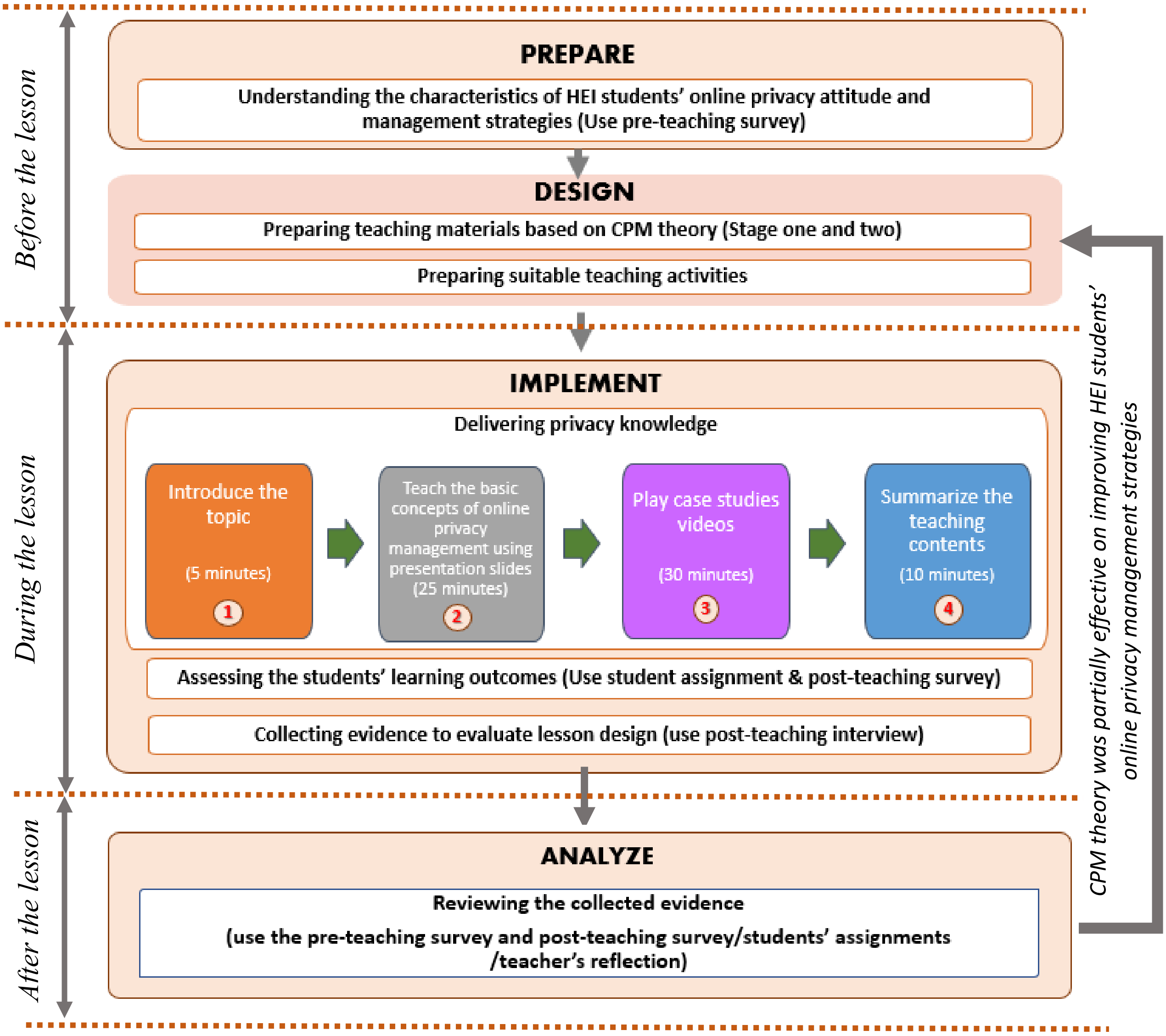
Figure 37 shows the more effective pedagogical models in developing HEI students' OPMS for mobile devices. Figure 38 exhibits the key ideas of our CPM-theory-based pedagogical model, which only focuses on Stage 1 and 2 of CPM theory.

Figure 37: Effective Pedagogical Models



Session	*Duration (Minutes)*	*Pedagogical Model*
1	15	Conduct pre-teaching survey (one week before the lesson).
2	5	Introduce the topic.
3	30	Teach the basic concepts of online privacy management using presentation slides ◎ Section one: Malware related to online privacy ◎ Section two: Online privacy on mobile devices ◎ Section three: Six PCPD data protection principles ◎ Section four: Mobile apps permission details ◎ Section five: Online privacy management strategies – CPM theory
4	60	Case studies: online video ◎ Case one: Managing Andy's Facebook information ◎ Case two: Managing Mr. Lau's private information such as mobile phone number and medical records
5	10	Summarise the teaching contents.
6	30	Complete the designated online assignment.
7	15	Conduct post-teaching survey.
8	60	Conduct post-teaching interview (volunteer students).

Figure 38: CPM-theory-based Pedagogical Model


Before the lesson
During the lesson
After the lesson
PREPARE
Understanding the characteristics of HEI students' online privacy attitude and management strategies (Use pre-teaching survey)
DESIGN
Preparing teaching materials based on CPM theory (Stage one and two)
Preparing suitable teaching activities
IMPLEMENT
Delivering privacy knowledge
Introduce the topic (5 minutes) 1
Teach the basic concepts of online privacy management using presentation slides (25 minutes) 2
Play case studies videos (30 minutes) 3
Summarize the teaching contents (10 minutes) 4
Assessing the students' learning outcomes (Use student assignment & post-teaching survey)
Collecting evidence to evaluate lesson design (use post-teaching interview)
ANALYZE
Reviewing the collected evidence
(use the pre-teaching survey and post-teaching survey/students' assignments /teacher's reflection)
CPM theory was partially effective on improving HEI students' online privacy management strategies

7.3 Research implication

The results of this study led to three research implications in relation to the needs of privacy management education, the feasibility of using case-based learning and the effectiveness of using CPM theory to prepare teaching materials so as to focus on the development of the HEI students' OPMS for mobile devices.

With regard to the first implication, from the findings of the pre-teaching survey, the needs of privacy management education were strong. HEI students did not have a high sense of data and privacy protection. This finding was key in app installation, as revealed by the survey results.

