Original Paper

Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android

Tobias Dehling, Dipl -Wirt -Inf; Fangjian Gao, MSc; Stephan Schneider, Dipl -Wirt -Inf; Ali Sunyaev, PhD

Department of Information Systems, Faculty of Management, Economics and Social Sciences, University of Cologne, Cologne, Germany

Corresponding Author:
Ali Sunyaev, PhD
Department of Information Systems
Faculty of Management, Economics and Social Sciences
University of Cologne
Albertus-Magnus-Platz
Cologne, D-50923
Germany
Phone: 49 221 4705397
Fax: 49 221 4705386
Email: sunyaev@wiso.uni-koeln.de

Abstract

Background: Mobile health (mHealth) apps aim at providing seamless access to tailored health information technology and have the potential to alleviate global health burdens. Yet, they bear risks to information security and privacy because users need to reveal private, sensitive medical information to redeem certain benefits. Due to the plethora and diversity of available mHealth apps, implications for information security and privacy are unclear and complex.

Objective: The objective of this study was to establish an overview of mHealth apps offered on iOS and Android with a special focus on potential damage to users through information security and privacy infringements.

Methods: We assessed apps available in English and offered in the categories “Medical” and “Health & Fitness” in the iOS and Android App Stores. Based on the information retrievable from the app stores, we established an overview of available mHealth apps, tagged apps to make offered information machine-readable, and clustered the discovered apps to identify and group similar apps. Subsequently, information security and privacy implications were assessed based on health specificity of information available to apps, potential damage through information leaks, potential damage through information manipulation, potential damage through information loss, and potential value of information to third parties.

Results: We discovered 24,405 health-related apps (iOS; 21,953; Android; 2452). Absence or scarceness of ratings for 81.36% (17,860/21,953) of iOS and 76.14% (1867/2452) of Android apps indicates that less than a quarter of mHealth apps are in more or less widespread use. Clustering resulted in 245 distinct clusters, which were consolidated into 12 app archetypes grouping clusters with similar assessments of potential damage through information security and privacy infringements. There were 6426 apps that were excluded during clustering. The majority of apps (95.63%, 17,193/17,979; of apps) pose at least some potential damage through information security and privacy infringements. There were 11.67% (2098/17,979) of apps that scored the highest assessments of potential damages.

Conclusions: Various kinds of mHealth apps collect and offer critical, sensitive, private medical information, calling for a special focus on information security and privacy of mHealth apps. In order to foster user acceptance and trust, appropriate security measures and processes need to be devised and employed so that users can benefit from seamlessly accessible, tailored mHealth apps without exposing themselves to the serious repercussions of information security and privacy infringements.

(JMIR mHealth uHealth 2015;3(1):e8) doi:10.2196/mhealth.3672

KEYWORDS

mobile health; mobile apps; data security; software and application security; patient privacy; health information technology

Introduction

mHealth Apps

Mobile health (mHealth) leverages various wireless technologies to provide health-related information and services on diverse mobile devices and is a promising subset of health information technology (IT) [1-6]. mHealth has the potential to alleviate global health burdens due to rising dissemination of mobile devices, standardized and easy access to cloud or Internet services, and the possibility of affordable global deployment [4,7-9]. mHealth apps target, for instance, prevalent global diseases [10,11] and offer vital health information at an individual as well as population level [12]. On the other hand, users, albeit deeming access to health information and related services beneficial, are concerned with information security and privacy issues, and want to control access to their information [13-15].

Information security and privacy issues impede users' willingness to share information [16,17], and render thus the promising benefits to be reaped from mHealth apps moot, in order to tailor offered information and services to users' needs, mHealth apps require access to relevant personal health information. Thus, mHealth apps will only offer more general services or cannot be used at all if users are not willing to share their health information. Moreover, infringements of information security and privacy lead not only to leakage or manipulation of private, sensitive information, but make also serious consequences like worsened morbidity or death more likely [18].

Mobile Devices for mHealth

Typical mobile devices for mHealth are smartphones and tablets [11], which are characterized by a rapidly rising market penetration and access to a wide range of embedded technology like sensors for audio, video, location, orientation, and acceleration [8,11,19,20]. The main platforms for mobile devices are Google's Android and Apple's iOS [8]. The associated app stores (Apple iTunes, Google Play) [21,22] offer a vast amount of mHealth apps. These mHealth apps provide a variety of functionality requiring access to different kinds of information and supporting users in different ways, for example, support for weight management, tracking of workouts or medication regimens, facilitation of physician patient communication, management of chronic diseases, or implementation of Web-based interventions [23].

Mobile devices and apps have been addressed from various perspectives, for instance, security aspects [24-26], privacy [18,27-29], software engineering [30-32], medical implications [33,34], hardware [19,35], or user implications [20,36,37]. In contrast, pertinent governmental regulations, for example, [38,39], and extant reviews of mHealth apps, for example, [10,11,40-55], focus mostly on functional aspects and utility of apps for specific diseases or health conditions. Information security and privacy of mHealth apps is only scarcely addressed by extant research. With respect to information security and privacy, extant research offers, to the best of our knowledge, neither clear analysis of the peculiarities that distinguish mHealth apps from "common apps" (eg, weather apps or games), nor of the differences distinguishing apps available from each other. In short, understanding of information security and privacy implications of mHealth apps is lacking and hard to grasp due to the diversity and range of mHealth apps available. In order to address this gap, the objective of our research is to establish an overview of mHealth apps offered on iOS and Android, with a special focus on potential damage to users through information security and privacy infringements.

Our research contributes to practice and the knowledge base by shedding light on information security and privacy of mHealth apps. Aside from providing an overview of available mHealth apps, we contribute to the scientific knowledge base by deepening the understanding of information security and privacy of mHealth apps. Instead of treating mHealth apps as a monolithic technology, we focus on the multi-facetted nature of mHealth apps and identify different mHealth app archetypes with respect to information security and privacy. For practical audiences, our work fosters awareness of information security and privacy implications of mHealth apps. Besides substantiating the need for attention to information security and privacy of mHealth apps, our work demonstrates that mHealth apps are of a diverse nature and require tailored attention to information security and privacy. For developers and end users of mHealth apps, the identification of mHealth app archetypes is especially useful to recognize where and understand when attention to information security and privacy is of particular importance. Deepening the understanding of information security and privacy of mHealth apps is an important step toward realization of the promising potential of mHealth apps to transform and improve the health care environment [2].

Methods

App Discovery

We surveyed English language mHealth apps in the official iOS and Android App Stores. App stores organize their offerings in categories (eg, Books, Games, and News). We selected apps from the Medical and Health & Fitness categories, offered in both stores in May 2013. The iOS app store lists all apps by category and offers the desired information in plain hypertext markup language (HTML), enabling us to automatically parse app information to extract data. The Android App Store employs dynamically generated HTML pages so that the HTML texts displayed in the browser do not convey useful information, which is dynamically loaded from an underlying database. Hence, we used a third party open-source interface for retrieving app information [56]. However, Google imposes various constraints on app store access [8,57]; for instance, only a maximum of 500 apps is returned per search request, even if more apps match the query. Our approach for Android app discovery builds search queries based on words from a publicly available English word list [58] appended once with the string "medical" and once with the string "health". Supplemented with missing health-related words and phrases identified during app tagging (see next paragraph), the word list consists of 111,632 distinct words and phrases (see Multimedia Appendices 1 or 2).

Apps that were not available in English, did not have an English description, or were not health-related, despite being offered in the categories Medical or Health & Fitness (eg, apps offering wallpapers), were excluded from further assessment. We employed tagging, that is, assignment of arbitrary terms describing an object to that object, to filter the initially discovered apps (iOS, 32,614; Android, 4632). Instead of assigning tags directly to an app, we assigned tags to corresponding strings in app descriptions. Only tags referring to health-related information collected by apps, health-related app purposes, handling of information, or other health-related app characteristics were used. For example, apps that provide medication-related functionality should be tagged with the tag "Medication". Yet, app descriptions use different wording (eg, medication, pharmaceutical, or drug). Assigning tags to all encountered strings referring to medication reduces the number of redundant tags and establishes a corpus of string tag relationships that facilitates automated tagging of apps. Since extant research offered no clear guidance to determine cut-off points for manual tagging or the number of required tag matches, cut-off points were determined according to the available data in group discussions of the authors. We manually tagged 200 frequently rated apps (100 Health & Fitness, 100 Medical). Based on this initial tag corpus, we employed string matching [59] to automatically tag the remaining apps. With this approach, apps that do not offer English descriptions or health-related functionality are not assigned any or assigned only a small number of tags, because tags are assigned based on English, health-related words. Apps not matched by at least four distinct tags were excluded from further assessment.

App Clustering

Clustering Approach

App tagging created a machine-readable description of app functionality. Since all apps were tagged based on the same tag corpus, apps with similar characteristics are assigned similar tags. We clustered [60] apps based on their tags to aggregate the data and identify the various kinds of apps in our sample. We used a graph—a set of vertices that are connected by a set of edges [61]—to represent the apps and their tag relationships. Vertices represent apps and edges represent tags both vertices have in common.

