Journal of International Technology and Information Management

Volume 26 | Issue 4 Article 5

12-1-2017

Privacy Risks and Security Threats in mHealth apps

Brinda Hansraj Sampat
NMIMS University, brinda.sampat@nmims.edu

Bala Prabhakar
NMIMS University, bala.prabhakar@nmims.edu

Privacy Risks and Security Threats in mHealth apps

Cover Page Footnote

The authors would like to sincerely thank all the anonymous reviewers for their valuable comments and suggestions.

Privacy Risks and Security Threats in mHealth Apps

Prof. Brinda Sampat *
Assistant Professor
NMIMS- Global Access School for Continuing Education (NGA-SCE),
NMIMS University,
Mumbai, India

Dr. Bala Prabhakar
Dean
Shobhaben Pratapbhai Patel School of Pharmacy & Technology Management (SPP SPTM),
NMIMS University,
Mumbai, India

ABSTRACT

mHealth (Mobile Health) applications (apps) have transformed the doctor-patient relationship. They help users with varied functionalities such as monitoring their health, understanding specific health conditions, consulting doctors online and achieving fitness goals. Whilst these apps provide an option of equitable and convenient access to healthcare, a lot of personal and sensitive data about users is collected, stored and shared to achieve these functionalities. Little is known about the privacy and security concerns these apps address. Based on literature review, this paper identifies the privacy risks and security features for evaluating thirty apps in the Medical category across two app distribution platforms in India namely Google Play and App Store. Factors identified through the review formed a basis of the scoring model which helped to arrive at the 'Privacy Risk Score' and 'Safety Score' for each app. A comparative analysis of the selected apps was performed by studying their privacy policies. The results indicate that adopting these apps pose a risk. Finally, recommendations are provided to consumers such as examining the app before downloading it, customizing the app settings, and to developers to develop robust and transparent privacy policies.

KEYWORDS: mHealth, Apps ,Smartphones, mobile devices, Privacy, Privacy Policies, Risks, Security.

INTRODUCTION

The recent technological advancements and unprecedented spread of mobile technology usage in the area of healthcare has led to the emergence of a new field called mHealth (Mobile Health). It is a subset of eHealth (Electronic Health) that involves the use of the mobile platform to support a number of growing functionalities (Mechael, 2009). It is defined as "The medical and public health practice carried out with mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" (Kay et al., 2011). mHealth refers to the healthcare based mobile computing, medical sensors, and communications technologies (Istepanian et al., 2006). With the presence of high capacity computing devices, improvement in wireless communication with the emergence of 3G, 4G and wearable sensors, mHealth is now a reality. mHealth proposes to deliver healthcare applications anytime, anywhere at low and affordable costs (Akter & Ray, 2010). The three key components in mHealth are mobile devices, software platform (providing basic services such as networking and database), and mHealth applications (apps) (Rebolj et al., 2004). mHealth apps are software applications that can be installed and run on hardware platform, to help manage chronic diseases, empower the elderly and expectant mothers, remind people to take timely medication etc.

Mobile phones have achieved a high penetration rate. Almost 1.5 billion smartphones were sold to end users in 2016. Over one third of the world's population is estimated to own a smartphone by 2017 (Statistica[1], 2017). Mobile apps are designed to run on smartphones, phablets, tablets and other mobile devices. They are made available through app stores. The two major app distribution platforms that are available are the App store that supports the iOS and the Google Play store that supports the Android operating system. As of March 2017, there were 2.2 billion apps available in the App Store and 2.8 million available apps on the Google Play store. As of June 2017, 180 billion apps have been downloaded from the App store (Statistica[2,3], 2017). A plethora of apps are available which range from medical appointments to customized fitness advice, blood pressure measurement, pregnancy apps for first time fathers, blood sugar measurement to name a few. These apps are either free or paid. Apps have made way for patients to record their daily activities and vital signs. They help to deliver interactive health services to patients, clinicians and caregivers.

These apps have the ability to collect wide range of data from the users such as their daily diet or lifestyle patterns, their location, physical activity regime etc. Free apps ask for more permissions than paid apps. Apps can vary widely in how many permissions they require with one app asking for 47 permissions, and others only

ISSN: 1941-6679-On-line Copy

one. In all, there were 126 different permissions apps can ask for, but the list of possible permissions continues to grow. (Olmstead, 2014). In order to provide high quality, on demand and context aware services some apps use the embedded technology in the smartphones including cameras and sensors, acceleration, audio to collect and store personal data. In many apps, users are prompted to give up their geo-location, unique phone identifier and details of their contact list even before they start using the app (McAllister, 2014). The Google Play Store seeks users' permissions when they download apps. These are mentioned in the table below.

Table 1.List of App Permission Requests in the Google Play Store

App Permission Group	Other Permissions
1. In-app purchases	1. Receive data from Internet
2. Device & app History	2. View network connections
3. Cellular data settings	3. Full network access
4. Identity	4. Control vibration
5. Contacts	5. Prevent device from sleeping
6. Calendar	6. Storage
7. Location	7. Change your audio settings
8. SMS	8. Modify system systems
9. Phone	9. Run at start-up
10. Photo/Media/Files	10. Google Play license
11. Camera	11. Manage access to documents
12. Microphone	
13. Wi-fi Connection Information	
14. Bluetooth Connection Information	
15. Wearable sensors/Activity data	
16. Device ID and call information	

These permissions are not limited to apps alone. Wearable devices such as FitBit, Jawbone, Apple Watch, Pebble Watch and the likes also collect information about the users. Apps provide features with which users register themselves with their social media account to share information with their family and friends. The practical issues with respect to privacy involve data protection and data transfer (Subramanian, 2017). Some of the apps collect patient data continuously which can be analysed by the doctors directly to foster remote health monitoring. Despite the many benefits mHealth offers, little attention has been paid to the information

security and privacy policies and practices of mHealth app vendors (Sunyaev et al., 2014).

Healthcare involves privacy issues concerning patients, physicians, and primary care providers. The most important aim is to secure healthcare information systems and prevent unauthorized people from accessing medical records and confidential information (AlHamad et al., 2014). Sensitive health data of patients is exchanged through wireless networks and thus addressing the privacy and security concerns in the usage of mHealth aps is essential. In today's networked interconnectivity, more than 500,000 new malware variants surface on a regular basis (Emmnauel & Mohammed, 2017). Many apps provide extensive clauses regarding data collection included in privacy policies. Users are presented with options to select their willingness to share data but most of them are surprised with the amount of data leakage that takes place via their phone (Lederer et al., 2003; Lin et al., 2012). Most users are not fully aware of what data is being collected and how it is used or reused (Shklovski et al., 2014).

