Original Paper

Analysis of Diabetes Apps to Assess Privacy-Related Permissions: Systematic Search of Apps

José Javier Flors-Sidro[1], MSc; Mowafa Househ[2], PhD; Alaa Abd-Alrazaq[2], PhD; Josep Vidal-Alaball[3,4], MD, MPH, PhD; Luis Fernandez-Luque[5,6], PhD; Carlos Luis Sanchez-Bocanegra[7], PhD

[1]Information Systems Department, Consorci Hospitalari Provincial de Castelló, Castelló de la Plana, Spain

[2]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

[3]Health Promotion in Rural Areas Research Group, Gerència Territorial de la Catalunya Central, Institut Català de la Salut, Sant Fruitós de Bages, Spain

[4]Unitat de Suport a la Recerca de la Catalunya Central, Fundació Institut Universitari per a la recerca a l'Atenció Primària de Salut Jordi Gol i Gurina, Sant Fruitós de Bages, Spain

[5]Salumedia Labs, Sevilla, Spain

[6]Adhera Health Inc, Palo Alto, CA, United States

[7]Faculty of Health Sciences, Universitat Oberta de Catalunya, Barcelona, Spain

Corresponding Author:
Alaa Abd-Alrazaq, PhD
Division of Information and Computing Technology
College of Science and Engineering
Hamad Bin Khalifa University
Education City
Doha,
Qatar
Phone: 974 55708549
Email: aabdalrazaq@hbku.edu.qa

Abstract

Background: Mobile health has become a major vehicle of support for people living with diabetes. Accordingly, the availability of mobile apps for diabetes has been steadily increasing. Most of the previous reviews of diabetes apps have focused on the apps' features and their alignment with clinical guidelines. However, there is a lack of knowledge on the actual compliance of diabetes apps with privacy and data security guidelines.

Objective: The aim of this study was to assess the levels of privacy of mobile apps for diabetes to contribute to the raising of awareness of privacy issues for app users, developers, and governmental data protection regulators.

Methods: We developed a semiautomatic app search module capable of retrieving Android apps' privacy-related information, particularly the dangerous permissions required by apps, with the aim of analyzing privacy aspects related to diabetes apps. Following the research selection criteria, the original 882 apps were narrowed down to 497 apps that were included in the analysis.

Results: Approximately 60% of the analyzed diabetes apps requested potentially dangerous permissions, which pose a significant risk to users' data privacy. In addition, 28.4% (141/497) of the apps did not provide a website for their privacy policy. Moreover, it was found that 40.0% (199/497) of the apps contained advertising, and some apps that claimed not to contain advertisements actually did. Ninety-five percent of the apps were free, and those belonging to the "medical" and "health and fitness" categories were the most popular. However, app users do not always realize that the free apps' business model is largely based on advertising and, consequently, on sharing or selling their private data, either directly or indirectly, to unknown third parties.

Conclusions: The aforementioned findings confirm the necessity of educating patients and health care providers and raising their awareness regarding the privacy aspects of diabetes apps. Therefore, this research recommends properly and comprehensively training users, ensuring that governments and regulatory bodies enforce strict data protection laws, devising much tougher security policies and protocols in Android and in the Google Play Store, and implicating and supervising all stakeholders in the apps' development process.

(JMIR Diabetes 2021;6(1):e16146) doi: 10.2196/16146

KEYWORDS

diabetes mellitus; privacy; mobile apps; dangerous permissions

Introduction

Background

Diabetes mellitus (DM) is one of the most common chronic conditions around the globe. The number of people with DM has risen globally from 108 million in 1980 to 422 million in 2014 [1]. Its prevalence has been increasing everywhere, especially in middle-income countries, from 4.7% in 1980 to 8.5% in 2014. DM increases the risk of serious health problems such as myocardial infarction, renal failure, stroke, and lower limb amputation [2]. Diabetic retinopathy is one of the most important causes of blindness worldwide, especially in developed countries [3]. DM has also been linked to an increased risk of other conditions such as dementia, depression, and some types of cancer [4]. In order to reduce the risk of complications, intensive patient education and support are needed, which can be enhanced by the use of mobile technology.

Along with the exponential increase in the number of health apps [5,6], in particular the number of diabetes apps has increased significantly in the last several years [7]. Mobile health (mHealth) has become a major vehicle of support for people living with diabetes, and the availability of mobile apps for diabetes has been steadily increasing. Most of the previous reviews of diabetes apps have focused on their features and their alignment with clinical guidelines [8,9]. However, there is a lack of knowledge on the actual compliance of diabetes apps with privacy and data security guidelines.