With the regard to the second implication, due to the integration of the convenience of the Internet and multimedia, HEI students, as a generation of the digital world, took advantage of learning through online case videos which could be provided by popular online platforms such as YouTube. Our case video teaching adopted online case studies obtained from YouTube and produced by the RTHK and the PCPD. HEI students obviously benefited from this online case study. Compared with the traditional teaching method like using current events (i.e. newspaper clippings), online case studies were more interactive, attractive and visual. This study reflected that the use online case studies would become more popular in future learning trends.

With regard to the last implication, CPM theory not only helped students, with a lower online privacy attitude, understand how to protect and manage their own privacy but also others' privacy. Students had little control on how other parties would use or even collect their personal data. However, if students learned the importance of protecting privacy regardless if it is their own or others', they could consider those privacy aspects they learned through CPM today when they became policymakers in the future. Moreover, if teachers know how to use CPM to develop a set of privacy teaching and learning materials especially using stage 1 and 2 of CPM, students will be benefitted from this.

7.4 Recommendation

This study provides recommendation for online privacy for policy makers on the basis of the research findings and the pedagogical model developed in the iterations. Suitable recommendations in conducting related teachings will also be given to teachers.

7.4.1 Recommendation on Online Privacy Policymaking

A number of incidents involving the possible leakage of personal data have caused public concern (Apple Next Media, 2016; Oriental Daily, 2016; Hodge, 2020; Ethan, 2021). With the rapid development of Internet technologies, personal registration and payment procedures on online platforms have become increasingly popular, and organisations and enterprises have collected a huge amount of personal data from citizens. To enhance students' online privacy concerns and OPMS, should the EDB increase the teaching hours of privacy education in primary and secondary school levels?

7.4.2 Recommendation on Pedagogical Model

The results of the DBR iterations show that the pedagogical model using online case studies with the designated student assignment was the most effective model. Case video teaching can cover several daily life cases that demonstrate privacy issues in an interesting way. Students are usually engaged in watching case study videos and participate actively in the discussion. Finally, the student assignments show that students learn much better regarding the privacy knowledge and obtain higher scores in the assignments through case study teaching. Therefore, we recommend teachers to adopt online case study videos with the designated student assignment to conduct privacy lessons.

7.5 Research Limitation and Further Studies

A major research limitation was the choice of the online video cases. The teaching materials were limited by the existing resources and recent news. This study employed the RTHK online video which was produced several years ago. The RTHK has not produced new series of privacy online videos recently. Unlike traditional teaching materials, teachers could not produce videos by themselves. The choice of the online videos was limited even in YouTube. Besides, teachers were difficult to product their own video cases. As such, teachers were restricted in finding suitable case videos with good quality.

The case video teaching method is currently widely used in professional fields such as business management education, medical education and teacher training to develop professionalism (Beckisheva, Gasparyan, & Kovalenko, 2015; Brattseva & Kovalev, 2015, Zheng el at., 2018). Case video teaching can also provide learners with a bridge between theory and practice, allowing them to apply theory to problem solving in cases. The usage of online case study as a pedagogical model is worth an in-depth study.

Besides, more volunteer students should be recruited to form a focus group to strengthen the triangulation of the quantitative and qualitative results. A lengthy survey may affect the quality of students' responses, as they may not answer all question items seriously. Therefore, the number of question items in this study should be reviewed to balance the quality of responses and the scope of the survey.

Apart from the research limitations, two directions are provided for extending this research in the future.

Firstly, a larger sample size can be used in each iteration. Future research could include more HEI students from different HEIs. This modification would increase the representativeness of the research findings.

Secondly, to enhance and confirm a more effective pedagogical model to develop HEI students' OPMS, more DBR iterations can be conducted. Thus, in further studies, more empirical testing is inevitable.

The last direction is to further investigate the unfolding relationship between OPA and online privacy behaviour. If a high online privacy attitude of HEI students is unrelated to their OPMS when they are using their mobile devices, then privacy paradox occurs. Then, we need to determine what factors are related to HEI students' OPMS when they are using mobile devices. Hence, more systematic investigations are required in future studies.

References

3 Incoming call blocking Apps leaked the personal information of 3 billion users. (2016). *Apple Next Media*. Retrieved from: http://hk.Apple.nextmedia.com/realtime/news/20161121/55944339.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *In: EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce.* P. 21-29.

Adam, L. (2016). *Smartphone Apps Are Now 50% of All U.S. Digital Media Time Spent.* comScore. Retrieved from https://www.comscore.com/Insights/Blog/Smartphone-Apps-Are-Now-50-of-All-US-Digital-Media-Time-Spent.

Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). The privacy paradox applies to IoT devices too: A saudi arabian study. *Computers & Security, 96*, 101897. doi:https://doi.org/10.1016/j.cose.2020.101897

Alghamdi, A. H., & Li, L. (2013). Adapting Design-Based Research as a Research Methodology in Educational Settings. *International Journal of Education and Research*, 1(10), 1-12. Retrieved from: https://www.ijern.com/journal/October-2013/27.pdf.

Alzahrani, A., Alalwan, A., & Sarrab, M. (2014). Mobile Cloud Computing: Advantage, Disadvantage and Open Challenge. Proceedings of the 7th Euro American on Telematics and Information Systems, (EATIS 2014) Article No. 20. Valparaiso, Chile. 1-4.

Anderson, T., & Shattuck, J. (2012). Design-based research: A decade of progress in education research? *Educational Researcher, 41*(1), 16-25.

Anderson, T., & Shattuck, J. (2012). Design-based research: A decade of progress in education research? *Educational Researcher, 41*(1), 16-25.

Anderson, T., & Shattuck, J. (2012). Design-based research: A decade of progress in education research. *Educational Researcher, 41*(1), 16-25.

APEC Privacy Framework document. (2005). APEC website. Retrieved from: http://www.apec.org/Groups/Committee-on-Trade-and-investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

APEC. (2016). *Key APEC Milestones*. Retrieved from: http://www.apec.org/apec/about_apec/history.html.

Australian Government. (2014). *Mobile privacy: a better practice guide for mobile App developers*. Retrieved from: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-App-developers.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). http://dx.doi.org/10.5210/fm.v11i9.1394

Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). Retrieved from http://firstmonday.org/article/view/1394/ 1312.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. doi: https://ezproxy01.hsu.edu.hk:2088/10.1016/j.tele.2017.04.013

Beckisheva, T. G., Gasparyan, G. A., & Kovalenko, N. A. (2015). Case study as an active method of teaching business English. *Procedia - Social and Behavioral Sciences, 166*, 292-295.

Bell, P. (2004). On the theoretical breadth of design-based research in education. *Educational Psychologist*, 39(4), 243-253.

Berghel, H. (2002). Hijacking the web. *Association for Computing Machinery.* doi:10.1145/505248.505263.