PRIVACY AND SECURITY

Privacy and security issues impede the adoption and diffusion of technology in the IT domain (Cho et al., 2009; Zorotheos et al., 2009; Lee et al., 2011). In the context of Information Systems (IS), privacy is defined as an individual's tendency to be concerned about overall information privacy (Li, 2011). Studies have found privacy concerns in the area of using IS, wherein users had concerns related to the use of websites which impacted their behaviour and this was evident through a limited disclosure of personal information (Li.,2011). Individuals with high privacy concerns perceive a new IS to be more risky eventually developing concerns about it (Kim et al., 2010).

These concerns regarding privacy are more directed towards the appropriateness of technology to safeguard personal information. mHealth apps stores communicate personal information about users, and this unfamiliarity with the app environment develops many app-related privacy concerns for consumers. mHealth has empowered users to manage their own health creating a shift from the physician's office to mobile apps and storage in the cloud which raises many privacy and security concerns (He et al., 2014). According to National committee on Vital and Health Statistics (NCVHS), "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security refers to physical,

ISSN: 1941-6679-On-line Copy

technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" (NCVHS, 2006).

Not only do apps enable data sharing with doctors (healthcare providers) for a healthy doctor-patient relationship but also with the patient's insurance company, lifestyle coaches, athletic coaches, family and friends which raises a lot of privacy concerns (Avancha et al., 2012). Apps provide the ability to share data with third party organizations (Dredge, 2013) such as advertisers, or payment service partners (Vodafone Group 2013), risking the confidentiality of consumers' data.). Studies have highlighted that data security and invasion of privacy are the major factors that inhibit the users from using Electronic Health Records (EHR's) (Yuksel et al., 2017; Pussewalage & Oleshchuk, 2016). A study of 43 fitness apps revealed that 74% of the free apps and 60% of the paid apps had a privacy policy which was available either in the app or on the developer's website. This study observed that, only 25% of the free apps and 48% of the paid apps informed consumers about the privacy policy (Mc Carthy, 2013). The main objective of this study is to focus on the issues related to privacy risks and security threats with use of mHealth apps. In order to meet the objective, the following research questions have been formulated.

Table 2. Research Questions and Methodology

	Research Question (RQ)	Motivation	Methodology
RQ1.	What are the general privacy and security concerns underlying the use of mHealth apps and what are the measures that can be used to address them?	This question allows us to get an overview of the different privacy and security concerns prevalent in mHealth apps usage and what measures can be taken to avert them.	Literature review is used to identify the factors related to privacy risks and security threats in the use of mHealth apps and the measures used to address them.
RQ 2.	What are the privacy and security features that the current mHealth apps address?	This question permits us to study the privacy risk and security features available in the mHealth apps.	In-app documentation, Privacy Policies , privacy related text on the websites of the selected apps were studied to devise a scoring model to perform a comparative analysis.

METHODOLOGY

In order to answer the first question regarding the privacy and security concerns and the measures to address them, review of literature was conducted. For this the authors sought for published papers retrieved from systems like Proquest, JSTOR and Science Direct using the following search keywords. Privacy AND security AND mobile AND health AND applications; privacy AND security AND mobile AND health AND apps; privacy AND security AND smartphones AND health. A variety of papers were returned as a part of including these terms as the search string. The two terms privacy and security were grouped together to search for papers as identifying papers solely on privacy and security led to unmanageable results. The results included papers on privacy and security in apps; laws used to address privacy in the US and EU nations, conceptual frameworks for the security of mobile health applications, encryption, safe data transfer techniques, authentication etc. The inclusion criteria for the papers decided by the researchers were: Papers published in English only; Scholarly and peer-reviewed; the search was limited to the last 7 years, from 2010-2017; the applications must have studied security and privacy in mHealth apps. The initial search across all the three systems returned high results. The researchers limited these to review and research articles. These were further narrowed down by the researchers by reading the abstracts to include only those articles where the abstracts clearly mentioned privacy and security of mHealth apps were being examined in the study. Since the inclusion/ exclusion of papers are subjective, both the researchers identified the papers independently and later cross-examined the work. Certain published papers where the researchers faced discrepancies, they mutually resolved them by studying the reading the full-length article and arriving at a consensus. Initially the systems returned 5398 papers. Out of the remaining, papers were eliminated as there were duplications and they did not meet the criteria for this study, which left the researchers with a final count of 50 papers to be included in this study to address the first question.

In order to answer the second research question, that aimed to understand the risks and safety features that the current mHealth apps address, the researchers searched the in-app documentation, Privacy Policies and websites to look of the thirty free apps under the medical category from the two app distribution platforms namely, Google Play and App store. These apps were selected based on the ranking available on the AppAnnie website. The AppAnnie website is an app market data and insights company. It was used to identify these top free medical apps in the Indian context, based on the ranking of the apps. Based on the the in-app documentation, Privacy Policies of the apps, related website privacy text a scoring model was developed to study privacy risks and the safety score . The scoring

model helped to rank the apps in terms of the privacy and safety score they meet and analyze and highlight the privacy practices across medical apps available. Finally, the last part of the study, the creation of privacy and security recommendations for mHealth apps designers and users, and conclusions to the study is provided. The following sections address the two research questions.

PRIVACY RISKS

RQ# 1 : In order to address the first research question, this section highlights a few of the Privacy Risks and Security Threats that prevail while using mHealth apps. These factors have been identified with the help of Review of Literature.

Poor Data Collection and Inappropriate Storage Mechanisms

The ubiquitous data collection of mobile devices poses serious privacy and security concerns. Apps collect operational, behavioural and sensitive information with the rationale of personalization, social interaction and sharing it with third parties for better app experience. In many cases, this information is used to push notifications and provide supervision. A study that analysed 600 most frequently used apps, found that only 183 (30.5%) had privacy policies. Two thirds (66.1%) of privacy policies failed to address the app itself (Sunyaev et al., 2015). Open platforms used for app development pose privacy policies which do not specifically address the app itself. The available privacy policies were not transparent to the users in terms of their privacy practices, required college-level literacy, and were often not focused on the app. Developers fail to inform users about how their personal data is being used or excessively demand their personal data (Ackerman, 2013). According to Pew Internet Survey, 54% of the app users have decided to not install a cell phone app when they realized the amount of personal information they would need to share in order to use it. Likewise, 30% of app users have uninstalled an app that was already on their cell phone as the app collected personal information they were reluctant to share. Not all apps have taken the appropriate steps to protect the sensitive data of sexual practices/partners and the data related to reproductive functions (Lupton & Jutel, 2015).