Therefore, there is a growing concern to review diabetes apps because in many cases they do not possess the quality and content that they should according to their own declared purposes [10,11]. In addition, some studies that have investigated the effectiveness of mobile apps clearly demonstrate data privacy problems [12], as well as a lack of transparency with the provided information [13].

Studies on mHealth and privacy have raised some serious concerns in recent years. Because very sensitive information is increasingly accessed and shared using mobile apps, there is an obvious need for clinicians, software developers, users, and patients to be aware of and trained on information privacy aspects. Personal data may be collected through different means, such as being entered directly by the user or being recorded by the phone’s camera, microphone, or paired wireless device (eg, Bluetooth glucometer apps). It is crucial to note that the treatment of these critical data demands a special approach regarding security and privacy. However, some apps do not even provide information regarding their privacy policies. In some instances, these privacy terms are difficult to understand by nontechnical users, and some privacy policies may even be regarded as abusive. To make matters worse, the ecosystem of mobile apps is so complex that even app developers and users may not know with whom the data is being shared and for what purpose [14-16].

An additional challenge is that very often stakeholders are not involved in the app development process and consequently cannot provide feedback on privacy preferences [10].

To deal with these issues, some researchers such as Stoyanov et al [17] have attempted to develop a suitable framework—the Mobile App Rating Scale—that allows for the evaluation of the quality of apps. Alternatively, other investigations have focused specifically on privacy or legal issues [18]. In the case of mHealth for diabetes, recent reviews looked into aspects linked to the efficacy of interventions [19,20] but did not address aspects related to privacy. Other research has investigated privacy aspects in generic mHealth apps [12,21]. However, to the best of our knowledge, this study is the first to focus on investigating privacy issues and dangerous permissions in diabetes mobile apps. Studies looking at diabetes apps have not conducted in-depth analyses of dangerous permissions on the Android platform [22].

Objectives

The aim of this study was to evaluate the privacy-related permissions of Android diabetes apps in Google's Play Store using a semiautomatic approach that relies on the extraction of privacy-related features (eg, permissions, terms of usage). This approach was designed to assist in identifying strategies to raise the awareness of app users, patients, and clinicians. To illustrate our approach, we provide two case studies of diabetes apps that were comprehensively analyzed (Multimedia Appendix 1).

Methods

Study Design

The first step in this study was the extraction of metadata from mobile apps’ metadata using a web-based application programming interface (API) [23]. We used the platform 42Matters, which offers a web-based commercial tool that facilitates access to the Android Google Play Store and to other mobile platforms’ apps’ metadata through a proprietary API [24]. Searches were conducted with the developed script module 42Matters’ index of Android apps. Since the 42Matters platform did not allow the extraction of privacy-related permissions from Apple’s App Store, the research centered on Android apps from Google’s Play Store. Data extraction was focused on potentially dangerous permissions [25] that allow the requesting app access to private user data or control over the mobile device, both of which can negatively impact the user. Because this type of permission introduces potential risk, the system does not automatically grant it to the requesting app. Our methodology was based on similar studies of health apps that used the 42Matters platform, but focusing on privacy-related information [26,27].