For identification of clusters, we used a heuristic by Blondel et al [62], called Louvain method, which is based on modularity optimization. Modularity is a measure for cluster quality introduced by Newman and Girvan [63]. Basically, modularity measures the fraction of edges in the graph that connect vertices within the same cluster minus the expected value of connections within a cluster if edges were inserted at random. Hence, a higher modularity value indicates that detected clusters are less random. The Louvain method performed well in comparative analyses of clustering algorithms [64,65], has low runtime so that it breaks our dense app tag graph down into clusters within a feasible amount of time, and does not require a priori determination of the number of clusters to be discovered, which is unfeasible due to the large numbers of apps, tags, and possible combinations. The Louvain method is an agglomerative clustering algorithm [60] that runs in multiple iterations until a maximum of modularity is reached [62]. Required algorithms were implemented in the programming languages PHP and Java. The Java library JGraphT [66] was used to represent graphs. The relational database management system MySQL was used for data management.

Cluster Assessment

Health IT faces various threats, for instance, intentional and unintentional disclosure or manipulation of information through insiders or outsiders, user errors, maintenance errors, software failures, or hardware failures, as well as environmental threats [67-70]. If such threats materialize, users will be in harms' way. Based on extant research on information security and privacy in health care [68,71-79], we assess information security and privacy implications according to five characteristics: (1) health specificity of information available to apps, (2) potential damage through information leaks, (3) potential damage through information manipulation (change), (4) potential damage through information loss, and (5) potential value of information to third parties (Table 1). Cluster assessment is focused on risks specific to mHealth apps. Hence, risks associated with information ordinarily available to apps [24,27], like location information or device identifier, do not contribute to a more grave assessment.

Characteristic 1, health specificity of information available to apps, assesses whether the app has access to medical user information, access to other nonstandard information, or only access to standard information ordinarily available to apps like location information or device identifiers [24,27]. Characteristic 2 assesses the potential damage through information leaks, which can be classified as none, low, or high. Depending on offered functionality, health IT has access to information with low sensitivity like users' height, weight, or common past illnesses and treatments like a cough or broken bones [71,72]. Other health IT offerings have, however, access to information with high sensitivity like abortions, mental illness, sexually transmitted diseases, HIV status, substance abuse, or genetic predispositions to disease [71-73]. Leaks of such information increase the likelihood of potential damage to users through socioeconomic repercussions [74], embarrassment or damage of reputation [68,71-73,75,76], social stigma [75], loss of affection or respect of family members [77], monetary repercussions through medical fraud (billing for treatments never rendered) or medical identity theft (obtainment of medical services with a fake medical identity) [68,73,74], more expensive insurance coverage or problems to obtain insurance coverage [71,72,75,77,78], or lessened employment possibilities [68,71,72,75,77]. Characteristic 3 assesses potential damage through information manipulation (change), possible values are none, low, or high. Potential damage through information manipulation was, for instance, assessed as low for information on eating patterns or past workouts. Manipulation of such information is inconvenient and undesirable, but poses only low potential damage. Potential damage through information manipulation was assessed as high for apps where information manipulation causes greater harm to users. If, for example, erroneous information is added to users' information due to medical fraud, medical identity theft, negligence, malicious intent, or other threats, treatment can be based on

erroneous information [68,73]. In addition, users' quality of care is affected, potential for harm to health or death is increased, and later efforts to obtain medical, life, or disability insurance are impeded [68,73,74,76]. Potential damage through loss of information is assessed with characteristic 4, possible values are none, low, or high. Loss of uncritical information or information that can be restored was assessed as low. Loss of information was assessed as high in cases where, for instance, important information required for users' care is no longer available [71,75,76]. Finally, the potential value of information for third parties is assessed by characteristic 5, possible values are none, low, or high. If apps have access to information valuable to third parties, infringements of information security and privacy are more likely because they are more rewarding for third parties. For mHealth apps that have only access to information commonly available to mobile apps, value was assessed as none. Value was assessed as low for collected information that is not directly useful to third parties, like unspecific information or information not attributable to users. On the other hand, information like insurance policy information, date of birth, or social security numbers is highly valuable to third parties; for instance, to commit medical identity theft or medical fraud [68,71,73]. Further uses of others' private medical information that are not in the best interest of the data subject include the selling of medical information of celebrities [71], better fitting of insurance policies to insurees' risks and selection of insurees [71,78,79], selection of healthy employees [68,71,78,79], or targeted marketing [71,72,78].

Table 1. Cluster assessment characteristics.

#	Name	Definition	Possible values
1	Specificity	Health specificity of information available to apps (eg, phone identifiers, eating habits, disease history)	Standard, nonstandard, medical
2	Leaks	Potential damage through leaks of information (eg, embarrassment, lessened employment prospects)	None, low, high
3	Change	Potential damage through manipulation (change) of information (eg, treatment errors)	None, low, high
4	Loss	Potential damage through loss of information (eg, loss of information important for treatment)	None, low, high
5	Value	Value of information to third parties (eg, medical identity theft, selection of employees)	None, low, high

Assessing Discovered Clusters

There were two researchers that assessed all discovered clusters. To maintain a consistent interpretation of clusters during assessment, each rater annotated each cluster with a short description based on connotation and prevalence of tags assigned to the cluster. These descriptions were verified through comparison to apps contained in the respective cluster. Subsequently, clusters were assessed according to the five characteristics addressing information security and privacy implications. Reliability assessment with Janson's and Olsson's ι, an multivariate extension of Cohen's κ for multiple judges on the same scale [80], led to a "substantial" [81] agreement score of ι=0.71. All remaining differences were resolved by discussion; if necessary, a third researcher was consulted for dispute resolution.

mHealth app archetypes (AT), with respect to information security and privacy are identified by grouping clusters with identical assessments in a final aggregation step. An archetype is "the original pattern or model of which all things of the same type are representations or copies" [82]. Hence, archetypes constitute underlying or core conceptions of objects observed in the real world. Real-world representations of archetypes may, however, materialize in different forms. For example, from an information security and privacy perspective, a medication reminder, as well as a patient interaction app are real-world representations of the same archetype; they both have access to sensitive medical information that should not be leaked to third parties, must remain accurate, and is of value to third parties. Yet, there is only a low demand for data preservation; medication reminders only need to store information until they have reminded users to take their medication, and patient interaction apps only need to store the data until the interaction has happened. Identification of mHealth app archetypes, with respect to information security and privacy, establishes, thus, a graspable overview of the thousands of mHealth apps offered in the app stores. To foster interpretability of app archetypes, identified app archetypes are numbered and additionally characterized by a natural language descriptor. The medication reminder and patient interaction app from the previous example are, for instance, both representations of the archetype AT 11 (Treatment Reminders). Due to the large diversity of possible real-world representations of mHealth app archetypes, it is unfeasible to identify meaningful descriptors capturing all facets of functionality offered by real-world archetype representations. The final descriptors were determined in group discussions of the authors. Hence, the archetype descriptors characterize exemplary functionality of real-world representations to foster archetype interpretability.

Results

Discovered Apps

We discovered a total of 37,246 apps (iOS, 32,614; Android, 4632) in the categories Medical and Health & Fitness (Figure 1 shows this). After automatic tagging, 34.48% of apps (12,841/37,246; iOS, 32.69%, 10,661/32,614; Android, 47.06%, 2180/4632) were excluded from further assessment. The ratio of iOS mHealth apps to Android mHealth apps is 8.95 (21,953 to 2452).

In both stores, users rate apps on 5-star integer rating scales, ranging from 1 to 5 stars. Mean rating scores of rated iOS and Android mHealth apps are 3.1 (median 3, SD 1.01) and 3.7

(median 3.92, SD 1.08), respectively. Figures 2 and 3 illustrate app ratings and rating counts in more detail. There are 81.36% (17,860/21,953) of iOS and 76.14% (1867/2452) of Android apps that have been rated less than 10 times. There are 75.76% (16,631/21,953) of iOS and 42.37% (1039/2452) of Android apps that have not been rated. There are 1.38% (302/21,953) of iOS and 1.55% (38/2452) of Android apps that have been rated more than 1000 times. There are 39.36% (2095/5322) of rated iOS apps that are rated four stars or more and 27.85% (1482/5322) of rated iOS apps are rated two stars or less. On Android, 64.83% (916/1413) of rated apps are rated four stars or more and 14.23% (201/1413) of rated apps are rated two stars or less. As illustrated in Figure 2, Android mHealth apps are rated higher than iOS mHealth apps (Mann Whitney U(6733)=2,592,190; P<.001; r=0.31; 95% CI 0.99997-0.99998). App category has no significant influence on app rating (iOS, Mann Whitney U(5320)=3,516,696; P=.92; r=0.002; Android, Mann Whitney U(1411)=203,559.5; P=.13; r=0.05).

For Android apps, rating count and download count are strongly positively correlated (Spearman ρ=0.89, n=2452, P<.001), indicating that rating count is a good proxy for download count (Figure 4 shows this).

Figure 1. Flow chart of apps selection.