Disclosure of Information

mHealth apps pose similar challenges with the sheer number of people involved in the exchange of user data and in many cases, the data was not always collected with users consent (Ranchordas & Kaplan, 2016). The use of mHealth apps among users may bring significant issues, such as security and privacy challenges (Faudree

& Ford 2013). McCarthy (2013) found that many free mHealth apps send data, connect to third-party advertisers/sites, allow them to store it externally and use unencrypted connections. Some mobile apps use the internet connection to track and record a patient's condition or activity in real-time with the help of embedded sensors on their phones which can pose a security threat. Access to such data discloses detailed information about the user's habits, location, movements which further exaggerates the risks. According to a survey conducted on 23 most popular free health apps, it was found that 50 % send data to third-party advertisers and 39% send data to unidentified parties without any data encryption of which users have not been informed (HealthCareBusinessTech 2014)

SECURITY THREATS

mHealth apps which are available in the online distribution platform namely Android handle increasingly sensitive data for professionals and patients over unsecured Internet communications and third party servers. This sensitive data which is collected can be sniffed or injected or put into system logs where it is not secured. In many cases these unencrypted files are stored on SD card which are accessible by any other app. Android app components, intended to be private, and are set as exported, making them accessible by other apps. Sensitive information can be inferred by a malicious app. With mHealth apps, the attack areas that need protection are Internet, Third Party Services, Bluetooth, Logging, SD Card Storage, Exported Components, and Side Channels. (He et al., 2014).

Data Encryption

Encryption is defined as the form of converting text into a format that is difficult to understand by an unauthorized user. Apps that do not exercise encryption, pose the risk of exposing data to any unauthorized user or be hacked, stolen or displayed in an inappropriate location. This risk is aggravated if the device has malware or spyware (Schulke, 2013). In a study of 43 health and fitness apps, none of the free apps while only a few paid apps encrypted the users data collected by the apps (McCarthy, 2013).

Vulnerability of the Device

Users takes steps to maintain control over their personal data however, lost mobile phones or lack of security authentication pose higher privacy and security concerns Mobile phones could fall into wrong hands. A research reports that 31% of mobile

ISSN: 1941-6679-On-line Copy

owners have lost their phone or had it stolen, while 12% of mobile phone owners say that another person has accessed their phone's contents in a way that made them feel that their privacy had been invaded. Many users back up the data on their phone as a safeguard in the event of loss or stolen phone. Despite the fact that backing up one's phone is typically conducted as a safeguard in the event that the phone is lost or stolen, cell owners who have actually experienced a lost or stolen phone are no more likely than average to back up the contents of their phone.(Pew Internet Report)

Data Security Breaches

A survey by Beckers Hospital Review (2014) revealed that the risk of data breaching is the most worrying and impeding aspect to mHealth adoption. Figg and Kam (2011) pointed out that data breaches in healthcare are common where many doctors now are able to view patient's records without their knowledge which could further lead to medical identity theft. Data breaches occur when medical records are stored or are transmitted from one server to another. In order to avoid this data encryption techniques need to be used (Bhuyan et al., 2017). Also, privacy and security concerns on patients' clinical data have been widely acknowledged as being significantly critical to the widespread adoption of mobile technologies in various healthcare domains (Farzandipour et al., 2010). The consequences of breach of data can be very significant.

The following diagram gives a summary of the Privacy Risks and Security Threats prevalent in the use of mHealth apps.

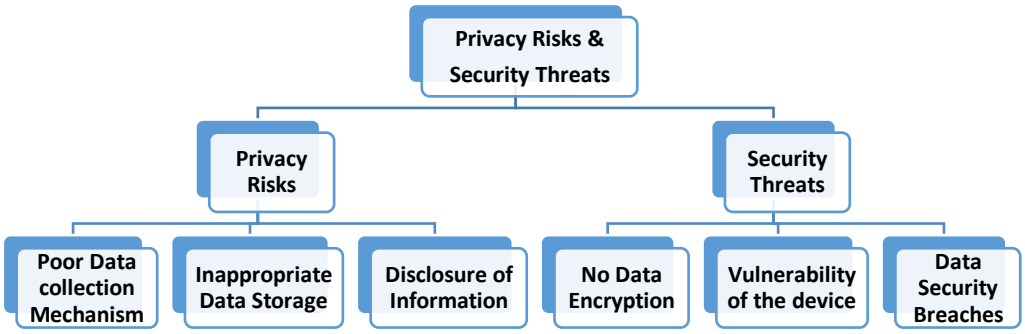

Fig 1. Privacy and Security Threats in mHealth app usage

As suggested in various studies, the following table represents the privacy risks and security threats and the measures that can be taken to avert the privacy risks and security threats that can hinder the adoption of mHealth apps by users (Refer Table 2).

Table 3. Measures to take to avoid privacy and security risks while using mHealth apps

Privacy Risks & Security Threats	Measures to Take
Data Collection Procedure (Arora, 2014)	Familiarize users with the data that is being collected and educate them what the collected data can be used for. Provide options to control what data users can share
Data Storage (PRC,2016; Jain and Shanbaug, 2012; He at al., 2014)	Apps to store data remotely, such as on a secure server or in a cloud. Secure data storage and personal and sensitive information by encrypting or authenticating it with username and password
Data Transmission (PRC,2016; Addonizio, 2017)	Users to prohibit accessing data over unsecured Wi-Fi network or hotspot
Data Accessibility (Adhikari et al.,2014;	App developers to enable password authentication, One-Time Password for users to access the apps
Data Encryption (Arora, 2014; Wirth, 2012;Yang et al., 2014; Borja et al., 2015; Addonizio, 2017; Jain & Shanbaug, 2012; He at al.,2014))	App developers to use WPA2 and 128-bit key encryption. It is advised to add a tag or header to the encrypted message. Encrypting the data guarantees that only authorized users can decipher it. Applications can encrypt sensitive data in transit end-to-end via SSL/TLS encryption mechanisms
Data Breach (Adhikari et al.,2014; Figg & Kam 2011;)	Users to install firewalls and anti-virus to protect against virus/malware based attacks and malicious applications.