Bogdan, R., & Biklen, S. (2006). Qualitative research for education: An introduction to theory and methods (5th ed.). Boston: Allyn & Bacon.

Brattseva, E. F., & Kovalev, P. (2015). The power of case study method in developing academic skills in teaching business English (time to play). *Rossijskij Gumanitarnyj Žurnal, 4*(3), 234-242.

Bremer, D., & Bryant, R. (2005). A comparison of two learning management systems: Moodle vs. Blackboard. *Concise paper*, 135-140, Retrieved from: http://cvonline.uaeh.edu.mx/Cursos/Maestria/MTE/Gen02/Admon_aprendizaje/Unidad%204/lec_5_a_comparison_of_two_learning_management.pdf.

Brown, A. L. (1992). Design experiments: theoretical and methodological challenges in creating complex interventions in classroom settings. *The Journal of the Learning Sciences, 2*(2), 141P2118.

Cahir, J., McNeill, M., Bosanquet, A. & Jacenyik-Trawöger, C. (2014). Walking out the door: casualisation and implementing Moodle. *International Journal of Educational Management*, 28 (1), 5-14.

Cain, J., Black, E. P., & Rohr, J. (2009). An audience response system strategy to improve student motivation, attention, and feedback. *American Journal of Pharmaceutical Education*, 73(2), 21. https://doi.org/10.5688/aj730221.

Campbell, A. (1997). Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes About Information Privacy. *Journal of Direct Marketing,* 11, 8:44-57.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the doubleclick experience. *Journal of Business Ethics*, 35, 243–254.

Chennamaneni, A., & Taneja, A. (2015). Communication privacy management and self-disclosure on social media - a case of Facebook. *In Proceedings of the 21st Americas Conference on Information Systems (AMCIS)*, Puerto Rico, USA.

Cheung, C. M.; Chan, G. W.; and Limayem, M. (2005). A critical review of online consumer behavior: Empirical research. Journal of Electronic Commerce in Organizations, 3(4), pp. 1-19.

Chica, S.D. (2004). *Event-Based Learning: Educational and Technological Perspectives*.

Collins, A. (1992). Toward a Design Science of Education. In E. Scanlon & T. O'Shea (Eds.), *New directions in educational technology* (pp. 15-22). New York: Springer-Verlag.

Conger, S., Pratt, J. H., Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23(5), pp. 401–417.

Couldry, N., & Turow, J. (2014). Advertising, Big Data, and the Clearance of the Public Realm: Marketers' New Approaches to the Content Subsidy. *International Journal of Communication*, 8, 1710–1726.

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research. 4. ed., internet ed*. Boston; Munich: Boston; Munich: Pearson: Pearson.

Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage.

Creswell, J. W., Klassen, A. C., Plano Clark, V. L., & Smith, K. C., for the Office of Behavioral and Social Sciences Research. (2011, August). *Best practices for mixed methods research in the health science*s. Washington, DC: National Institutes of Health. Retrieved from http://obssr.od.nih.gov/training/mixed-methods-research.

Demetriadis, S.N., Papadopoulos, P.M., Stamelos, I.G., & Fischer, F. (2008). The effect of scaffolding students' context–generating cognitive activity in technology–enhanced case–based learning. *Computers & Education, 51*(2), 939–954. http://www.sciencedirect.com/science/article/pii/S0360131507001169

Demetriadis, S.N., Papadopoulos, P.M., Stamelos, I.G., & Fischer, F. (2008). The effect of scaffolding students' context–generating cognitive activity in technology–enhanced case–based learning. *Computers & Education, 51*(2), 939–954. http://www.sciencedirect.com/science/article/pii/S0360131507001169

Design-Based Research Collective. (2003). Design-based research: An emerging paradigm for educational inquiry. *Educational Researcher*, 32(1), 5-8.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297.

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior, 58*, 214-220.

EDB of the Government of the HKSAR. (2015). *Technology Education - Curriculum Documents: Information and Communication Technology (S4-6) 2007*. Retrieved from: http://334.edb.hkedcity.net/doc/chi/curriculum2015/ICT_CAGuide_e_2015.pdf.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook ''friends:'' Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), article 1. Retrieved February 17, 2008, from http://jcmc.indiana.edu/vol12/issue4/ellison.html

eMarketer. (2016). *US Internet Users Rely on Mobile Devices for Digital Access*. Retrieved from: https://www.emarketer.com/Article/US-Internet-Users-Rely-on-Mobile-Devices-Digital-Access/1013649#sthash.zBvHxrBd.dpuf.

Ericsson. (2019). *Ericsson Mobility Report.* Retrieved from:

https://www.ericsson.com/49d1d9/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf.

Ethan, P. (2021). Amid worldwide concerns over WhatsApp's new privacy terms, there's one question facing users: to switch, or not to switch?. *SCMP*. Retrieved from: https://www.scmp.com/news/hong-kong/society/article/3117631/amid-worldwide-concerns-over-whatsapps-new-privacy-terms?utm_source=copy_link&utm_medium=share_widget&utm_campaign=3117631.

Felten, E. W. , and Schneider, M. A. (2000). Timing attacks on Web privacy . *Proceedings of the 7th ACM Conference on Computer and Communications Security (CCS '00)*, Athens, Greece, November 1–4. New York: ACM.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. European Research on Management and Business Economics, 22(3), 167-176.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, 22(3), 167-176.

Fuad, M.M. & Debzani, D. (2014). Design and development of a mobile classroom response system for interactive problem solving. *In Proceedings of the Twenty-Sixth International Conference on Software Engineering and Knowledge Engineering* (SEKE), Vancouver, BC, Canada, pp. 49–52.

Giannakos, M.N. (2013). Exploring the video-based learning research: a review of the literature. *British Journal of Educational Technology,* 44(6), pp. 191-195.

Giannakos, M.N., Jaccheri, L. and Krogstie, J. (2016). Exploring the relationship between video lecture usage patterns and students' attitudes. *British Journal of Educational Technology.* doi: 10.1111/bjet.12313.

Gokce Attorney Partnership. (2019). Modaq. Retrieved from: https://www.mondaq.com/turkey/Privacy/784926/Are-Cookies-A-Threat-For-Our-Privacy.

Google. (2020). Clear, enable, and manage cookies in Chrome. Retrieved from: https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=en.

Grise-Owens, E. , Cambron, E. R. , Valade, R. , & Cooper, L. (2007, April). Katrina across the curriculum: Using current events to engage learning. Paper presented at the meeting of the Kentucky Association of Social Work Educators, Murray, KY.