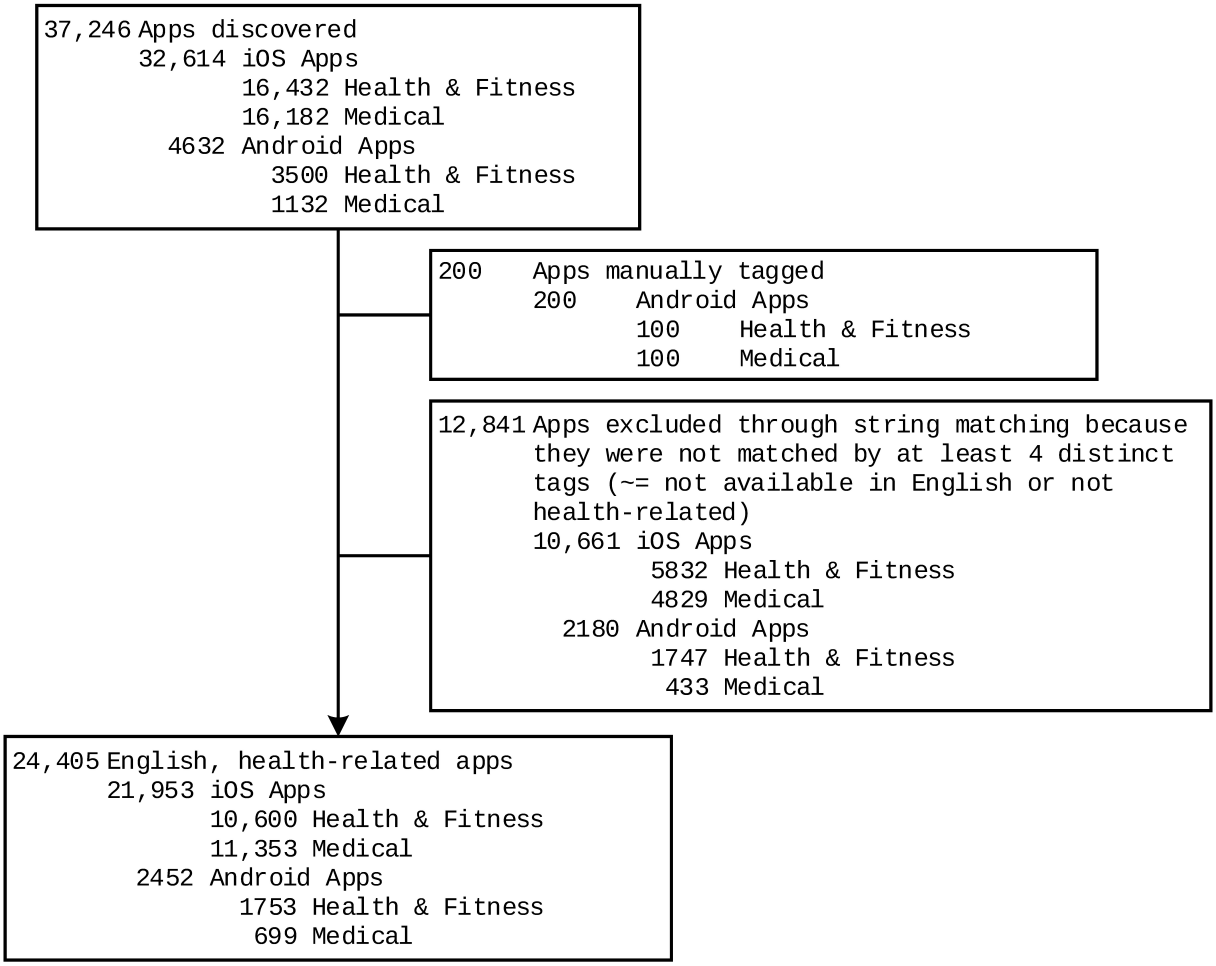


Figure 2. Rating count of mHealth apps by store. Number of ratings increases from left to right.

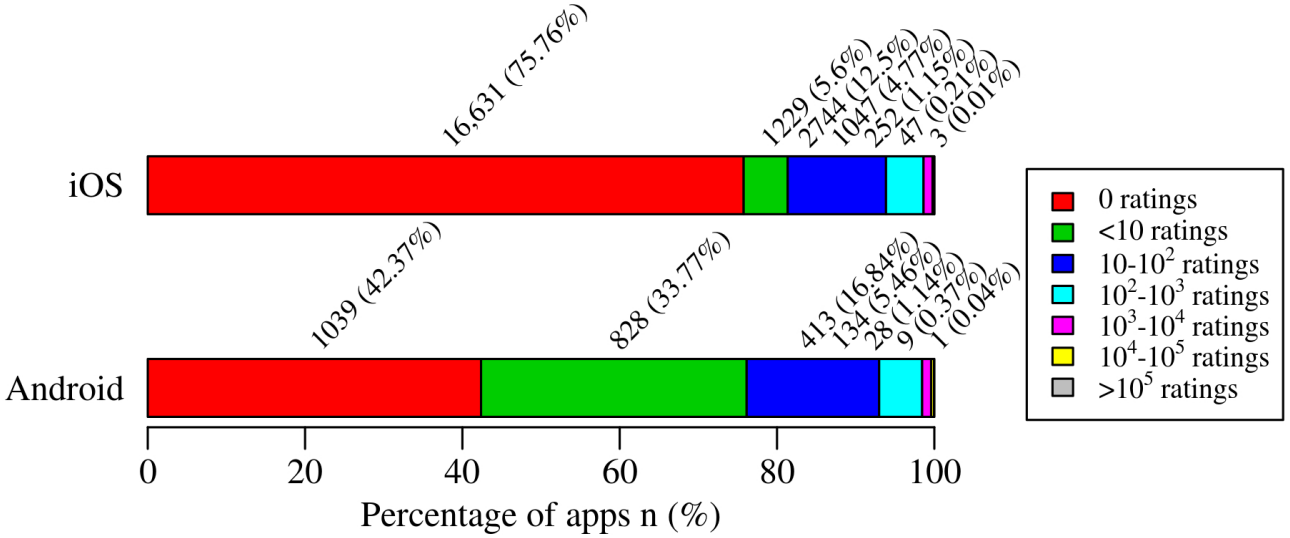


Figure 3. Rating of rated mHealth apps by store.

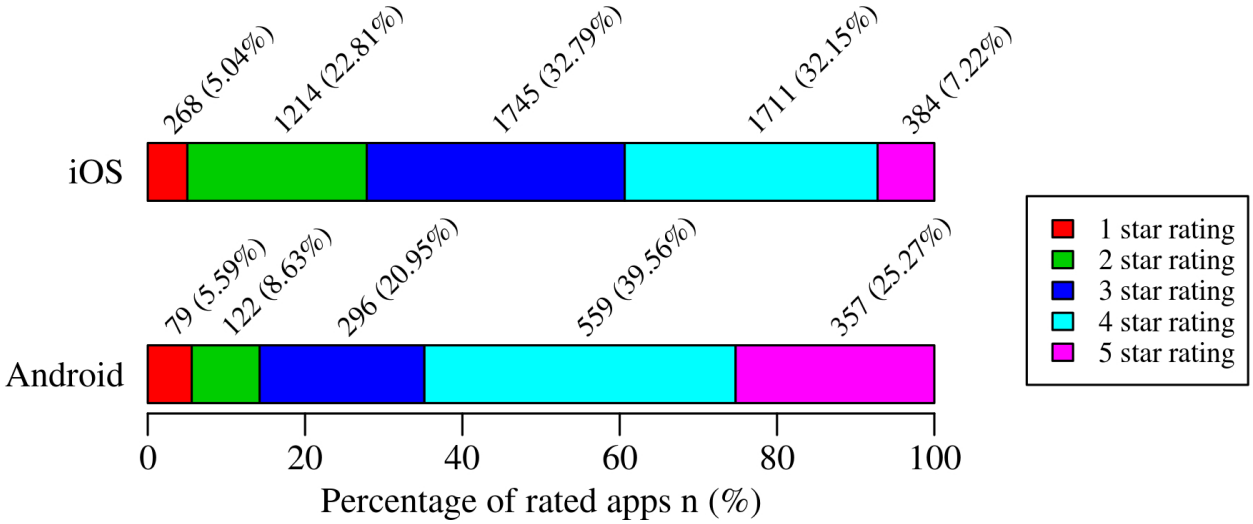
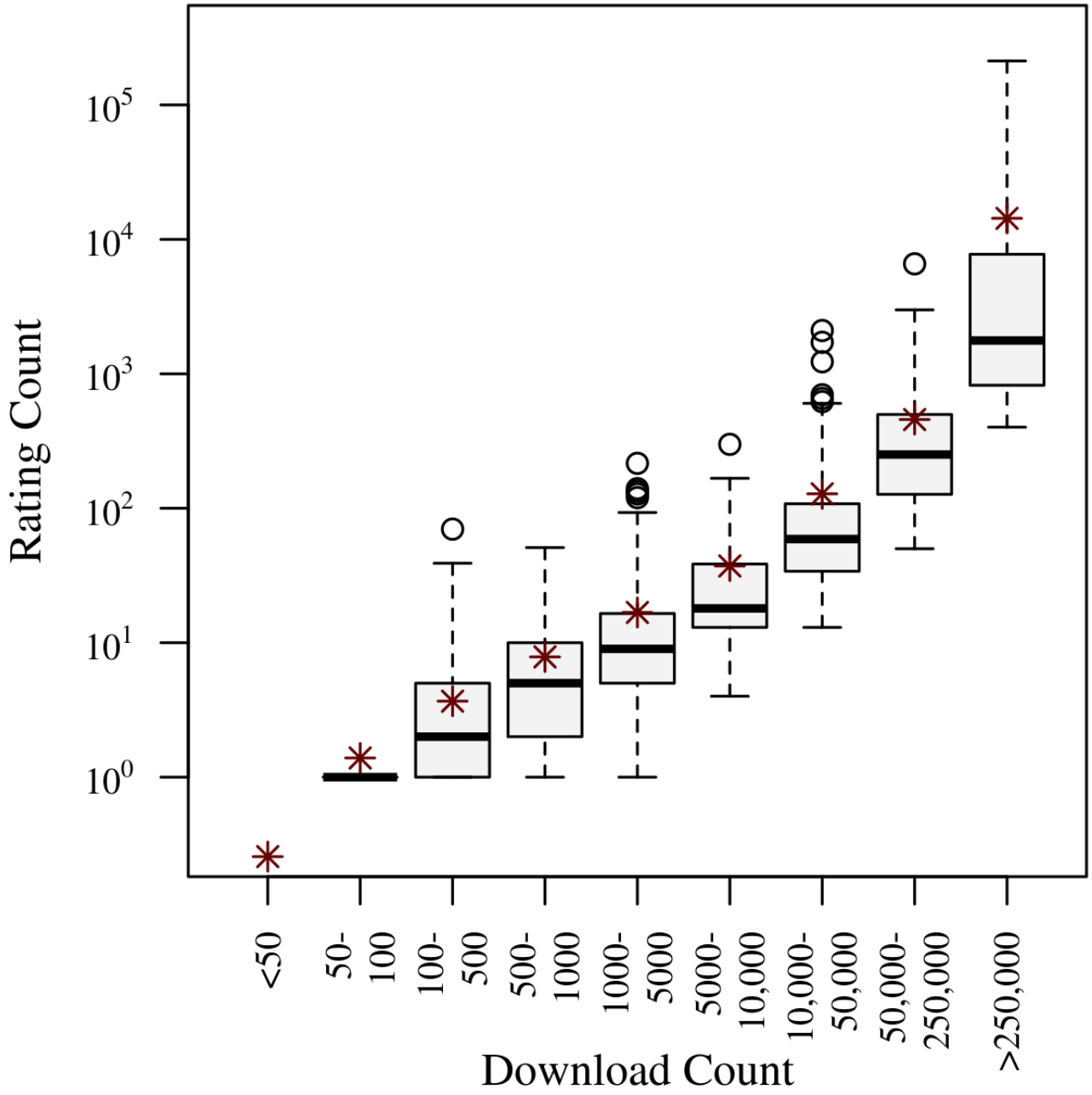