RQ# 2: In order to address the second Research Question, thirty mHealth apps present across the two app distribution stores namely Google Play for Android and App Store for iOS users were studied. The process to address the second research question involved the following steps.

ISSN: 1941-6679-On-line Copy

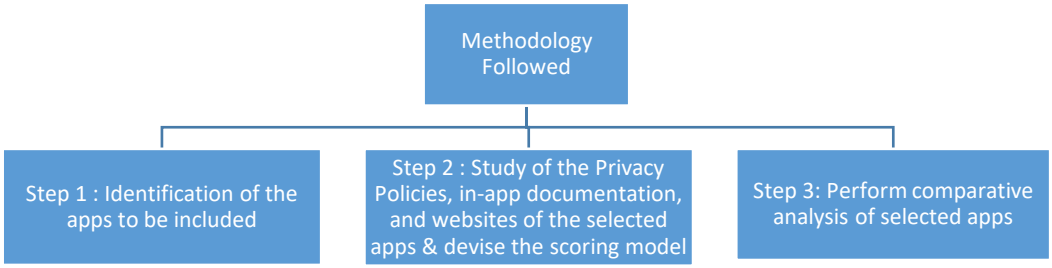

Fig 2. Methodology followed for addressing Research

Question 2
Step 1: Identification of the apps:

Apps that belonged to the Medical category from both the app distribution stores in India were selected for the purpose of this study. App Annie was used to identify the top fifteen mHealth apps from both the app stores. App Annie is an app market data and insights company which produces consumer and competitive information on downloads, revenue, ratings, usage, search terms, etc. that aids in improved decision making (App Annie, 2017). The App Annie website was accessed on 25th September 2017. The top fifteen free apps on the App Annie website from the Google Play store in India belonging to the medical category were selected.

These apps are described below.

Table 4. Top 15 apps in the Medical category from Google Play in App Annie

Sr.No.	Name of the App	Description
1	1mg	1mg is an e-commerce health care company based in Gurgaon, Haryana, India. It operates an online marketplace for medicines, facilitates medical appointments, consult doctors online and diagnostic test bookings. The health app tells one about the medicines, their substitutes and side effects.
2	Blood Group Detector Prank	An application for all android users which detects their fake blood group showing random results by simply scanning the finger prints. This is an interesting entertainment application that make fun with your friends and family.
3	DocsApp (Consult	This app helps Indians to consult MD specialist doctors on demand within 30 minutes without booking appointment.

	Doctor 24x7)	
4	Netmeds (India Ki Pharmacy)	This app allows users to conveniently place orders for medicines anytime, anywhere in India. It can be used to reorder medicines, Track orders, Rate Items, Check Reward Points and contact the company when on the go.
5	Practo your home for health	This app helps book doctor appointments, consult doctors online, order medicines online, maintain detailed digital medical records, and subscribe to health tips in order to stay healthy.
6	Lybrate Consult a Doctor	It is a medical platform connecting over 10 million users to over 100,000 top Doctors and pathology labs. One can ask a FREE question about any health or fitness query and get multiple helpful answers from the best doctors within a few minutes
7	Medlife Delivering Medicines	This app enables customers to order medicines online from the comfort of their homes, get free delivery within 24 to 48 hours and get good discount on the order.
8	Ada Your health Companion	Ada is a personal health companion app designed by a dedicated team of doctors and computer scientists to help understand the symptoms, answer personalized, simple questions and get relevant information.
9	PharmEasy	It is the India's largest subscription pharmacy where users can order healthcare products, OTC products and medicines (on valid prescriptions) and get them delivered to your doorstep. It also has provisions where users can book health tests and packages from the convenience of their home.
10	Dr.Lal PathLabs	Dr. Lal PathLabs provides patients to book a home collection from a list of 350+ Pathalogy tests
11	MedPlus Medicines and Grocery	MedPlus online Pharmacy/ medicine and General store app helps users order medicines and general products conveniently. All orders are filled within 6 hours during the regular business hours and on the next day for evening or weekend orders
12	Blood Group Checkup Prank	This is an entertainment prank app for detecting blood groups of various users.
13	Blood Sugar Test	This app is for entertainment and playing pranks as it is easy to use. It scans and detects your blood sugar and provides features to share it with other users.
14	Skin diseases and treatment	This app is a collection of skin diseases and its treatment in Hindi.

ISSN: 1941-6679-On-line Copy

15	The AIIMS App	This app helps to book appointments, get video consultation, upload lab reports, share and keep all health records in one place.

The top fifteen free apps from the App Annie website from the Apple App store belonging to the Medical category were selected. These are described below. The apps that were in common with those available in Google Play have been eliminated to include more apps.

Table 5. Top 15 apps in the Medical category from App Store in App Annie

Sr.No.	App Name	Description
1	DOCTOR INSTA- Consult Online -	DOCTOR INSTA provides focused care being in the confine of your home or office. It is equipped with video and phone capabilities which help specialists to engage with the patient to diagnose issues and provide an effective treatment plan.
2	Myra Medicines	An online pharmacy that helps you to buy medicines, baby care, dental and hygiene products in under an hour and offers great discounts.
3	Star Health Insurance App	Star Health Insurance Company has launched mobile app which helps in instant policy renewal, find a hospital close by, locate branch office in the vicinity, get quote for various products etc.
4	Medscape	This app provides fast and accurate clinical answers at the point-of-care and is the leading medical resource for physicians, medical students and other healthcare physicians.
5	Medical Dictionary	This app is an iOS dictionary app that gives one instant access to 180000 medical terms over 50000 audio pronunciations and 12000 images, from authoritative sources.
6	Visual Anatomy 3D	This app is an interactive visual guide for learning and understanding human anatomy. Helps to get a quick and complete 3 dimensional understanding of all muscles, bones and organs of the human body.
7	Practo Pro	An app for doctors that makes healthcare simpler for doctors and patients alike.
8	Porn and Sex Addiction Support	This app supports people with porn and sex addiction by interacting with people all over the world by chatting, watching videos or listening to podcasts.
9	Sminq	This app helps to book appointments with the doctors without any wait. It provides live status and alerts of the queue remotely.
10	Medical dictionary and	This app provides free, instant access to in-depth information on 4000+ prescription drugs and over-the-counter medications in a drug dictionary trusted by healthcare professionals.