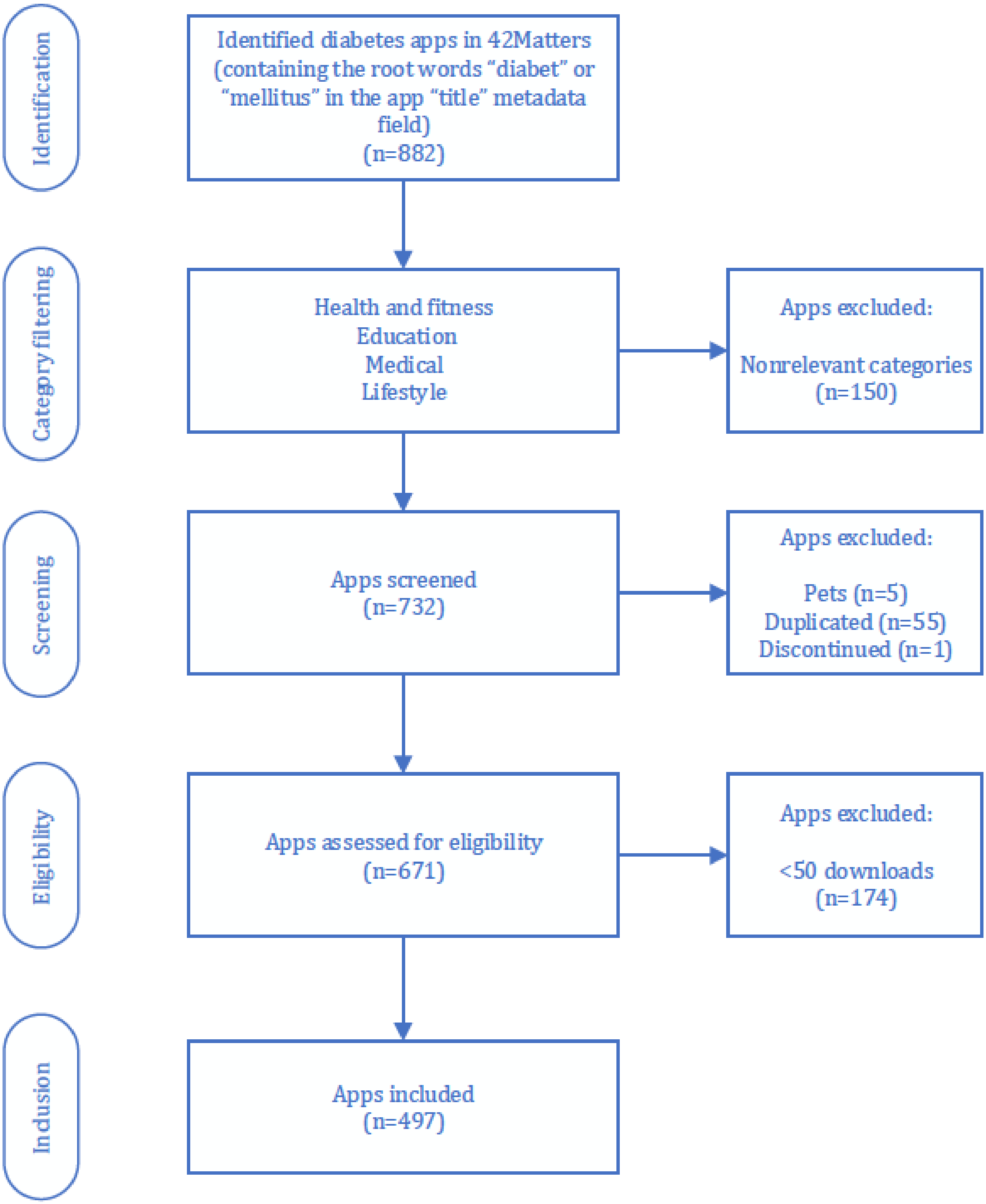
In order to complement the quantitative results already presented, we described and investigated two very popular and well-rated diabetes apps (presented in Multimedia Appendix 1) from a qualitative perspective.

For the extraction of the diabetes apps' metadata, we first devised the architecture [28] and subsequently developed the corresponding software module for the automatic extraction of mobile app metadata using the web-based API of 42Matters. The output of this module is a data set stored locally in a comma-separated values (CSV) file. The source code for the module was released under the GNU AGPLv3 license and can be found on the GitHub link [29]. This module is capable of querying the API of the 42Matters platform to retrieve metadata related to diabetes apps, including the Android permissions required by the apps. The module was designed to extract apps with the following search parameters: (1) language (we searched for English-language apps), (2) keyword search (we searched for apps whose titles included the root words "diabet" and "mellitus"), and (3) app categories (we selected the categories medical, health and fitness, lifestyle, and education).

The resulting apps were manually reviewed (see Multimedia Appendix 1) to assess whether they were related to diabetes. All apps were related to diabetes, but we did not address the quality of their content. As explained in the "Limitations" section, choosing a method where search fields matched the description—and not only the title—would have resulted in more apps, many of which would not have been related to diabetes.

Once the most suitable app categories were identified, it was then possible to move on to design the entire app selection process, which consisted of the following steps (see Figure 1):

Figure 1. App selection process flowchart.