Figure 4. Boxplot of Android app rating count (log-scaled) and download count. Mean values are indicated with asterisks.



App Clustering

Application of the Louvain method [62] grouped the 24,405 apps applicable for clustering into 245 distinct clusters with a modularity score of 0.47, which indicates a good division of the graph [63,83]. Discovered clusters have a mean size of 99.6 apps (minimum 2; maximum 910; median 90; SD 113.6). There are 28.6% (70/245) of clusters containing 26.33% (6426/24,405) of apps that conveyed no information relevant to our research scope and were excluded from further assessment. Some clusters are, for instance, too ambiguous because contained apps match mainly a single tag (eg, “Pain” or “Care Giver”) that is uninformative on its own with respect to our research scope. Cluster assessment, according to the five characteristics, led to further consolidation of the 175 informative clusters into 12 app archetypes, grouping clusters with identical characteristic assessments. The 12 app archetypes have a mean size of 14.6 clusters (minimum 3; maximum 58; median 8; SD 4.6) and 1498.25 apps (minimum 60; maximum 5603; median 615; SD 506.18). Figure 5 shows the clustering process.

Table 2 provides an overview of the cluster assessments with respect to health specificity of information, potential damage through leaks, manipulation, loss of information, and value of collected information to third parties. Medical information is available to apps in 33.7% (59/175) of clusters. There are 16.0% (28/175) of clusters that have access to information not available to ordinary apps [24,27], and apps in 50.3% (88/175) of clusters do not have access to more information than ordinary apps. Apps in 73.7% (129/175) of clusters have no or low potential damage through leaks of information. There are 39.4% (69/175) of clusters that are comprised of apps with high potential damage through manipulation of information. There is no potential damage through loss of information in 67.4% (118/175) of clusters. There are 77.7% (136/175) of clusters that consist of

apps that have only access to information with no or low value for third parties.

Table 2. Cluster assessments with respect to the five information security and privacy characteristics.

		Clusters n (%)[a] N=175	Apps n (%)[a] N=17,979
Specificity [b]			
	Standard[c]	88 (50.3)	8463 (47.07)
	Nonstandard[d]	28 (16.0)	4818 (26.80)
	Medical[e]	59 (33.7)	4698 (26.13)
Leaks [f]			
	None	88 (50.3)	8463 (47.07)
	Low	41 (23.4)	5388 (29.97)
	High	46 (26.3)	4128 (22.96)
Change [g]			
	None	9 (5.1)	786 (4.37)
	Low	97 (55.4)	11,641 (64.75)
	High	69 (39.4)	5552 (30.88)
Loss [h]			
	None	118 (67.4)	10,049 (55.89)
	Low	32 (18.3)	5832 (32.44)
	High	25 (14.3)	2098 (11.67)
Value [i]			
	None	88 (50.3)	8463 (47.07)
	Low	48 (27.4)	6108 (33.97)
	High	39 (22.3)	3408 (18.96)

[a] Uninformative clusters are not included in percentages

[b] Health specificity of information available to apps

[c] Apps only have access to information ordinarily available to apps, for example, phone identifiers or location information

[d] Apps have access to information not ordinarily available to apps, but no access to medical information, for example, workout history or eating habits

[e] Apps have access to medical information, for example, disease history or health insurance information

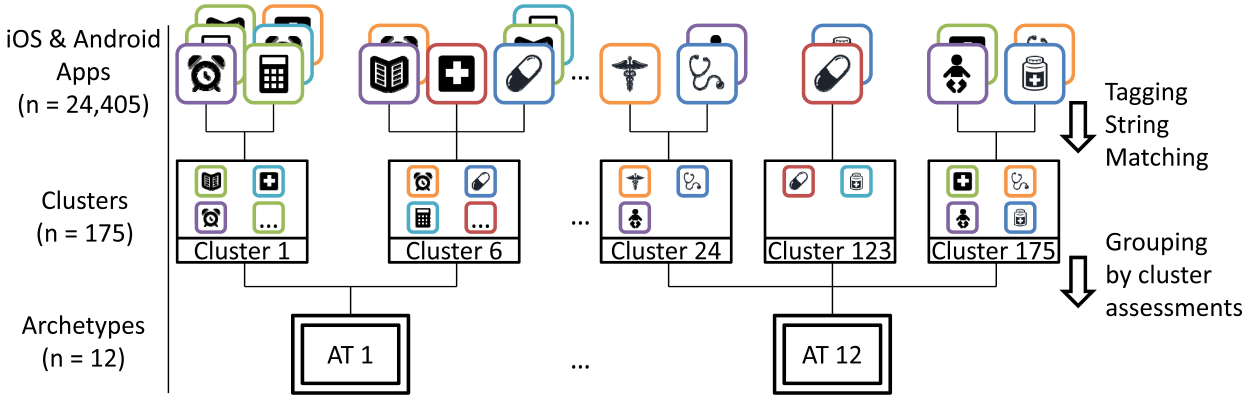
[f] Potential damage through leaks of information, for example, embarrassment, lessened employment possibilities

[g] Potential damage through manipulation, change, of information, for example, treatment based on erroneous information

[h] Potential damage through loss of information, for example, loss of information important for treatment

[i] Value of information to third parties, for example, medical identity theft, selection of employees

Figure 5. Outline of clustering process (AT = archetype).



App Archetypes

Archetype descriptors and examples for functionality offered by apps of the different app archetypes are listed in Table 3. Table 4 illustrates the twelve discovered app archetypes with distinct value combinations according to the five characteristics. AT 1 (Casual Tools) represents 5.1% (9/175) of clusters and 4.37% (786/17,979) of apps. Apps of AT 1 only have access to information also available to ordinary apps and provide no critical functionality, so that their use cannot cause more damage than the use of any other app. Apps of AT 1 offer mostly generic information and are only marginally health-related. AT 2 (Common Knowledge Providers) is the archetype with the most representations in our sample (33.1%, 58/175 of clusters; 31.16%, 5603/17,979 of apps). Apps of AT 2 also have no access to other information than ordinary apps, so that there is no damage through leaks or loss of information. Apps of AT 2 have low potential damage through manipulation of information. More critical information is provided by apps of AT 3 (Treatment Guides), which provide information directly relevant for (self-)treatment or intended to guide users in emergency situations. Information provided by apps of AT 3 needs to be correct to serve as reliable foundation for (self-)treatment decisions; accidental or malicious provision of erroneous information promotes wrong or counterproductive treatment decisions. AT 3 represents 12.0% (21/175) of clusters and 11.54% (2074/17,979) of apps. AT 4 and AT 5 (Fitness Ad-Hoc Tools and Fitness Trackers; 16.0%, 28/175 of clusters; 26.80%, 4818/17,979 of apps) have access to more information than ordinary apps. Yet, they do not collect medical information, so that there is at most low potential damage because collected information is not sensitive, not crucial for provision of medical services, not important for future endeavors, and not valuable to third parties. The remaining seven app archetypes collect medical information (33.7%, 59/175 of clusters; 26.13%, 4698/17,979 of apps). AT 6 (Treatment Support Tools) is the only app archetype that collects medical information and has low potential damage through leaks of information. AT 6 represents calculators and tools for medical professionals or tools offering very specific functionality, so that collected information is either not attributable to patients or not informative. Hence, there is only low potential damage through leaks of information and low value of information to third parties. AT 3 (Treatment Guides), AT 6 (Treatment Support Tools), AT 10 (Health Monitors), AT 11 (Treatment Reminders), and AT 12 (Health Records) offer functionality directly relevant for treatment or decision making so that there is high potential damage through information manipulation. There are four app archetypes, AT 8 (State of Health Tests), AT 10 (Health Monitors), AT 11 (Treatment Reminders), and AT 12 (Health Records) that collect medical information detailed enough to be of high value to third parties (eg, blood test results, medication histories, or health records). While the other app archetypes do not require long storage times of collected information, apps of AT 12 (Health Records) collect medical information relevant for future decision making (eg, disease management tools, medication history, or health records), so that potential damage through loss of information is high. Since apps of AT 12 also tend to collect very detailed, personal information, potential damage through leaks or manipulation and value of information to third parties is high as well.