	Prescription Drug Guide	
11	Lecturio (Med school study app)	This app is a single point resource for medical school where students can learn with videos, memorize with recall questions, reinforce with textbook articles and prepare for board-style questions.
12	myForits	This app helps the Fortis customers to connect with Fortis Hospital network to book appointments, receive alerts related to appointments, maintains profile, emergency and medical contacts etc.
13	Blood Pressure (Smart Blood Pressure (SmartBP) BP Tracker)	Smart Blood Pressure (SmartBP) BP Tracker- This app allows users to record, track, analyze and share your Blood Pressure information using your iPhone/iPod touch/iPad devices (check compatibility requirements). It connects with Apple HealthKit and Microsoft HealthVault. With your health information at your fingertips, you can now take a more active role in your own health.
14	LifCare Pharmacy	This app is a subscription Pharmacy for chronic patients which helps them to take medicines for various health-related conditions. Provides free delivery and heavy discounts, ensures monthly refills and better patient adherence to medication.
15	Pregnancy+	This app helps track one's pregnancy and share it with family members. It provides beautiful interactive images and maintains all information regarding the baby. This includes doctor visits, kick counters, contraction timer, baby names, baby size, week by week information on pregnancy etc.

Step 2: Study of the Privacy Policies of the selected apps:

The researchers searched the in-app documentation, Privacy Policies of the apps and visited related website to study privacy related texts of the shortlisted apps in Step 1. Issues related to privacy include unauthorized collection of data, data breach, data storage and sharing mechanisms which have been pointed out in the literature. From the literature the researchers identified certain parameters and grouped them as Privacy risks (PR1-PR4) and Safety Measures (SS1-SS6) to develop a scoring model. 1 point was marked for the presence of the feature and a 0 was allocated for the absence of the feature. These were further aggregated to arrive at a final score for Privacy Risks score and the Safety Score based on which they could be compared. The criteria for the Privacy Risks include (PR1-PR4)

- PR1: Does the app ask for the user details during the Registration Process (Personal Information Collection)
    - While examining the Privacy policies of the apps it was observed that the apps collect information such as contact data (name, user-id, email address, postal address, phone number), demographic data (gender, date of birth, and pin-code), data regarding the usage of the services and history of the appointments, valid financial account information and other details as the user may volunteer. This vast amount of data when revealed can pose privacy concerns.
- PR2: Does the app store data about the users? (Data Storage).
    - Most apps store information about their users in electronic form either on cloud or on its equipment or on the equipment of its employees. In some cases this information may be converted into physical form. User's data when stored in any form on devices or cloud can pose several risks.
- PR3: Does the app Store browsing data (Internet Access details)
    - Apps maintain the user's browsing history including the URL of the site that the user visited prior to visiting their website, the IP address of the browsing computer, the user's operating system , type of web browser, the User's ISP, use of temporary cookies for user administration.
- PR4: Disclosure of information to third parties (Access to Third Party)
    - Most apps disclose user information to third parties for the purpose of targeted marketing. Customization of the website and to carry out certain services

The criteria to assess the Security features mentioned as the Safety Score include (SS1-SS6):

- SS1: Does the app allow users to update or correct the details they want to share?
    - Users may wish to modify, correct, and delete the personal information provided by them. Allowing users with these features ensures they have a control of the information they share.
- SS2: Does the app allow users to completely delete any personal information?
    - When consumers quit using an app they should be able to delete all the data related to them on the app such as their profile or any data archives that have been created.
- SS3: Does the app retain user information (Retention of Information)
    - Some apps store the user information on their equipment or on the employees' equipment in electronic form. They may also share this information with the sellers to improve sales of the products.
- SS4: Does the app follow security practices and procedures? (Data encryption)

    - Data encryption ensures that the data if intercepted or breached will not make sense to the infiltrator except the intended recipient.
- SS5: Does a privacy policy for the app exist?
    - The privacy policy is essential for all the apps that assess, collect and transmit personal information from users to app owners.
- SS6: Does the app ask for user authentication?
    - Unauthorized access to health information is a serious threat to the privacy and security. Ensuring user authentication by means of username, password ensures the right person has access to user information.

ISSN: 1941-6679-On-line Copy

Table 6. Scoring model for the top 15 apps in Medical category from Google Play app store in India

Name of the app in the Medical category	Name of the developer	Star Rating	Rating	PR1	PR2	PR3	PR4	SS1	SS2	SS3	SS4	SS5	SS6	Privacy Risk score out of 4	Safety score out of 6
1mg	1mg Technologies	4.2	87104	1	1	1	1	1	1	1	1	1	1	4	6
Blood Group Detector Prank	DaniPani Apps	3.2	4251	0	0	0	0	0	0	0	0	0	0	0	0
DocsApp - Consult Doctor Online 24x7 on Chat/Call	DocsApp	4.4	19421	1	1	1	1	0	0	1	0	1	1	4	3
Netmeds - India Ki Pharmacy	NETMEDS	4.4	38607	1	1	1	0	1	0	1	1	1	1	3	5
Practo - Your home for health	Practo	4.3	63505	1	1	1	1	1	0	1	1	1	0	4	4
Lybrate - Consult a Doctor	Lybrate	4.3	51521	1	1	1	1	1	0	1	0	1	1	4	4
Medlife - Delivering Medicines	Medlife International Pvt. Ltd.	4	7984	1	1	0	1	1	0	1	0	1	1	3	4
Ada - Your Health Companion	Ada Health	4.7	30252	1	1	1	1	1	1	1	0	1	1	4	5
PharmEasy - Healthcare App	91streets Media Technologies Pvt. Ltd.	4.1	14451	1	1	1	1	1	0	1	1	1	1	4	5
Dr Lal PathLabs	Dr Lal PathLabs	4.5	2536	1	1	1	1	1	0	1	1	1	1	4	5
MedPlus - Medicines & Grocery	MedPlus Health Services Pvt. Ltd	3.7	4952	1	1	1	0	1	0	1	1	1	1	3	5
Blood Group Checkup Prank	HighApps	3.2	1793	0	0	0	0	0	0	0	0	0	0	0	0
BloodSugar Test	HighApps	3.9	941	0	0	0	0	0	0	0	0	0	0	0	0
Skin diseases and treatment	Jai Tuto	4.1	296	0	0	0	0	0	0	0	0	0	0	0	0
The AIIMS App	OyeHelp Aiims	4	453	1	1	1	0	0	0	1	1	1	0	3	3