- Step 1: "Identification" phase—all of the diabetes apps that contained the root words "diabet" or "mellitus" in an app's title field were selected, resulting in 882 apps; by matching diabet or mellitus, it was possible to ensure that any relevant potential variations of the words that contained these root words (ie, diabetes, diabetic, diabetics, mellitus, etc) were included in the search.
- Step 2: "Category filtering" phase—in order to guarantee that only relevant diabetes apps were included in the study, all the retrieved apps that did not belong to the medical, health and fitness, education, or lifestyle categories [30] were automatically filtered out by the 42Matters script module and excluded from the study; this filtering resulted in 732 apps.
- Step 3: "Screening" phase—in this phase, we manually filtered apps and excluded 5 diabetes apps related to pets, 1 discontinued app, and 55 duplicated apps; this screening resulted in 671 apps.
- Step 4: "Eligibility" phase—we excluded apps that did not have a minimum of 50 downloads, and therefore discarded 174 apps.

- Step 5: "Inclusion" phase—the resulting 497 apps were analyzed, which were the objects of analysis of this research.

Data Extraction: Retrieved Metadata Fields

After the final set of apps was selected in June 2019, a process was initiated to extract all the relevant metadata and information, which were stored in a CSV file. All the retrieved fields are described in the table below.

Table 1. Description of apps' retrieved metadata as provided by 42Matters.

App's metadata field	Description
Title	Main name of the app
Price	Price and currency (0 if it was free)
Permission	Required Android permissions of the app
Rating	App's average rating from 0 to 5 (0=worst, 5=best)
Number of downloads	Number of times the app was downloaded
Number of ratings	Number of times the app was rated
Contains advertising	True if the app contained advertising and false if it did not
Category	Category to which the app belonged (medical, health and fitness, education, or lifestyle)
Short description	Short description of the app's declared purpose
Website	Website of the app
Privacy policy	Website showing the app's privacy policy

Extraction of Android Privacy-Related Permissions

Starting with Android 6.0 (API 23 level), users grant permissions to apps while using them, not when an app is installed. On the one hand, this approach simplifies the process of installing the app because the user does not need to grant permissions when installing or updating the app. In addition, it provides the user with more control over the app's functionalities because users can revoke the granted permissions from the app's configuration screen at any time. On the other hand, this new approach complicates the app's usability because dangerous permissions have to be granted while using the app, which poses an additional challenge for untrained users. Android distinguishes between 4 categories of permissions: normal, signature, dangerous, and special [31].

Signature and special permissions will not be explained here because they are rarely used and were not found in any of the apps included in our research. The most frequently requested permissions are normal and dangerous permissions. If an app declares a normal permission in its manifest, the system grants permission to it automatically without the user's intervention. On the other hand, Android considers dangerous permissions as critical because they allow apps to access users' critical data.

More concretely, an Android dangerous permission [25,32] allows the requesting app access to private user data or control over the mobile device. Because this type of permission allows developers to access users' data, photos, and videos stored on the device, it introduces potential risk, and the system does not automatically grant it to the requesting app [33,34].

In brief, normal permissions do not put the user's privacy at risk directly. Consequently, if an app declares a normal permission in its metadata, the system grants permission to it automatically without the user's intervention. On the other hand, a dangerous permission allows an app to access the user's critical data, and consequently the user should explicitly authorize this permission [35]. The 10 most required dangerous permissions found in this research are shown in Multimedia Appendix 2.

Results

App Functions

The process described in the "Methods" section retrieved a total of 497 apps (Multimedia Appendix 3). The breakdown of privacy-related permissions is summarized in Table 2. Most of the apps required at least one dangerous permission.

Table 2. Summary of the privacy-related main features of retrieved diabetes apps.

Assessed parameter	Diabetes apps (N=497), n (%)
Does not require any permissions (either normal or dangerous)	89 (17.9)
Only requires normal permissions	111 (22.3)
Requires at least one dangerous permission	297 (59.8)
Does not provide a website link to its privacy policy	141 (28.4)
Contains advertising	199 (40.0)

The reason for apps not requesting any permissions is that they serve very basic functions (eg, calculators, logs, diaries, etc) that only need access to very basic and noncritical Android resources. Only 22.3% (111/497) of the apps required normal (noncritical) permissions alone. On the other hand, 59.8% (297/497) of the apps required at least one dangerous permission. This might be partially justified by these apps' more advanced functionalities (eg, doctor-patient interaction, connecting to a glucometer, calorie-burning calculation, scanning the barcode of diabetic food, etc).

Regarding privacy, it was worrying to discover that 28.4% (141/497) of the apps did not return the privacy policy metadata field, consequently posing additional difficulty for users to adequately understand how these apps would treat very sensitive personal information.