Grise-Owens, E., Cambron, S., & Valade, R. (2010). Using current events to enhance learning: A social work curricular case example. *Journal of Social Work Education,* 46(1), p. 133–146. Retrieved from: https://doi.org/10.5175/JSWE.2010.200800062

Haung, C.C., Wang, Y.M., Wu, T.W., & Wang, P.A. (2013). An empirical analysis of the antecedents and performance consequences of using the Moodle platform. *International Journal of Information and Education Technology*, 3, 217-221.

Heo, M. (2011). Communication privacy disclosure management: An empirical study of socialization support in a pseudo-online course. Journal of Interactive Online Learning, 10(2), 76-95.

Hodge, R. (2020). Zoom security issues: Zoom could be vulnerable to foreign surveillance, intel report says. *CNet.com*. Retrieved from: https://www.cnet.com/news/zoom-security-issues-zoom-could-be-vulnerable-to-foreign-surveillance-intel-report-says/.

Hong Kong Airlines App Suspected of Leaking the Privacy of Over 100 Customers. (2016). *Oriental Daily*. Retrieved from: http://orientaldaily.on.cc/cnt/news/20161229/00176_042.html.

Hong, W. & Thong, J. Y. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly* (37:1), pp 275-298.

Huser, V. & Cimino, J. J. (2015). Impending challenges for the use of big data. *International Journal of Radiation Oncology • Biology • Physics, 95*(3), 890-894.

Isiaka, B. (2007). Effectiveness of video as an instructional medium in teaching rural children agricultural and environmental sciences. International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2007, Vol. 3, Issue 3, pp. 105-114.

Ito, M. et al., 2008. Living and Learning with New Media: Summary of Findings from the Digital Youth Project. *The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning*, 52.

Jin, S. A. (2012). “To disclose or not to disclose, that is the question”: A structural equation modeling approach to communication privacy management in e-health. *Computers in Human Behavior, 28*(1), 69-77. doi: https://doi.org/10.1016/j.chb.2011.08.012

Jin, S. A. (2012). To disclose or not to disclose, that is the question: A structural equation modeling approach to communication privacy management in e-health. *Computers in Human Behavior, 28*(1), 69-77. doi:https://doi.org/10.1016/j.chb.2011.08.012.

Jin, S. A. (2013). Peeling back the multiple layers of Twitter's private disclosure onion: The roles of virtual identity discrepancy and personality traits in communication privacy management on twitter. *New Media & Society,15*(6), 813-833.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25* (1), 1–24. doi:10.1080/07370020903586662

Jonassen, D. H., Howland, J., Moore, J., & Marra, R. M. (2003). *Learning to solve problems with technology: A constructivist perspective*. 2 ed. Prentice Hall

Kannamanani, R. (2008). *Software to provide security for web browser cookies and passwords using trusted computing technology*.

Kaspersky. (2020). *Android Mobile Security Threats*. Retrieved from: https://www.kaspersky.com/resource-center/threats/mobile.

Kelly, A. E., & Seppälä, M. (2016). Changing policies concerning student privacy and ethics in online education. International Journal of Information and Education Technology, 6(8), 652-655.

Kennedy-Lightsey, C., Martin, M. M. 2., Thompson, M., Himes, K. L., & Clingerman, B. Z. (2012). Communication privacy management theory: Exploring coordination and ownership between friends. *Communication Quarterly, 60*(5), 665-680.

Kennedy-Lightsey, C., Martin, M. M., Thompson, M., Himes, K. L., & Clingerman, B. Z. (2012). Communication privacy management theory: Exploring coordination and ownership between friends. *Communication Quarterly, 60*(5), 665-680.

Kevin, L., Jason, K. & Nicholas, C. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network, *Journal of Computer-Mediated Communication*, 14(1), 79–100.

https://doi.org/10.1111/j.1083-6101.2008.01432.x.

Koutoumanos, A., Protonotarios, V., Drakos, A. (2014). Seeding courses on Moodle: the AgriMoodle case. *Agris on-line Papers in Economic and Informatics*, 6, 49-58.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109–125. doi:10.1057/jit.2010.6

Kruck, S. E., Gottovi, D., Moghadami, F., Broom, R., & Forcht, K. A. (2002). Protecting personal privacy on the internet. Information Management & Computer Security, 10(2/3), 77.

Kshetri, N. (2014). The emerging role of big data in key development issues: Opportunities, challenges, and concerns. *Big Data & Society, 1*(2) doi:10.1177/2053951714564227.

Lang, F. R., John, D., Lüdtke, O., Schupp, J., & Wagner, G. G. (2011). Short assessment of the big five: Robust across survey methods except telephone interviewing. *Behavior Research Methods, 43*(2), 548-567.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication, 14(1), 79-100.

Li, X., & Chu, S. K. W. (2018). *Using design-based research methodology to develop a pedagogy for teaching and learning of chinese writing with wiki among chinese upper primary school students* doi: https://doi.org/10.1016/j.compedu.2018.06.009

Li, Y. (2009). A comparison of learning management systems, *Proceedings of 22nd Annual NACCQ Conference*, 157.

Lincoln, Y. S. & Guba, E. G. (1985). Naturalistic inquiry. Thousand Oaks. Calif.: Sage.

Luzak, J. A. (2014). Privacy Notice for Dummies? Towards European Guidelines on How to Give “Clear and Comprehensive Information” on the Cookies’ Use in Order to Protect the Internet Users’ Right to Online Privacy. *Journal of Consumer Policy*, *37*(4), 547–559.

MacDonald, R. J. (2008). Professional development for information communication technology integration: Identifying and supporting a community of practice through design-based research. *Journal of Research on Technology in Education, 40*(4), 429-445.

Machado, M. & Tao, E. (2009). Blackboard vs. Moodle: Comparing user experience of Learning Management Systems, *Proceedings of the 37th ASEE/IEEE Frontiers in Education Conference*, S4J-7 – S4J-12. doi: 10.1109/FIE.2007.4417910.

Malekigorji, M. & Hatahet, T. (2020). Classroom Response System in a Super-Blended Learning and Teaching Model: Individual or Team-Based Learning? *Pharmacy*, 8(4), p. 197. https://doi.org/10.3390/pharmacy8040197

Malganova, I. & Rahkimova, A. (2016). E-learning practice using Moodle by leading universities in the Russian region. *Academy of Strategic Management Journal*, 15, 14-19.