Table 7. Scoring model for the 15 apps in the Medical category from App Store in India

Name of the app in the Medical category	Name of the developer	Star Rating	Rating	PR1	PR2	PR3	PR4	SS1	SS2	SS3	SS4	SS5	SS6	Privacy Risk score out of 4	Safety score out of 6
Myra Medicines	MetaRain	4	48	1	1	0	1	1	0	1	0	1	1	3	4
Star Health insurance app	Digit secure India Pvt.Ltd.	1.5	14	1	1	0	1	1	0	1	0	1	1	3	4
Medscape	webmd	4.1	7	1	1	1	1	1	0	1	0	1	1	4	4
Medical dictionary - Healthcare Terminology	farlex	4.2	47	0	0	1	1	0	0	0	1	1	0	2	2
Visual anatomy 3D	GraphicVizion	4	10	0	0	1	1	0	0	0	0	1	0	2	1
Practo Pro	Practo Technologies Private Limited	4.2	635	1	1	1	1	1	0	1	1	1	1	4	5
Porn and Sex Addiction Support	Social Systems LLC	3.5	50	1	1	1	1	0	0	1	0	0	1	4	2
Sminq	Sminq India Solutions Private Limited	3.5	9	1	1	1	1	1	0	1	0	1	1	4	4
Medical dictionary and Prescription Drug Guide	Farlex	4.5	16	0	0	1	1	0	0	0	1	1	0	2	2
Lecturio- Med school study app	Lecturio GmBH	4	11	1	1	1	1	1	1	0	0	1	1	4	4
myForits	Fortis healthcare Limited	1.5	14	1	1	1	1	1	0	1	0	1	1	4	4
Blood Pressure - Smart Blood Pressure (SmartBP) BP Tracker	Evolve Medical Systems, LLC	4.5	19	1	1	1	1	1	0	1	1	1	1	4	5
LifCare Pharmacy	CornerStone	3.5	10	1	1	1	1	1	1	0	0	1	1	4	4
Pregnancy+	Health Monitoring	4.5	201	1	1	1	1	1	1	1	1	1	0	4	5

Step 3: Perform Comparative analysis of the selected apps

A variety of apps belonging to the Medical category in both the app distribution stores have been examined ranging from apps that disseminate health information to online pharmacies to apps that book doctor's appointments online. The in-app documentation, Privacy Policies of the apps and documents on the website were visited to study privacy related texts of the apps to cull out information related to the features relevant to this study. If the parameter was present in the privacy policy of the app, it was awarded a point. If the parameter was absent, it scored a zero. Based on this methodology a final score for each of them was arrived at for all the

30 apps. This score helped compare how the apps differed in terms of the risks that they exposed the users to and also the security measures they had in place.

From the two tables above we notice that most of the apps collect user information and store it as a part of registration. The details collected range from name, age, gender to linking the app with the users social media accounts. Apps that disseminate information about diseases usually do not ask users to register on the app. Of the apps studied in this research, 74% of the apps on Google Play store and 80% apps in the App Store, collect and store the customer information. This is used to provide them with a personalised experience when they use the app the next time. From the apps that formed a part of this study, 67% of the apps in Google Play store and 87 % of the apps in the App Store collect users browsing data such as their domain name and IP address. Some apps also use cookies so that users need not enter the same information repeatedly. Apps consult with third parties to provide a host of services. Privacy Risk scores of the apps are rated out of 4. The higher the score obtained here indicates that these apps pose a risk in protecting the privacy of the users as they may expose the user collected data to various risks.

Apps from the Google Play store such as 1mg, DocsApp, Practo, Lybrate, Ada, PharmEasy, Dr Lal Path Labs and apps that belonged to App Store namely Medscape, PractoPro, Porn and Sex Addiction support, Sminq, Lecturio, myFortis, Blood Pressure, Lifecare Pharmacy, Pregnancy+ scored four points on the privacy risk score indicating they collected users data, stored it, shared it with third parties and also accessed the users internet browsing history.

The safety score is a measurement of the safety practices these apps follow in order to ensure that these apps give users the ability to completely delete their personal information from the app, the app follows data encryption methods and have appropriate authentication practices. Only one app, 1mg among the 30 studied had taken sufficient measures to ensure the safety risks of the patients are minimized and thus, it scored 6 on these parameters as against any of the other apps. As a part of apps included in this study, none of the apps that belong to the App store met the required safety score of 6. Apps that have managed to keep the safety of users in mind scoring a 5 in the Google Play store are Netmeds, Ada, Pharmeasy, Dr. Lal PathLabs, MedPlus and apps such as Practo Pro, Blood Pressure and Pregnancy + in the App store, indicating that adequate measures are taken to ensure that the users data is kept secure.

All apps in App Store, that are a part of this study, provide access to third parties whereas 54 % of the selected apps from Google Play Store do the same. 60% of the apps on Google Play and 74% of the apps on Apple Play Store provide users with

the ability to update their details on the apps/websites by sending requests for the modification/ updation of the data. 14% of the apps on Google Play and 20% of the apps on Apple Play Store provide users with the ability to completely delete their details on the apps/websites by sending requests for the deletion of the data from their databases.

80% of the apps on Google Play and 60% of the apps on Apple Play Store retain user data on their system or employees' system. 47% of the apps on Google Play and 34% of the apps on Apple Play Store encrypt the user data before transmitting it, which ensures that the data is not deciphered by any unintended recipient.

73 % of the selected apps in Google Play store and 94% of the apps selected from Apple App store have a privacy policy, but the data collection method they employ to collect data is risky as the risk score for most of the apps is high. Users must be made aware of the data that these policies aim to collect and use.

Only 40% of the selected apps from the Google Play Store and 20 % of the selected apps from the Apple App store have a safety score ranging from 83% to 100% which is alarming. These risks need to be mitigated and uniformity in the guidelines be adopted for all the apps.