Table 3. Exemplary functionality of apps represented by the AT.

Archetype	Descriptor	Exemplary kinds of contained apps
AT 1	Casual Tools	Life improvement guides; mosquito repellents; brain fitness trainer
AT 2	Common Knowledge Providers	Information provision for education; alarm clocks; fitness guides
AT 3	Treatment Guides	First aid guides; home remedy guides; medication guides
AT 4	Fitness Ad-Hoc Tools	Diet calculators; weight control calculators; fitness calculators
AT 5	Fitness Trackers	Workout tracker; smoking cessation tools; diet tracker
AT 6	Treatment Support Tools	Diabetes calculators; dosage calculators; diagnosis support tools
AT 7	Intimate Ad-Hoc Tools	Fertility calculators; pregnancy calculators; physician finder
AT 8	State of Health Tests	Acuity tests; color vision tests; blood alcohol calculators
AT 9	Intimate Trackers	Menstruation, intercourse, fertility, and pregnancy tracker
AT 10	Health Monitors	Heart rate monitors; disease counseling; tools for blood test analysis
AT 11	Treatment Reminders	Medication reminder; patient interaction and communities
AT 12	Health Records	Health/emergency records; disease management tools; medication tracker

Table 4. AT with respective assessments of the five information security and privacy characteristics and contained clusters and apps.

AT	Specificity[a]	Leaks[e]	Change[f]	Loss[g]	Value[h]	Clusters n (%)[i] N=175	Apps n (%)[i] N=17,979
1	Standard[b]	None	None	None	None	9 (5.1)	786 (4.37)
2	Standard	None	Low	None	None	58 (33.1)	5603 (31.16)
3	Standard	None	High	None	None	21 (12.0)	2074 (11.54)
4	Nonstandard[c]	Low	Low	None	Low	7 (4.0)	216 (1.20)
5	Nonstandard	Low	Low	Low	Low	21 (12.0)	4602 (25.60)
6	Medical[d]	Low	High	None	Low	13 (7.4)	570 (3.17)
7	Medical	High	Low	None	Low	3 (1.7)	60 (0.33)
8	Medical	High	Low	None	High	4 (2.3)	500 (2.78)
9	Medical	High	Low	Low	Low	4 (2.3)	660 (3.67)
10	Medical	High	High	None	High	3 (1.7)	240 (1.33)
11	Medical	High	High	Low	High	7 (4.0)	570 (3.17)
12	Medical	High	High	High	High	25 (14.3)	2098 (11.67)

[a] Health specificity of information available to apps

[b] Apps only have access to information ordinarily available to apps, for example, phone identifiers or location information

[c] Apps have access to information not ordinarily available to apps, but no access to medical information, for example, workout history or eating habits

[d] Apps have access to medical information, for example, disease history or health insurance information

[e] Potential damage through leaks of information, for example, embarrassment, lessened employment possibilities

[f] Potential damage through manipulation, change, of information, for example, treatment based on erroneous information

[g] Potential damage through loss of information, for example, loss of information important for treatment

[h] Value of information to third parties, for example, medical identity theft, selection of employees

[i] Uninformative clusters are not included in percentages

Discussion

Principal Results

Discovered Apps

Since their inception in 2008, the iOS and Android App Stores underwent a rapid development. After a few years, the app portfolios of both stores encompass hundreds of thousands of apps [8,29,57], which include thousands of mHealth apps. However, absence or scarceness of ratings for 81.36% (17,860/21,953) of iOS and 76.14% (1867/2452) of Android apps indicates that over three quarters of mHealth apps are not in widespread use. A fraction of users who download apps provide ratings [15,84]. Hence, apps less often rated are likely

to be less often used than more often rated apps. An explanation for this is the increased visibility of better-rated apps [85], apps with higher and more ratings are more prominently displayed in app stores and thus more likely to be discovered by potential users. More ratings make the resulting app assessment also more reliable, which attracts more users. Furthermore, many apps offer similar or competing functionality (eg, calculation of the body mass index, tracking of workouts, or prediction of date of birth), so that only a few first-movers, heavily promoted apps, or high quality apps will gain a large user base. App ratings indicate that most users are not dissatisfied with rated apps, 72.15% (3840/5322) of iOS and 85.77% (1212/1413) of Android apps are rated average or above. Another impediment for more widespread use of mHealth apps might be users' concerns about information security and privacy implications [15]. Our cluster analysis of mHealth apps sheds some light on the potential damage through information security and privacy infringements.

App Clustering

Since mHealth apps usually offer functionality related to users' health, it is not a surprising finding that information security and privacy infringements cause potential damage for the majority of apps (94.9%, 166/175 of clusters; 95.63%, 17,193/17,979 of apps). mHealth apps offer, however, diverse functionality so that potential for damage through information security and privacy infringements differs. Manipulation of information is a threat common to most mHealth apps (94.9%, 166/175 of clusters; 95.63%, 17,193/17,979 of apps). Even apps that do not collect any medical information, like AT 2 (Common Knowledge Providers) or AT 3 (Treatment Guides), must ensure that information they provide is correct and stays correct because, at least some, users will act on offered information and base (self)treatment decisions on provided information. Apps offering information or functionality directly relevant for treatment or care must especially ensure that offered information is not accidentally or maliciously manipulated. mHealth apps that only provide information have, however, no information security and privacy implications through leaks or loss of collected information since no information is collected. About one half of the apps in our sample (50.3%, 88/175 of clusters; 47.07%, 8463/17,979 of apps) only provide information. Such apps are probably the most "pleasant" apps when it comes to protecting information security and privacy since no user-collected information must be protected. Thus, providers can focus on protection of integrity of information in rest and during transport, as well as offering accurate information from the onset. Still, extant research shows that information provided by some apps does not concur with current evidence and recommendations or is even contradicting [49,51].

There are 33.7% (59/175) of clusters and 26.13% (4698/17,979) of apps that have access to medical user information. All of these apps have high potential damage through information security and privacy infringements in at least one characteristic. Some apps, for example, AT 6 (Treatment Support Tools) do not collect detailed information or information attributable to users and do not retain entered information, so that there is no potential damage through loss of information, low potential damage through leaks of information, and low value of information for third parties. Yet, they serve as foundation for treatment decisions (eg, appropriate medication dosage), so that there is high potential damage through manipulation of information. Other apps collect information users want to keep private, for example, AT 9 (Intimate Trackers), so that there is high potential damage through leaks of information, but collected information is not directly relevant for treatment or state of health, so that the other characteristics pose only low potential damage. Potential damage of other apps, for example, AT 12 (Health Records) was rated with the most critical assessment in all five characteristics since contained information is sensitive and must be kept private, has to be accurate and accessible to inform treatment decisions, and allows for misuse motivated by financial gain. Consequentially, there is no one-size-fits-all approach for ensuring information security and privacy of mHealth apps. mHealth apps offer different functionality so that they are also subject to different threats. Accordingly, measures for protection of information security and privacy must be tailored to the app to be protected [70].

Our identification of the twelve mHealth app archetypes elucidates information security and privacy of mHealth apps, instead of a hazy collection comprised of the thousands of mHealth apps available in the app stores, the archetypes constitute a lucid, descriptive collection of twelve mHealth app archetypes with different information security and privacy characteristics. Future research can build on the archetypes, for instance, to prioritize information security and privacy requirements with respect to app type, devise collections of security measures ensuring sound protection of information security and privacy, analyze user perceptions of information security and privacy with respect to different kinds of apps, or to further theory and methodology for app development that takes information security and privacy implications into account. For example, potential damage through information security and privacy infringements would obviously be reduced if apps that mainly provide information did not store any user information and focused rather on secure interoperability with specialized storage apps. An overview of app archetypes with respect to information security is also helpful for practical audiences. Associating an mHealth app of interest with the respective archetype improves, for instance, the understanding of perks and perils associated with app use. The overview of the archetypes alone is useful to foster user comprehension and awareness of information security and privacy implications of mHealth app use. In order to continuously benefit from mHealth apps, users must be able to make informed decisions about mHealth app adoption and use.