Malhotra, N., Kim, S., and Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* (15:4), pp 336-355. doi:10.1287/isre.1040.0032

MarTech Advisor. (2019). *In the Age of 5G, Is Privacy Just A Myth?* Retrieved from: https://www.martechadvisor.com/articles/mobile-marketing/5g-internet-and-data-privacy/.

Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. (2016). An analysis of personal information privacy concerns using Q-methodology. *Corr, abs/1606.03547*

Mary, M., Sandra, C., Urs, G., Amanda, L., & Maeve, D. (2012). *Parent, Teen and Online privacy*. Pew Research Center. Retrieved from: http://www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy/.

May, M., & George, S. (2011). Privacy concerns in E-learning: Is Using Tracking system a threat? International Journal of Information and Education Technology, 1(1), 1.

McKenna-Buchanan, T., Munz, S. & Rudnick, J. (2015). To Be or Not To Be Out in the Classroom: Exploring Communication Privacy Management Strategies of Lesbian, Gay, and Queer College Teachers. *Communication Education, 6(*3), 280-300. DOI: 10.1080/03634523.2015.1014385

Metzger, M. J. (2007). Communication privacy management in electronic commerce. Journal of Computer-Mediated Communication, 12(2), 335-361.

Mikalef, P., Pappas, I.O. & Giannakos, M. (2016). An integrative adoption model of video-based learning. *International Journal of Information and Learning*

Technology, 33(4), pp. 219-235. Retrieved from: https://doi.org/10.1108/IJILT-01-2016-0007

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing, 27*, 19-33.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366–2375. doi:10.1016/j. chb.2012.07.008

Montgomery K. (2000). Youth and digital media: a policy research agenda. *Journal of Adolescent Health*, 27, 61–68.

Moodle. (2019). *Moodle statistics*. Retrieved from: https://moodle.net/stats/?lang=zh_tw.

Morse, J. M., & Niehaus, L. (2009). *Mixed method design: Principles and procedures*. Walnut Creek, CA: Left Coast Press.

Moscardell, D.M., & Liston-Heyes, C. (2004). Teens Surfing The Net: How Do They Learn To Protect Their Privacy? *Journal of Business and Economics Research, 2*(9), 43-56.

Muliati, S., Rabiah, A., & Othman, N. F. (2018). Motivational factors in privacy protection behaviour model for social networking. *MATEC Web of Conferences, 150*, 05014.

Nadeem, M. S. (2020). Common threats to online privacy and digital security. Retrieved from: https://blog.mailfence.com/viruses-spywares-malware-botnets-protect/.

Ngwenya, N., Farquhar, M., & Ewing, G. (2016). Sharing bad news of a lung cancer diagnosis: understanding through communication privacy management theory. Psycho-Oncology, 25: 913– 918. doi: 10.1002/pon.4024.

Okamoto, S.K., Helm, S., McClain, L.L., & Dinson, A.L. (2012). The development of videos in culturally grounded drug prevention for rural native Hawaiian youth. *Journal of Primary Prevention, 33*(5-6), 259-269. http://link.springer.com/article/10.1007%2Fs10935-012-0281-0

Oomen I. & Leenes R. (2008). Privacy Risk Perceptions and Privacy Protection Strategies. In: de Leeuw E., Fischer-Hübner S., Tseng J., Borking J. (eds) Policies and Research in Identity Management. *The International Federation for Information Processing,261*. Springer, Boston, MA. https://doi.org/10.1007/978-

0-387-77996-6_10

Paul, O. (2012). Don't Build a Database of Ruin. *Harvard business review*. https://hbr.org/2012/08/dont-build-a-database-of-ruin.

PCPD. (2012). Report on Privacy Awareness Survey on Smartphones and Smartphone Apps. Retrieved from: https://www.pcpd.org.hk/english/resources_centre/publications/surveys/files/smartphone_survey_e.pdf.

PCPD. (2020a). *Six Data Protection Principles.* Retrieved from: https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html.

PCPD. (2020b). *The Personal Data (Privacy) Ordinance.* Retrieved from: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.

Petronio S., & Durham W. T. (2015). Communication privacy management theory: Significance for interpersonal communication. In Braithwaite D. O., Schrodt P. (Eds.), *Engaging theories in interpersonal communication: Multiple perspectives* (pp. 335–347). Thousand Oaks, CA: SAGE.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* Albany, NY: SUNY Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*, 6-14.

Petronio, S., & Jones, S. M. (2006). When "friendly advice" becomes a privacy dilemma for pregnant couples: Applying Communication Privacy Management Theory. In L. H. Turner & R. West (Eds.), *The family communication sourcebook* (pp. 201–218). Thousand Oaks, CA: Sage.

Petronio, S., & Kovach, S. (1997). Managing privacy boundaries: Health providers' perceptions of resident care in Scottish nursing homes. *Journal of Applied Communication Research*, 25, 115–131. doi: 10.1080=00909889709365470

Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon*, *9*(5), 1-6.

Privacy Concerns on Cookies. https://www.allaboutcookies.org/privacy-concerns/.

Quan-Haase, A. (2007). University students' local and distant social ties: Using and integrating modes of communication on campus. *Information, Communication &*

Society, 10(5), 671–693.

Quinn, K. (2016). Why we share: A uses and gratifications Approach to privacy regulation in social media use. Journal of Broadcasting & Electronic Media, 60(1), 61-86.

Randall, N. (1997). The new Cookie Monster. *PC Magazine* 16 (8), April 22.

Rauscher, E. A., & Durham, W. T. (2015). “As long as you're sure you don't want any more children”: Men's collective boundary coordination of information about their affirmative vasectomy decision. *Communication Studies, 66*(2), 186-203.

Reis, L.O., Ikari, O., Taha-Neto, K.A., Gugliotta, A. & Denardi, F. (2015). Delivery of a urology online course using Moodle versus didactic lectures methods. *International Journal of Medical Informatics*, 84, 149-154.

Reuters. (2019). *Special report - Hobbling Huawei: Inside the U.S. war on China's tech giant.* Retrieved from: https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-us-war-on-chinas-tech-giant-idUSKCN1SR1EU?zd_source=mta&zd_campaign=14205&zd_term=vanditagrover.

Robson, C. (1993). *Real world research*. Oxford: Blackwell.

Roche, S. E., Dewees, M., Trailweaver, R., Alexander, S., Cuddy, C., & Handy, M. (1999). Contesting boundaries in social work education: A liberatory approach to cooperative learning and teaching. Alexandria, VA: Council on Social Work Education.

Ruiz-Martínez, A., Martinez-Carreras, M.A. & Ramallo-Gonzalez, A.P. (2020). Enhancing Check-Reinforce Introduction With a Class Response System: The C2RI Method—A Five-Year Study. *IEEE Access*, 8, p. 15178–15193.