RESULTS

According to this study, there is a clear evidence of variation in the privacy policies of the mHealth apps belonging to the medical category in terms of content quality, functionality and security features offered, across the two app distributions stores. The use of mHealth apps for self-management in developing nations like India can help to ease the burden of the rising healthcare costs, provided they do not leave users vulnerable to cyber-attacks. The consequences of cyber-attacks can be severe for conditions such as HIV or AIDS (Knorr et al., 2015). This poses concerns about the certification process of the apps. Lack of standard app development guidelines raises many security questions about the mHealth apps (Kharrazi et al. 2012). Similar to the findings of (Ranchordas & Kaplan, 2016), this study highlighted that the healthcare policies are fragmented and incomplete which underlines the need for more clarity and certainty for mHealth to be an empowerment tool.

From this study, it is noted that areas that need attention are deletion of personal information from the app once the user has uninstalled the app and better data encryption practices. In this study, it was observed that some apps did not have a privacy policy. Mobile vendors must mandate the need for apps to have privacy

ISSN: 1941-6679-On-line Copy

policies (Knorr et al., 2015). A study by Sunyaev et al., (2015) indicated that privacy policies have poor availability rates, correlation of app ratings and privacy policy availability is weak, privacy policies lacks scope and transparency. The developers need to start self-regulating by developing policies that provide disclosures and notices, and share information about the app users with necessary third parties upon receiving an affirmation from the user (Addonizio, 2017). The selected apps saw a lack of encryption standards which indicated that security was not a top priority for the developers.

DISCUSSION

The consumers must examine the app before they download it to understand the level of information that the app requests for. This can be done based on the basis of the privacy policy if there exists one for the app or based on the reviews by other app users (Ranchordas & Kaplan, 2016). The data collected by the app may be provided to the third parties, advertisers, marketers to provide better services. Users can customize the settings which will potentially restrict the amount of information disclosed to the apps. Consumers must consider downloading those apps that offer better privacy protection, even if they charge a fee for the same. If the user wishes to discontinue using an app altogether, it is recommended to drop a mail to the provider to delete/ destroy the sensitive personal information which prevents unauthorized use of stored data. App developers must invest time and efforts in framing app development policies. Likewise the app distribution stores can enforce the existence of privacy policies to be listed under the health section (Knorr et al., 2015). Developers must expend time and effort in formulating the Privacy Policies for healthcare apps (Sunyaev et al., 2015; Dehling et al., 2015; Zhang et al., 2015)
The first limitation is the number of apps that were used for this study. Selected thirty apps that belonged to the app distribution platforms in India were a part of this study. Future studies could examine apps that have high download rates. Further empirical studies are needed to examine how the familiarity with using mHealth apps affects user's attitude towards the privacy and security of mHealth apps. Also, this study recommends that a more nuanced and contextual framework of mHealth privacy and security for users is required. Further empirical work can also examine the attitude to the safety, security, and privacy problems of mHealth app users and reasons why developers create insecure apps.

CONCLUSION

There is a need for a secure healthcare environment which can be achieved by adopting standard guidelines to develop these apps that will foster trust among mHealth app users and developers (Faudree & Ford 2013). Regulation in India for mHealth app development is at a nascent stage and there is a need for stringent regulations to be incorporated in order to develop and protect the interests of the people to avoid unforeseen conditions (Kotlo et al., 2015).Creating a regulatory framework, will help address the challenges the apps face and having a government and legal framework for their use in clinical practice would help avoid the security risks (Marley and Farooq, 2015). Regulators must develop standards that the developers need to adhere to ensure privacy and security of users is not compromised (Huckvale et al., 2015).

The potential of mHealth will not be realized if patients are deterred to use these apps due to lack of Trust (Huckvale & Car, 2014). Involvement of healthcare professionals in the evaluation of functionality, usability and security will enhance the trustworthiness of the apps and increase their adoption. Developers, healthcare professionals must work together to establish standards and develop clear guidelines for app development (Adhikari et al., 2014). mHealth will be adopted by people provided people have trust the system. A good mhealth policy should inform the users of what data is collected, how it is stored and used. This study aims to enlighten the users to take caution when using mHealth apps at the same time recommends the app developers to educate the users with the information being collected about them and how it is being put to use. This will enable them to weigh the benefits and risks of using mHealth apps. These privacy and security concerns need to be addressed by all the stakeholders' right from the manufacturers of the devices, developers who make these remote monitoring systems, to policy makers to ensure data privacy and security in the healthcare system is not compromised.

REFERENCES

Ackerman, L. (2013). Mobile health and fitness applications and information privacy. *Privacy Rights Clearinghouse, San Diego, CA*.

Adhikari, R., Richards, D., & Scott, K. (2014). Security and privacy issues related to the use of mobile health apps. ACIS.

Addonizio, G. (2017). "The Privacy Risks Surrounding Consumer Health and Fitness Apps, Associated Wearable Devices, and HIPAA's Limitations"

Akter, S., & Ray, P. (2010). mHealth-an ultimate platform to serve the unserved. Yearb Med Inform, 2010, 94-100.

AlHamad, A. Omari, F., & AlHamad, A. (2014). Recommendation for Managing Patients' Privacy in an Integrated Health Information Network, *Journal of IT and Economic Development*, 5(1), 47-52.

Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol research: current reviews*, *36*(1), 143.

Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. ACM Computing Surveys (CSUR), 45(1), 3. http://dx.doi.org/10.1145/2379776.2379779

Bhuyan, S. S., Kim, H., Isehunwa, O. O., Kumar, N., Bhatt, J., Wyant, D. K., ... & Dasgupta, D. (2017). Privacy and security issues in mobile health: Current research and future directions. *Health policy and technology*, *6*(2), 188-191.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. New Media & Society, 11(3), 395-416. http://dx.doi.org/10.1177/1461444808101618

Dehling, T., Gao, F., Schneider, S., & Sunyaev, A. (2015). Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. *JMIR mHealth and uHealth*, *3*(1).

Dredge, S. (2013) Yes, those free health apps are sharing your data with other companies. The Guardian.com, Accessed 28 September 2017 from http://www.theguardian.com/technology/appsblog/2013/sep/03/fitnesshealth-apps-sharing-data-insurance.

Emmnauel, U., & Mohammed, T. (2017). Cyber security, threat intelligence: Defending the digital platform. *Journal of International Technology and Information Management*, 26(1), 138-160.

Faudree, B., & Ford, M. (2013). Security and Privacy in Mobile Health. *CIO Journal*.

Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. *Journal of medical systems*, *34*(4), 629-642.