The apps with the most serious assessment of potential damage through information security and privacy infractions (AT 12, Health Records; 14.3%, 25/175 of clusters; 11.67%, 2098/17,979 of apps) may also offer the most benefits to users [2]. AT 12 represents all the different facets of health records and disease management tools [86-89], which collect detailed health information, allowing them to offer functionality tailored to users' needs and individual peculiarities or to provide other apps with the information required for tailoring offered functionality. Apps of AT 12 could rise to central hubs in the emerging mHealth environment if interoperability issues are solved [12,90] and information security and privacy is

sufficiently addressed so that users can safely trust apps of AT 12 to protect their information [14,91,92].

It is noteworthy that some threats are common to all kinds of mHealth apps, even those without any data collection. Users' behavior, or the sole fact that a guide for stress relief or fighting depression, a support tool for hypertension, or an app providing information on cancer, chronic diseases, infertility, or incontinence, is installed on a device reveals sensitive, private, or embarrassing information [93]. In the end, it is up to users which apps they use and what information they intend to share. To support users in this decision, it is important that they are sensitized to the risks associated with sharing private, sensitive, medical information [16,94] and offered means to gauge, configure, and control information security and privacy practices of mHealth apps [95,96]. Moreover, app stores need to establish processes that ensure protection of information security and privacy prior to making apps publicly accessible, at least, for apps with high potential damage and value to third parties. App developers and providers need to implement appropriate security measures to protect information security and privacy. While ease of app development, free access to helpful apps, and fast dissemination of innovations is desirable, it is imperative that these do not come at the price of lacking information security and privacy. Last, but not least, experienced users, researchers, and further independent entities need to contribute as well by identifying malicious and harmful apps, publishing their findings, and eliminating sources of harm and malice.

Limitations

Since we established a broad overview of available mHealth apps and assessed all discovered apps fitting our selection criteria, it was unfeasible to install and test all apps, so that we focused on the information provided in app stores. This is, however, a common approach, for example, [8,40,51,52], which allowed us to analyze a large sample of over 30,000 apps. Moreover, we cannot ascertain how many of the English apps available on the Android App Store we discovered because the app store offers no complete listing of available apps and search results are limited to 500 apps. Extant reviews of apps in all categories offered in the Android App Store report around 20,000 apps offered in the categories Medial and Health & Fitness. However, these reviews collected apps independent of language and did not assess whether the apps actually offer functionality fitting the categories Medical or Health & Fitness. Our diverse wordlist, comprised of 111,632 distinct words and phrases (see Multimedia Appendices 1 or 2), introduced diversity to search queries and led to the discovery of a wide array of apps, while avoiding bias towards specific types of apps. Creation of search strings based on English words favored discovery of apps offered in English. While this may have reduced the number of discovered Android apps, it suits our research approach and objectives because apps not available in English were excluded from further assessment. Nevertheless, the reported difference in number of apps available on iOS and Android should be treated with care. For now, the iOS and Android App Stores offer far more apps than any other app store [8]. The dominant position of iOS and Android supports our focus on the iOS and Android App Store.

Conclusions

The iOS and Android App Stores offer a wide selection of mHealth apps. Analysis of rating counts indicates, however, that less than a quarter of available apps are in more or less widespread use. An issue impeding app dissemination might be users' information security and privacy concerns [15]. Our cluster analysis shows that most mHealth apps require access to sensitive personal information or offer other services potentially impacting users' treatment or state of health, which increases the potential damage through information security and privacy infringements. The diversity of mHealth apps prevents, however, a one-size-fits-all approach to ensuring information security and privacy of mHealth apps. To address arising challenges, app providers, developers, stores, as well as users, must be sensitized to potential threats and further research and development efforts are required to facilitate protection from information security and privacy infringements. It would be undesirable to diminish or undermine the promising potential of mHealth apps to transform and improve the health care environment [2] through lacking attention to information security and privacy.

Acknowledgments

Required computing resources were provided by the Regional Computing Center of the University of Cologne.

Authors' Contributions

AS, SS, and TD conceived of the project. AS, FG, and TD wrote the manuscript. FG, SS, and TD conducted data acquisition and analysis. TD performed the statistical analyses. SS and TD implemented required custom software.

Conflicts of Interest

None declared.

Multimedia Appendix 1

Word list used for construction of search queries for Android app discovery.

[CSV File, 1MB - mhealth_v3i1e8_app1.csv]

Multimedia Appendix 2

Word list used for construction of search queries for Android app discovery (alternate version in Microsoft Word format with new lines as seperator).

[DOC File, 3MB - mhealth_v3i1e8_app2.doc]

References

1. Collins F. Sci Am. 2012 Jul 10. The real promise of mobile health apps URL: http://www.scientificamerican.com/article/real-promise-mobile-health-apps/ [accessed 2014-12-29] [WebCite Cache ID 6VBe0HmL4]
2. Steinhubl SR, Muse ED, Topol EJ. Can mobile health technologies transform health care? JAMA 2013 Dec 11;310(22):2395-2396. [doi: 10.1001/jama.2013.281078] [Medline: 24158428]
3. Kumar S, Nilsen W, Pavel M, Srivastava M. Mobile health: Revolutionizing healthcare through transdisciplinary research. Computer 2013 Jan;46(1):28-35. [doi: 10.1109/MC.2012.392]
4. Mechael PN. The case for mHealth in developing countries. Innovations: Technology, Governance, Globalization 2009 Jan;4(1):103-118. [doi: 10.1162/itgg.2009.4.1.103]
5. Istepanian R, Jovanov E, Zhang YT. Introduction to the special section on M-Health: Beyond seamless mobility and global wireless health-care connectivity. IEEE Trans Inf Technol Biomed 2004 Dec;8(4):405-414. [Medline: 15615031]
6. Sunyaev A. Consumer facing health care systems. e-Service Journal 2014 Jan;9(2):1-23. [doi: 10.2979/eservicej.9.2.1]
7. Anthes G. HTML5 leads a web revolution. Commun. ACM 2012 Jul 01;55(7):16-17. [doi: 10.1145/2209249.2209256]
8. d'Heureuse N, Huici F, Arumaithurai M, Ahmed M, Papagiannaki K, Niccolini S. What's app? SIGMOBILE Mob. Comput. Commun. Rev 2012 Nov 12;16(2):16-27. [doi: 10.1145/2396756.2396759]
9. Muñoz R. Using evidence-based internet interventions to reduce health disparities worldwide. J Med Internet Res 2010;12(5):e60 [FREE Full text] [doi: 10.2196/jmir.1463] [Medline: 21169162]
10. Chomutare T, Fernandez-Luque L, Arsand E, Hartvigsen G. Features of mobile diabetes applications: Review of the literature and analysis of current applications compared against evidence-based guidelines. J Med Internet Res 2011;13(3):e65 [FREE Full text] [doi: 10.2196/jmir.1874] [Medline: 21979293]
11. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Mobile health applications for the most prevalent conditions by the World Health Organization: Review and analysis. J Med Internet Res 2013;15(6):e120 [FREE Full text] [doi: 10.2196/jmir.2600] [Medline: 23770578]
12. Chen C, Haddad D, Selsky J, Hoffman JE, Kravitz RL, Estrin DE, et al. Making sense of mobile health data: An open architecture to improve individual- and population-level health. J Med Internet Res 2012;14(4):e112 [FREE Full text] [doi: 10.2196/jmir.2152] [Medline: 22875563]
13. Simon SR, Evans JS, Benjamin A, Delano D, Bates DW. Patients' attitudes toward electronic health information exchange: Qualitative study. J Med Internet Res 2009;11(3):e30 [FREE Full text] [doi: 10.2196/jmir.1164] [Medline: 19674960]
14. Dhopeshwarkar RV, Kern LM, O'Donnell HC, Edwards AM, Kaushal R. Health care consumers' preferences around health information exchange. Ann Fam Med 2012;10(5):428-434 [FREE Full text] [doi: 10.1370/afm.1396] [Medline: 22966106]
15. Khalid H, Shihab E, Nagappan M, Hassan A. What do mobile app users complain about? A study on free iOS apps. IEEE Softw 2014;PrePrints:1-1. [doi: 10.1109/MS.2014.50]
16. Bélanger F, Crossler RE. MIS Q. 2011. Privacy in the digital age: A review of information privacy research in information systems URL: http://misq.org/cat-articles/privacy-in-the-digital-age-a-review-of-information-privacy-research-in-information-systems.html [accessed 2015-01-12] [WebCite Cache ID 6VbJ8Iq6s]
17. Anderson CL, Agarwal R. The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. Information Systems Research 2011 Sep;22(3):469-490. [doi: 10.1287/isre.1100.0335]
18. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. ACM Comput. Surv 2012 Nov 01;45(1):1-54. [doi: 10.1145/2379776.2379779]
19. Lane N, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell A. A survey of mobile phone sensing. IEEE Commun. Mag 2010 Sep;48(9):140-150. [doi: 10.1109/MCOM.2010.5560598]
20. Weiss GM, Lockhart JW. The impact of personalization on smartphone-based activity recognition. 2012 Presented at: Proc Act Context Represent Workshop; July 22-23, 2012; Toronto, Canada p. 98-104 URL: http://www.aaai.org/ocs/index.php/WS/AAAIW12/paper/viewFile/5203/5564 [WebCite Cache]
21. Apple. 2014. Apple iTunes App Store URL: https://itunes.apple.com/us/genre/ios/id36?mt=8 [accessed 2014-12-29] [WebCite Cache ID 6VBeRBI0n]
22. Google. 2014. Google Play App Store URL: https://play.google.com/store/apps [accessed 2014-12-29] [WebCite Cache ID 6VBeUxkIm]
23. Barak A, Klein B, Proudfoot JG. Defining internet-supported therapeutic interventions. Ann Behav Med 2009 Aug;38(1):4-17. [doi: 10.1007/s12160-009-9130-7] [Medline: 19787305]