Salmon, G. (2004). *E-moderating: The key to online teaching and learning*. 2 ed. Routledge.

Salomon, D. (2006). *Foundations of computer security*. Berlin: Springer.

Schmitz, B., Klemke, R., Walhout, J., & Specht, M. (2015). *Attuning a mobile simulation game for school children using a design-based research approach* doi:http://dx.doi.org.ezproxy.eduhk.hk/10.1016/j.compedu.2014.09.001.

Sean Keane. (2020a). Zoom boss says it'll freeze feature updates to address security issues.

CNet.com. Retrieved from: https://www.cnet.com/news/elon-musk-wants-spacex-to-launch-the-next-generation-of-space-telescopes/.

Sean Keane. (2020b). Zoom chalks up 300 million daily participants despite security issues. *CNet.com*. Retrieved from: https://www.cnet.com/news/zoom-chalks-up-300-million-daily-participants-despite-security-issues/.

Simon, H. (2015). Are cookies crumbling our privacy? We asked an expert to find out. Retrieved from 29 March, 2015: https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/.

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce, 10*(1), 1-16.

Smith, A. (2015). *The smartphone difference*. Pew Research Center. Retrieved from: http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

Smith, H., Dinev, T., and Xu, H. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* (35:4), 989–1015.

Smith, H., Dinev, T., and Xu, H. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly,* 35(4), pp. 989–1015.

Smith, H., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly,* 20:2, 167–196.

Sslamet Kurniawan Fahrurozi, Dwi Maryono, & Cucuk Wawan Budiyanto. (2017). The Development of Video Learning to Deliver a Basic Algorithm Learning. *IJIE Indonesian Journal of Informatics Education, 1*(2), 135-142.

Statista. (2017). Hong Kong: social network penetration Q3 2017. Retrieved from: https://www.statista.com/statistics/412500/hk-social-network-penetration/.

Statista. (2018a). Hong Kong: number of Facebook users 2015-2022. Retrieved from: https://www.statista.com/statistics/558226/number-of-facebook-users-in-hong-kong/.

Statista. (2018b). Instagram: distribution of global audiences 2018, by age group. Retrieved from: https://www.statista.com/statistics/325587/instagram-global-age-group/.

Stowell, J.R. (2015). Use of clickers vs. mobile devices for classroom polling. *Computers and Education*, 82, p. 329–334.

Tan, C. (2006). Philosophical reflections from the silver screen: using films to promote reflection in pre-service teachers. *Reflective Practice, 7* (4), 483-497. http://www.tandfonline.com/doi/abs/10.1080/14623940600987080#preview

Teddlie, C. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Thousand Oaks, CA: Sage Publications.

The Design-Based Research Collective. (2003). Design-based research: An emerging paradigm for educational inquiry. *Educational Researcher, 32*(1), 5-8.

The Direct Marketing Association (UK) Limited (DMA). (2015). Report on data privacy: what the consumer really thinks. Retrieved from: https://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf.

The Office of the Communications Authority. (2021). *Key Communication Statistics: Telecommunications Services*. Retrieved from http://www.ofca.gov.hk/en/media_focus/data_statistics/key_stat/.

Thompson, J. (2011). Communication privacy management in college athletics: Exploring privacy dilemmas in the athletic/academic advisor student-athlete interpersonal relationship. *Journal of Sport Administration & Supervision, 3*(1), 44-60.

Turner, T.N. (1995). Riding the rapids of current events! *The Social Studies*, 86(3), p. 117-121.

University of Massachusetts Amherst: Security Centre. (2020) *Malware: Viruses, Spyware, Adware & Other Malicious Software*. https://www.umass.edu/it/security/malware-viruses-spyware-adware-other-malicious-software.

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing*, 41, 409-418.

Wang, F., & Hannafin, M. J. (2005). Design-based research and technology: Enhanced learning environments. *Educational Technology Research and Development*, 53(4), 5-23.

Weber, A. S. (2016). The big student big data grab. *International Journal of Information and Education Technology, 6*(1), 65-70.

Westin, A. (1970). *Privacy and Freedom*. The Bodley Head Ltd, London, UK.

Wright, R. G. (1992). Event-based science. *The Science Teacher*, 59(2), p. 22-23.

Yang, C. C., Amanda, P. & Yowei, K. (2016). Exploring the Relationship between Privacy Concerns and Social Media Use among College Students: A Communication Privacy Management Perspective. *Intercultural Communication Studies*, 25(2), 46-62.

Yang, K. C. C., Pulido, A., & Kainan, Y. K. (2016). Exploring the relationship between privacy concerns and Social Media use among college students: A communication privacy management perspective. *Intercultural Communication Studies*, 2(47).