Figg, W.C., Ph.D, and Kam, H.J., M.S. 2011. "Medical Information Security," International journal of Security (IJS) (5:1).

He, D., Naveed, M., Gunter, C. A., & Nahrstedt, K. (2014). Security concerns in Android mHealth apps. In *AMIA Annual Symposium Proceedings*(Vol. 2014, p. 645). American Medical Informatics Association.

HealthCareBusinessTech. 2014. "Mobile Health Apps Create Privacy Risk, Study Says." Retrieved 27 September - 2017, from http://www.healthcarebusinesstech.com/mobile-health-apps-privacy/

Huckvale, K., & Car, J. (2014). Implementation of mobile health tools. Jama, 311(14), 1447-1448.

Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P. J., & Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC medicine*, *13*(1), 214.

Istepanian, R., Laxminarayan, S., & Pattichis, C. S. (2006). *M-health*. New York, NY: Springer Science+ Business Media, Incorporated.

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*(5), 28-33.

Kay, M., Santos, J., & Takane, M. (2011). mHealth: New horizons for health through mobile technologies. *World Health Organization*, *64*(7), 66-71.

Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: an evaluation of features and functionality. *International journal of medical informatics*, *81*(9), 579-593.

Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic commerce research and applications*, *9*(1), 84-95.

  ISSN: 1941-6679-On-line Copy

Knorr, K., Aspinall, D., & Wolters, M. (2015, May). On the privacy, security and safety of blood pressure and diabetes apps. In *IFIP International Information Security Conference* (pp. 571-584). Springer, Cham.

Kotlo, A., Muragundi, P. M., Ligade, V. S., & Udupa, N. (2015). Regulation of the mobile medical apps in india: Need of the hour. *Current Pharma Research*, *5*(4), 1600-1606.

Lee, C. H., Eze, U. C., & Ndubisi, N. (2011). Analyzing key determinants of online repurchase intentions. Asia Pacific Journal of Marketing and Logistics, 23(2), 200-221. http://dx.doi.org/10.1108/13555851111120498

Lederer, S., Mankoff, J., & Dey, A. K. (2003, April). Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems (pp. 724-725)*. ACM.

Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. Communications of the AIS, 28, 453–496

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 501-510). ACM.

Lupton, D., & Jutel, A. (2015). 'It's like having a physician in your pocket!'A critical analysis of self-diagnosis smartphone apps. *Social Science & Medicine*, *133*, 128-135.

Marley, J., & Farooq, S. (2015). Mobile telephone apps in mental health practice: uses, opportunities and challenges. *BJPsych Bull*, *39*(6), 288-290.

McCarthy, M. (2013) Experts warn on data security in health and fitness apps. British Medical Journal (f5600), http://www.bmj.com/content/347/bmj.f5600 (accessed 25 February 2017).

McAllister, N. (2014) Free of paid, Android or iOS, your apps are spying on YOU - report. The Register, http://www.theregister.co.uk/2014/02/21/appthority_app_privacy_study/ (accessed 16 March 2015).

Mechael, P. N. (2009). The case for mHealth in developing countries. *Innovations: Technology, Governance, Globalization*, *4*(1), 103-118.

Olmstead, K. (2014, April 29). Mobile apps collect information about users, with wide range of permissions. Retrieved from http://www.pewresearch.org/fact-tank/2014/04/29/mobile-apps-collect-information-about-users-with-wide-range-of-permissions/

Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, *36*(6), 1161-1173.

Ranchordas, S., & Kaplan, B. (2016). MHealth for Alzheimer's Disease: Regulation, Consent, and Privacy Concerns.

Rebolj, D., Menzel K.,(2004).Mobile computing in construction, ITCon 9, 281–283.

Schulke, D. F. 2013. "The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing," *Boston University Law Review* (93:5).

Schulke, D. F. (2013). The regulatory arms race: Mobile-health applications and agency posturing. *BUL Rev.*, *93*, 1699.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (pp. 2347-2356). ACM.

Subramanian, Ramesh (2017) "Emergent AI, Social Robots and the Law: Security, Privacy and Policy Issues," *Journal of International Technology and Information Management*: Vol. 26(3), Article 4.

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 22(e1), e28-e33.

  ISSN: 1941-6679-On-line Copy

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, *68*, 1-13.

Zorotheos, A., & Kafeza, E. (2009). Users‟ perceptions on privacy and their intention to transact online: A study on Greek internet users. Direct Marketing: An International Journal, 3(2), 139-153. http://dx.doi.org/10.1108/17505930910964795

Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., & Luo, H. H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. *IEEE Wireless Communications*, *22*(4), 104-112.

WEB REFERENCES

Statistica[1]: Number of smartphone users worldwide from 2014 to 2020 (in billions): Number of smartphone users worldwide from 2014 to 2020 (in billions). (n.d.). Retrieved November 10, 2017, from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Statistica[2]: Number of apps available in leading app stores as of March 2017[2]: Number of apps available in leading app stores as of March 2017 (n.d.). Retrieved October 11, 2017, from https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Statistica[3]: **No. of apps downloaded from App stores:** Cumulative number of apps downloaded from the Apple App Store from July 2008 to June 2017 (in billions). (n.d.). Retrieved October 15, 2017, from https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/

Definitions of Privacy and Security:
https://www.cdc.gov/nchs/data/ncvhs/ncvhs06-08.pdf Accessed 20th September 2017

PRC, 2016 : https://www.privacyrights.org/printpdf/67502 Accessed 31st march,2018

Google Play: Manifest.Permission
https://developer.android.com/reference/android/Manifest.permission.html
Accessed 24th September 2017

App Annie Link for Google Play store:
https://www.appannie.com/apps/google-play/top-chart/?country=IN&category=24&device=&date=2017-09-25&feed=All&rank_sorting_type=rank&page_number=0&page_size=100&order_type=desc&order_by=sort_order&table_selections

App Annie Link for Apple App store:
https://www.appannie.com/apps/ios/top-chart/?country=IN&category=6020&device=iphone&date=2017-09-25&feed=Free&rank_sorting_type=rank&page_number=0&page_size=100&order_type=desc&order_by=sort_order&table_selections=&metrics=grossing_rank,category,all_avg,all_count,last_avg,last_count,first_release_date,last_updated_date,est_download,est_revenue,wau

ISSN: 1941-6679-On-line Copy