24. Enck W, Octeau D, McDaniel P, Chaudhuri S. A study of Android application security. USA: USENIX Association; 2011. A study of Android application security URL: http://static.usenix.org/legacy/events/sec11/tech/full_papers/Enck.pdf [accessed 2015-01-12] [WebCite Cache ID 6VbJsumQl]
25. Goth G. Analyzing medical data. Commun. ACM 2012 Jun 01;55(6):13-15. [doi: 10.1145/2184319.2184324]
26. Chin E, Felt AP, Greenwood K, Wagner D. Analyzing inter-application communication in Android. USA: ACM; 2011 Presented at: Int Conf Mob Syst Appl Serv; June 28 - July 1, 2011; Washington, DC, USA p. 239-252. [doi: 10.1145/1999995.2000018]
27. Egele M, Kruegel C, Kirda E, Vigna G. PiOS: Detecting privacy leaks in iOS applications. USA: The Internet Society; 2011 Presented at: Netw Distrib Syst Secur Symp; February 6-9, 2011; San Dieg0, CA, USA URL: http://www.internetsociety.org/sites/default/files/egel.pdf [WebCite Cache]
28. Wicker SB. The loss of location privacy in the cellular age. Commun. ACM 2012 Aug 01;55(8):60-68. [doi: 10.1145/2240236.2240255]
29. Liccardi I, Pato J, Weitzner DJ. J Priv Confidentiality. 2013. Improving mobile app selection through transparency and better permission analysis URL: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1102&context=jpc [accessed 2015-01-12] [WebCite Cache ID 6VbKZXQeN]
30. Estrin D, Sim I. Health care delivery. Open mHealth architecture: An engine for health care innovation. Science 2010 Nov 5;330(6005):759-760. [doi: 10.1126/science.1196187] [Medline: 21051617]
31. Heitkötter H, Majchrzak TA, Kuchen H. Cross-platform model-driven development of mobile applications with md2. USA: ACM; 2013 Presented at: Annu ACM Symp Appl Comput; March 18-22, 2013; Coimbra, Portugal p. 526-533. [doi: 10.1145/2480362.2480464]
32. Mojica IJ, Adams B, Nagappan M, Dienst S, Berger T, Hassan AE. A large-scale empirical study on software reuse in mobile apps. IEEE Softw 2014 Mar;31(2):78-86. [doi: 10.1109/MS.2013.142]
33. Freifeld CC, Chunara R, Mekaru SR, Chan EH, Kass-Hout T, Ayala Iacucci A, et al. Participatory epidemiology: Use of mobile phones for community-based health reporting. PLoS Med 2010;7(12):e1000376 [FREE Full text] [doi: 10.1371/journal.pmed.1000376] [Medline: 21151888]
34. Ozdalga E, Ozdalga A, Ahuja N. The smartphone in medicine: A review of current and potential use among physicians and students. J Med Internet Res 2012;14(5):e128 [FREE Full text] [doi: 10.2196/jmir.1994] [Medline: 23017375]
35. Pathak A, Hu YC, Zhang M. Where is the energy spent inside my App?: Fine grained energy accounting on smartphones with Eprof. USA: ACM; 2012 Presented at: ACM Eur Conf Comput Syst; April 10–13, 2012; Bern, Switzerland p. 29-42. [doi: 10.1145/2168836.2168841]
36. Xu Q, Erman J, Gerber A, Mao ZM, Pang J, Venkataraman S. Identifying diverse usage behaviors of smartphone apps. USA: ACM; 2011 Presented at: ACM SIGCOMM Conf Internet Meas Conf; November 2–4, 2011; Berlin, Germany p. 329-344. [doi: 10.1145/2068816.2068847]
37. Xu H, Gupta S, Rosson MB, Carroll JM. Measuring mobile users' concerns for information privacy. 2012 Presented at: Int Conf Inf Syst; December 16-19, 2012; Orlando, FL, USA URL: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1108&context=icis2012 [WebCite Cache]
38. Food and Drug Administration. Mobile medical applications - guidance for industry and food and drug administration staff. USA: Food and Drug Administration; 2013. URL: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf [accessed 2015-01-01] [WebCite Cache ID 6VGNj7A6h]
39. European Commision. Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). Brussels, Belgium: European Commission; 2012. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=en [accessed 2015-01-01] [WebCite Cache ID 6VGO0XR8G]
40. West JH, Hall PC, Hanson CL, Barnes MD, Giraud-Carrier C, Barrett J. There's an app for that: Content analysis of paid health and fitness apps. J Med Internet Res 2012;14(3):e72 [FREE Full text] [doi: 10.2196/jmir.1977] [Medline: 22584372]
41. Plaza I, Demarzo MM, Herrera-Mercadal P, García-Campayo J. Mindfulness-based mobile applications: Literature review and analysis of current features. JMIR Mhealth Uhealth 2013;1(2):e24 [FREE Full text] [doi: 10.2196/mhealth.2733] [Medline: 25099314]
42. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Herreros-González J. Mobile apps in cardiology: Review. JMIR Mhealth Uhealth 2013 Jul 24;1(2):e15 [FREE Full text] [doi: 10.2196/mhealth.2737]
43. Bierbrier R, Lo V, Wu RC. Evaluation of the accuracy of smartphone medical calculation apps. J Med Internet Res 2014;16(2):e32 [FREE Full text] [doi: 10.2196/jmir.3062] [Medline: 24491911]
44. Bender JL, Yue RY, To MJ, Deacken L, Jadad AR. A lot of action, but not in the right direction: Systematic review and content analysis of smartphone applications for the prevention, detection, and management of cancer. J Med Internet Res 2013;15(12):e287 [FREE Full text] [doi: 10.2196/jmir.2661] [Medline: 24366061]
45. Donker T, Petrie K, Proudfoot J, Clarke J, Birch MR, Christensen H. Smartphones for smarter delivery of mental health programs: A systematic review. J Med Internet Res 2013;15(11):e247 [FREE Full text] [doi: 10.2196/jmir.2791] [Medline: 24240579]