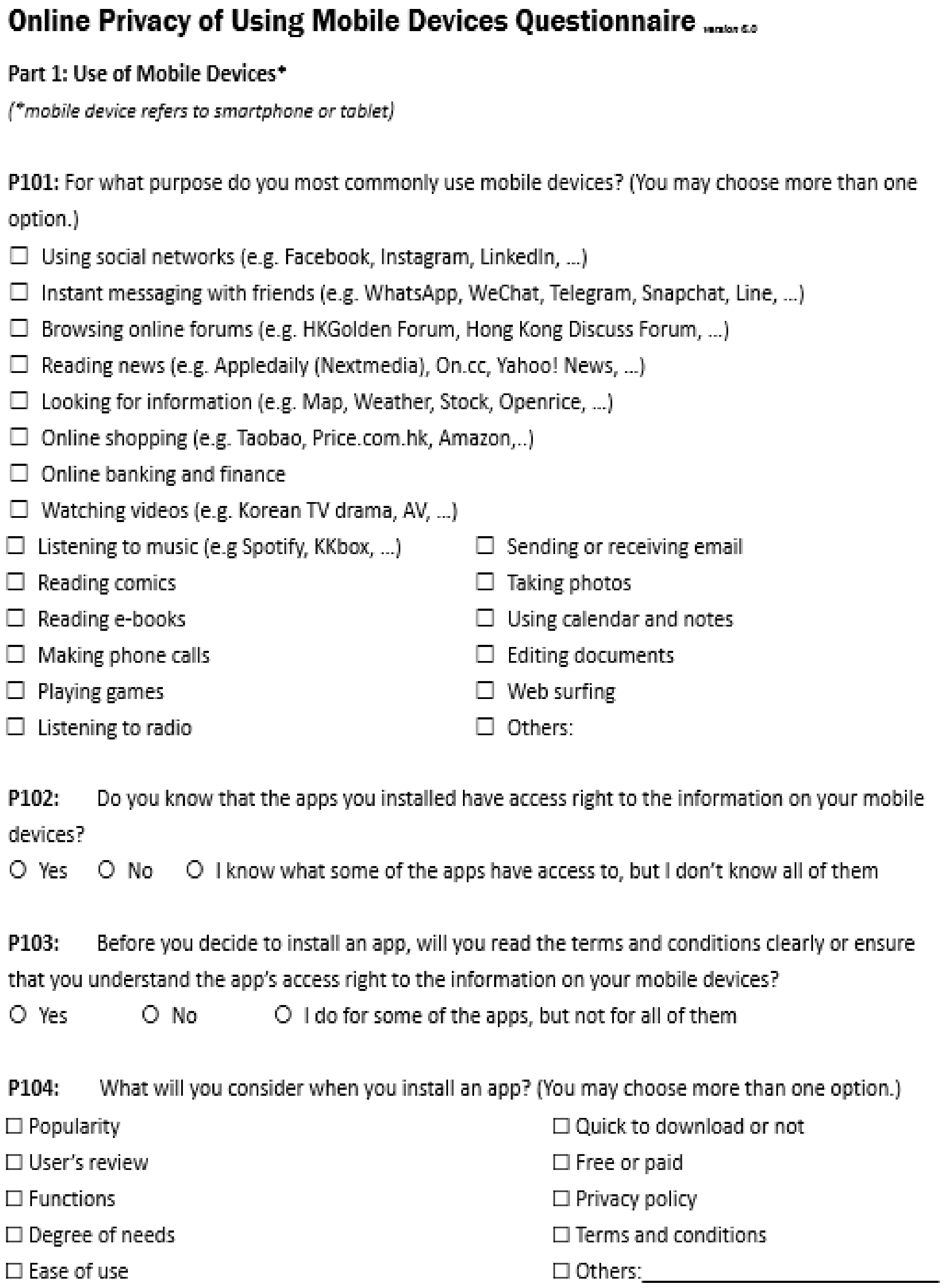
Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389-418.

Zhang, D. (2018). Big Data Security and Privacy Protection, *8th International Conference on Management and Computer Science*, 275-278.

Zhang, Y., Miller, L.E., & Harrison, K. (2008). The relationship between exposure to sexual music videos and young adults' sexual attitudes. *Journal of Broadcasting & Electronic Media, 52*(3), 368-386. http://www.tandfonline.com/doi/abs/10.1080/08838150802205462#preview

Zheng, Y., Li, J., Wu, Q., Wu, Y., Guo, M., & Yu, T. (2018). Study on the application of case teaching method in the cultivation of master of professional clinical surgery. *Creative Education, 9*(2), 272-279.

Appendix I



Online Privacy of Using Mobile Devices Questionnaire version 6.0

Part 1: Use of Mobile Devices*

*(*mobile device refers to smartphone or tablet)*

P101: For what purpose do you most commonly use mobile devices? (You may choose more than one option.)

☐ Using social networks (e.g. Facebook, Instagram, LinkedIn, ...)
☐ Instant messaging with friends (e.g. WhatsApp, WeChat, Telegram, Snapchat, Line, ...)
☐ Browsing online forums (e.g. HKGolden Forum, Hong Kong Discuss Forum, ...)
☐ Reading news (e.g. Appledaily (Nextmedia), On.cc, Yahoo! News, ...)
☐ Looking for information (e.g. Map, Weather, Stock, Openrice, ...)
☐ Online shopping (e.g. Taobao, Price.com.hk, Amazon,..)
☐ Online banking and finance
☐ Watching videos (e.g. Korean TV drama, AV, ...)
☐ Listening to music (e.g Spotify, KKbox, ...)
☐ Reading comics
☐ Reading e-books
☐ Making phone calls
☐ Playing games
☐ Listening to radio
☐ Sending or receiving email
☐ Taking photos
☐ Using calendar and notes
☐ Editing documents
☐ Web surfing
☐ Others:

P102: Do you know that the apps you installed have access right to the information on your mobile devices?

○ Yes ○ No ○ I know what some of the apps have access to, but I don't know all of them

P103: Before you decide to install an app, will you read the terms and conditions clearly or ensure that you understand the app's access right to the information on your mobile devices?

○ Yes ○ No ○ I do for some of the apps, but not for all of them

P104: What will you consider when you install an app? (You may choose more than one option.)

☐ Popularity
☐ User's review
☐ Functions
☐ Degree of needs
☐ Ease of use
☐ Quick to download or not
☐ Free or paid
☐ Privacy policy
☐ Terms and conditions
☐ Others:______________________________

P105: What kind of personal information has been stored in your mobile devices? (You may choose more than one option.)

□ Friends' contact information (e.g. phone number, email)
□ Your bank or credit card account password
□ Entrance code of building
□ ATM password
□ Your online account number and password
□ Your email address(es)
□ Your email account password
□ Personal and sensitive photo
□ Haven't stored any personal information
□ Others: ______________________

P106: What protective action(s) have you taken? (You may choose more than one option.)

□ Set up auto screen lock
□ Set up screen lock
□ Install anti-virus software
□ Install anti-theft software
□ Others

		Yes	No
P107:	Will you encrypt personal information on your mobile devices?	○	○
P108:	Do you worry about data leakage when you are using your mobile devices to download apps?	○	○
P109:	Have you taken any measures to protect the confidentiality of the information on your mobile devices?	○	○

		I know	I don't know
P110:	Do you know that your contact lists may be uploaded to the central servers of the social networking apps that you are using?	○	○
P111:	Do you know that some apps will take actions that they have not mentioned they would (e.g. download or upload your mobile devices information or record your voice conversation without notifying you)?	○	○
P112:	Do you know that, when you take a picture with your mobile devices, your geo-location may also be recorded in the photo?	○	○

		Very important	Important	Moderately Important	Slightly important	Not important
P113:	Convenience is important to you.	①	②	③	④	⑤
P114:	Privacy is important to you.	①	②	③	④	⑤

P115: What kind of personal information of **your friends, classmates, family members** have been stored in your mobile devices? (You may choose more than one option.)

☐ Friends' contact information (e.g. phone number, email)
☐ Entrance code of building which you and your family members live
☐ Someone ATM password(s)
☐ Someone's online account number and password
☐ Their email addresses
☐ Their email account passwords
☐ Their personal and sensitive photo
☐ Haven't stored any personal information of others
☐ Others

P116: What kinds of **your personal information** have been stored in your mobile devices? (You may choose more than one option.)