46. Muessig KE, Pike EC, Legrand S, Hightow-Weidman LB. Mobile phone applications for the care and prevention of HIV and other sexually transmitted diseases: A review. J Med Internet Res 2013;15(1):e1 [FREE Full text] [doi: 10.2196/jmir.2301] [Medline: 23291245]
47. Mosa AS, Yoo I, Sheets L. A systematic review of healthcare applications for smartphones. BMC Med Inform Decis Mak 2012;12:67 [FREE Full text] [doi: 10.1186/1472-6947-12-67] [Medline: 22781312]
48. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Sainz-De-Abajo B. Comparison of mobile apps for the leading causes of death among different income zones: A review of the literature and app stores. JMIR Mhealth Uhealth 2014;2(1):e1 [FREE Full text] [doi: 10.2196/mhealth.2779] [Medline: 25099695]
49. Huckvale K, Car M, Morrison C, Car J. Apps for asthma self-management: A systematic assessment of content and tools. BMC Med 2012;10:144 [FREE Full text] [doi: 10.1186/1741-7015-10-144] [Medline: 23171675]
50. Wolf JA, Moreau JF, Akilov O, Patton T, English JC, Ho J, et al. Diagnostic inaccuracy of smartphone applications for melanoma detection. JAMA Dermatol 2013 Apr;149(4):422-426 [FREE Full text] [doi: 10.1001/jamadermatol.2013.2382] [Medline: 23325302]
51. Breton ER, Fuemmeler BF, Abroms LC. Weight loss-there is an app for that! But does it adhere to evidence-informed practices? Transl Behav Med 2011 Dec;1(4):523-529 [FREE Full text] [doi: 10.1007/s13142-011-0076-5] [Medline: 24073074]
52. Rosser BA, Eccleston C. Smartphone applications for pain management. J Telemed Telecare 2011;17(6):308-312. [doi: 10.1258/jtt.2011.101102] [Medline: 21844177]
53. Abroms LC, Padmanabhan N, Thaweethai L, Phillips T. iPhone apps for smoking cessation: A content analysis. Am J Prev Med 2011 Mar;40(3):279-285 [FREE Full text] [doi: 10.1016/j.amepre.2010.10.032] [Medline: 21335258]
54. Liu C, Zhu Q, Holroyd KA, Seng EK. Status and trends of mobile-health applications for iOS devices: A developer's perspective. Journal of Systems and Software 2011 Nov;84(11):2022-2033. [doi: 10.1016/j.jss.2011.06.049]
55. Lewis TL, Wyatt JC. mHealth and mobile medical Apps: A framework to assess risk and promote safer use. J Med Internet Res 2014;16(9):e210 [FREE Full text] [doi: 10.2196/jmir.3133] [Medline: 25223398]
56. android-market-api. 2014. An open-source API for the Android market URL: http://code.google.com/p/android-market-api/ [accessed 2014-02-14] [WebCite Cache ID 6NNh225JS]
57. Viennot N, Garcia E, Nieh J. A measurement study of Google Play. USA: ACM; 2014 Presented at: ACM Int Conf Meas Model Comput Syst; June 16–20, 2014; Austin, TX, USA p. 221-233. [doi: 10.1145/2591971.2592003]
58. SIL International Linguistics Department. English wordlists. 2014. URL: http://www-01.sil.org/linguistics/wordlists/english/ [accessed 2014-02-17] [WebCite Cache ID 6NS0EItXU]
59. Faro S, Lecroq T. Festschr Bořivoj Melichar Prague, Czech Republic. Prague, Czech Republic: Prague Stringology Club; 2012. Twenty years of bit-parallelism in string matching URL: http://www.stringology.org/papers/Festschrift_BM70.pdf [accessed 2015-01-07] [WebCite Cache ID 6VPW34gIe]
60. Jain AK. Data clustering: 50 years beyond K-means. Pattern Recognition Letters 2010 Jun;31(8):651-666. [doi: 10.1016/j.patrec.2009.09.011]
61. Newman MEJ. The structure and function of complex networks. SIAM Rev 2003 Jan;45(2):167-256. [doi: 10.1137/S0036144450342480]
62. Blondel VD, Guillaume J, Lambiotte R, Lefebvre E. Fast unfolding of communities in large networks. J. Stat. Mech 2008 Oct 09;2008(10):P10008. [doi: 10.1088/1742-5468/2008/10/P10008]
63. Newman ME, Girvan M. Finding and evaluating community structure in networks. Phys Rev E Stat Nonlin Soft Matter Phys 2004 Feb;69(2 Pt 2):026113. [Medline: 14995526]
64. Lancichinetti A, Fortunato S. Community detection algorithms: A comparative analysis. Phys Rev E Stat Nonlin Soft Matter Phys 2009 Nov;80(5 Pt 2):056117. [Medline: 20365053]
65. Tibély G, Kovanen L, Karsai M, Kaski K, Kertész J, Saramäki J. Communities and beyond: Mesoscopic analysis of a large social network with complementary methods. Phys Rev E Stat Nonlin Soft Matter Phys 2011 May;83(5 Pt 2):056125. [Medline: 21728623]
66. Naveh B. 2003. JGraphT URL: http://jgrapht.org/ [accessed 2014-02-21] [WebCite Cache ID 6NYMn4Z4V]
67. Bakhtiyari Shahri A. A tree model for identification of threats as the first stage of risk assessment in HIS. JIS 2012;03(02):169-176. [doi: 10.4236/jis.2012.32020]
68. Kotz D. A threat taxonomy for mHealth privacy. Bangalore, India: IEEE; 2011 Presented at: Int Conf Commun Syst Netw; Jan 4-8, 2011; Bangalore, India. [doi: 10.1109/COMSNETS.2011.5716518]
69. Goth G. Mobile security issues come to the forefront. IEEE Internet Comput 2012 May;16(3):7-9. [doi: 10.1109/MIC.2012.54]
70. Dehling T, Sunyaev A. Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the German nationwide health information technology infrastructure. Electron Markets 2014 Feb 8;24(2):89-99. [doi: 10.1007/s12525-013-0150-6]
71. Rindfleisch TC. Privacy, information technology, and health care. Commun. ACM 1997;40(8):92-100. [doi: 10.1145/257874.257896]
72. Rohm AJ, Milne GR. Just what the doctor ordered. Journal of Business Research 2004 Sep;57(9):1000-1011. [doi: 10.1016/S0148-2963(02)00345-4]

73. Johnson ME. Data hemorrhages in the health-care sector. In: Dingledine R, Golle P, editors. Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers ... Computer Science / Security and Cryptology). USA: Springer; 2009.
74. Appari A, Johnson ME. Information security and privacy in healthcare: Current state of research. IJIEM 2010;6(4):279-314. [doi: 10.1504/IJIEM.2010.035624]
75. Appelbaum PS. Privacy in psychiatric treatment: Threats and responses. Am J Psychiatry 2002 Nov;159(11):1809-1818. [Medline: 12411211]
76. Gritzalis DA. Enhancing security and improving interoperability in healthcare information systems. Med Inform (Lond) 1998;23(4):309-323. [Medline: 9922951]
77. Shea S. Security versus access: Trade-offs are only part of the story. J Am Med Inform Assoc 1994;1(4):314-315 [FREE Full text] [Medline: 7719814]
78. Barrows RC, Clayton PD. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc 1996;3(2):139-148 [FREE Full text] [Medline: 8653450]
79. Rothstein MA, Talbott MK. Compelled authorizations for disclosure of health records: Magnitude and implications. Am J Bioeth 2007 Mar;7(3):38-45. [doi: 10.1080/15265160601171887] [Medline: 17366232]
80. Janson H, Olsson U. A measure of agreement for interval or nominal multivariate observations. Educational and Psychological Measurement 2001 Apr 01;61(2):277-289. [doi: 10.1177/00131640121971239]
81. Landis JR, Koch GG. The measurement of observer agreement for categorical data. Biometrics 1977 Mar;33(1):159-174. [Medline: 843571]
82. Merriam-Webster. 2014. Archetype - definition URL: http://www.merriam-webster.com/dictionary/archetype [accessed 2014-06-26] [WebCite Cache ID 6QdwYwRgI]
83. Newman ME. Analysis of weighted networks. Phys Rev E Stat Nonlin Soft Matter Phys 2004 Nov;70(5 Pt 2):056131. [Medline: 15600716]
84. Girardello A, Michahelles F. Explicit and implicit ratings for mobile applications. Germany: GI; 2010 Presented at: Informatik 2010; September 29 - October 1, 2010; Leipzig, Germany p. 606-612 URL: http://subs.emis.de/LNI/Proceedings/Proceedings175/606.pdf [WebCite Cache]
85. Pagano D, Maalej W. User feedback in the AppStore: An empirical study. : IEEE; 2013 Presented at: IEEE International Conference on Requirements Engineering; July 15-19, 2013; Rio De Janeiro, Brasil p. 125-134. [doi: 10.1109/RE.2013.6636712]
86. Caligtan CA, Dykes PC. Electronic health records and personal health records. Semin Oncol Nurs 2011 Aug;27(3):218-228. [doi: 10.1016/j.soncn.2011.04.007] [Medline: 21783013]
87. Dorr D, Bonner LM, Cohen AN, Shoai RS, Perrin R, Chaney E, et al. Informatics systems to promote improved care for chronic illness: A literature review. J Am Med Inform Assoc 2007;14(2):156-163 [FREE Full text] [doi: 10.1197/jamia.M2255] [Medline: 17213491]
88. Sunyaev A. Evaluation of Microsoft HealthVault and Google Health personal health records. Health Technol 2013 Feb 24;3(1):3-10. [doi: 10.1007/s12553-013-0049-4]
89. Sunyaev A, Chornyi D. Supporting chronic disease care quality. J. Data and Information Quality 2012 May 01;3(2):1-21. [doi: 10.1145/2184442.2184443]
90. Hufnagel SP. Interoperability. Mil Med 2009 May;174(5 Suppl):43-50. [Medline: 19562961]
91. Spiekermann S. The challenges of privacy by design. Commun. ACM 2012 Jul 01;55(7):38-40. [doi: 10.1145/2209249.2209263]
92. Klasnja P, Consolvo S, Choudhury T, Beckwith R, Hightower J. Exploring privacy concerns about personal sensing. Berlin, Germany: Springer; 2009 Presented at: Int Conf Pervasive Comput; May 11-14, 2009; Nara, Japan p. 176-183. [doi: 10.1007/978-3-642-01516-8_13]
93. Seneviratne S, Seneviratne A, Mohapatra P, Mahanti A. Predicting user traits from a snapshot of apps installed on a smartphone. SIGMOBILE Mob. Comput. Commun. Rev 2014 Jun 03;18(2):1-8. [doi: 10.1145/2636242.2636244]
94. Wilson DW, Valacich JS. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. : Irrational Decision-Making within the Privacy Calculus. Proc Thirty Third Int Conf Inf Syst ICIS 2012 Orlando, FL, U. S; 2012 Presented at: Int Conf Inf Sys; December 16-19, 2012; Orlando, FL, USA URL: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1286&context=icis2012 [WebCite Cache]
95. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. J Am Med Inform Assoc 2014 Aug 21. [doi: 10.1136/amiajnl-2013-002605] [Medline: 25147247]
96. Sunyaev A, Schneider S. Cloud services certification. Commun. ACM 2013 Feb 01;56(2):33-36. [doi: 10.1145/2408776.2408789]

Abbreviations

AT: app archetype
HTML: Hyper Text Markup Language

IT: information technology
mHealth: mobile health

Edited by G Eysenbach; submitted 06.07.14; peer-reviewed by A Knotts, L Ning, WC Su; comments to author 19.09.14; revised version received 21.10.14; accepted 03.11.14; published 19.01.15

Please cite as:
Dehling T, Gao F, Schneider S, Sunyaev A
Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android
JMIR mHealth uHealth 2015;3(1):e8
URL: http://mhealth.jmir.org/2015/1/e8/
doi:10.2196/mhealth.3672
PMID:25599627