☐ Contact information (e.g. phone number, email address)
☐ Entrance code of the building where you and your family members live
☐ ATM password
☐ Online account ID and password
☐ Email address
☐ Email account password
☐ Personal and sensitive photo
☐ Others
☐ Haven't stored any personal information

P117: Suppose that you are downloading an App on your mobile devices, after you have clicked to download, the App asks access to your contacts' personal information (i.e. other people's personal information such as phone numbers, names, … etc.) and sensitive photos about other people.
If you can cancel the download, please answer next question.
If you still continue with the download, state your reason here and then answer next section.

P118: Refer to the previous question, if you will cancel the download, state your reason here.

Part 2: Attitudes Towards Data Privacy

		Not concerned at all	Of little concerned	Of average concerned	Very concerned	Absolutely concerned
P201:	The information I submit on my mobile device(s) could be misused.	①	②	③	④	⑤
P202:	People can get hold of my private information on my mobile device(s).	①	②	③	④	⑤
P203:	Others might use my mobile device(s) to submit information.	①	②	③	④	⑤
P204:	Information submitted through my mobile device(s) could be used in many ways, such as advertising, that I cannot foresee.	①	②	③	④	⑤

		Strongly agree	Agree	Undecided	Disagree	Strongly disagree
P205:	Do you agree with the following statement? 「我行得正，企得正，無咩嘢資料或者其他嘢唔可以俾人知，所以我無保護我嘅手機資料。」 "I live an upright life. I have nothing to hide. Why should I care about my mobile privacy?"	①	②	③	④	⑤
P206:	The App developers are trustworthy.	①	②	③	④	⑤
P207:	The App developers keep their promises and commitments.	①	②	③	④	⑤
P208:	The App developers keep their customers best interests in mind.	①	②	③	④	⑤
P209:	It is not a serious matter even if my personal information is collected by the App developers.	①	②	③	④	⑤
P210:	I have perfect control of all my private information stored on my mobile device(s).	①	②	③	④	⑤
P211:	The security control on my mobile devices is enough to protect my own privacy.	①	②	③	④	⑤
P212:	Shopping on my mobile device(s) is risky.	①	②	③	④	⑤
P213:	Providing credit card information online via mobile device(s) is risky.	①	②	③	④	⑤
P214:	Providing my HKID number and/or full name via mobile device(s) is risky.	①	②	③	④	⑤
P215:	Providing my phone number via mobile device(s) is risky.	①	②	③	④	⑤

		Strongly agree	Agree	Undecided	Disagree	Strongly disagree
P216:	Providing my friends' phone numbers via mobile device(s) is risky.	①	②	③	④	⑤
P217:	Registering via mobile device(s) is risky.	①	②	③	④	⑤
P218:	Shopping online for certain products is riskier on mobile phones than via non-mobile computers.	①	②	③	④	⑤
P219:	I am familiar with the data protection act of Hong Kong.	①	②	③	④	⑤
P220:	I have a good practice of protecting my privacy on my mobile device(s).	①	②	③	④	⑤
P221:	Protecting my privacy on my mobile device(s) is important.	①	②	③	④	⑤
P222:	I have good knowledge of protecting my own privacy on my mobile device(s).	①	②	③	④	⑤

P223: Do you read the privacy policy before you download an App?

○ Always ○ Often ○ Sometimes ○ Rarely ○ Never

P224: Do you know what personal information of yours are collected by the App developer(s)?

○ Yes ○ No

P225: Did you try to find out what personal information of yours are collected by the App developer(s) before installing an App?

○ Yes ○ No

Part 3: Boundary Rules and Control of Private information on Mobile Devices

		Strongly agree	Agree	Undecided	Disagree	Strongly disagree
P301:	I feel that I can keep all my private information in an acceptable manner.	①	②	③	④	⑤
P302:	I have well managed the apps I have installed on my mobile device(s), such that I update them regularly or delete those that are unused.	①	②	③	④	⑤
P303:	I have checked and modified the privacy settings of my mobile device(s).	①	②	③	④	⑤
P304:	If the information stored on my mobile devices looks too private, I will delete it.	①	②	③	④	⑤
P305:	I have perfect control of all my SNS account.	①	②	③	④	⑤
P306:	I have checked and modified the privacy settings of my SNS account on my mobile device(s).	①	②	③	④	⑤
P307:	If the information I posted on SNS looks too private, I will delete it.	①	②	③	④	⑤
P308:	I do not share some things because I worry about who has access to my SNS(s).	①	②	③	④	⑤
P309:	I use real personal information to create my SNS account(s).	①	②	③	④	⑤
P310:	I have the choice to accept followers on my SNS(s).	①	②	③	④	⑤
P311:	My SNS entries are detailed.	①	②	③	④	⑤
P312:	I have my own criteria for who I will follow on SNS.	①	②	③	④	⑤
P313:	I comment on a SNS to ask others to visit my SNS.	①	②	③	④	⑤
P314:	I have blocked people who I do not know in the IM App(s) on my mobile device(s).	①	②	③	④	⑤
P315:	I have the choice to accept an IM contact.	①	②	③	④	⑤

P316: Have you forward the text messages or the photos of someone in your instant messaging (IM) App, such as WhatsApp, Snapchat and WeChat, to other people without getting his or her consent beforehand?

○ Always ○ Very often ○ Sometimes ○ Rarely ○ Never

Part 4: Demographic Information

#A01: Degree programme:

○ BBA ○ BTB ○ BJC ○ SCM ○ FA ○ MGT ○ CHI ○ AS ○ ENG
○ CMCT ○ Others: ____________________

#A02: Year:

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ Others: ____________

#A03: Age: ○ 17 ○ 18 ○ 19 ○ 20 ○ 21 ○ Others: ____________

#A04: Gender: ○ Female ○ Male

#A07: Do you join the compulsory workshop – Internet Security organized by HSUHK?

○ Not join ○ Joined ○ N/A

		Yes	No
#A08:	Did you take DSE ICT?	○	○
#X01:	Have your mobile device(s) been hacked by others?	○	○
#X02:	Have your personal data stored on your mobile device(s) been misused by others?	○	○

#J01: From where did you learn the knowledge or skills of protecting your online privacy? (You may choose more than one option.)

□ From your Primary education
□ From your Secondary education
□ From your Higher education
□ From Media such as newspapers or TV
□ From Social Networking Sites
□ From parents
□ From friends
□ Others: ____________________

~~ END OF SURVEY ~~

~~ THANK YOU VERY MUCH ~~