Finally, 40.0% (199/497) of the apps contained advertising, which can imply the sharing of critical personal data (eg, a user's precise location) with unknown third parties for geolocated advertisement. Consequently, because the advertising business model in the mobile ecosystem is usually linked to the sharing or selling of critical personal data [36], the aforementioned findings unquestionably confirm the necessity to educate users and raise awareness regarding user privacy in diabetes apps.

Dangerous Permissions

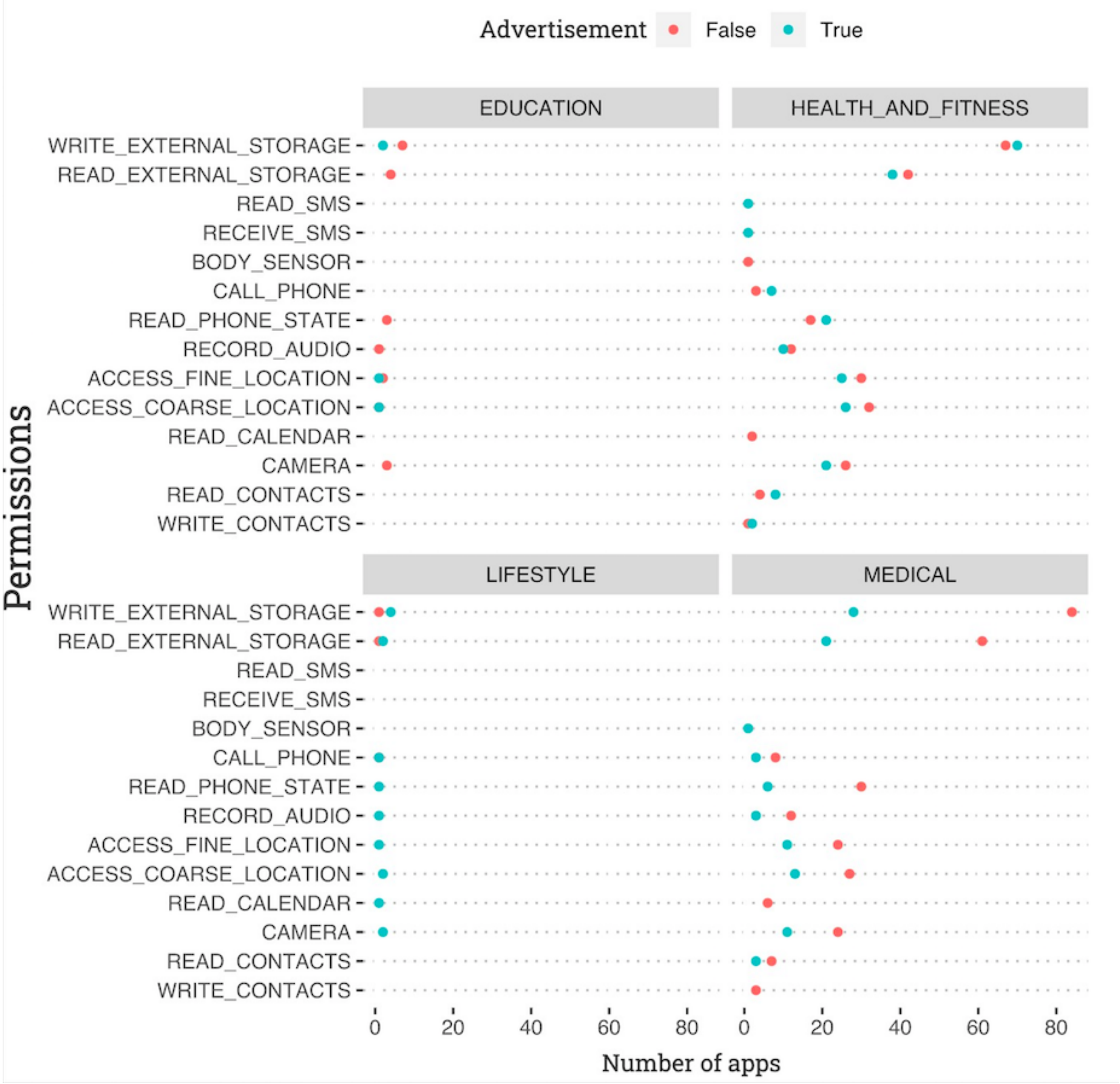
As explained below, dangerous permissions refer to permissions that might lead to data breaches of private information [37]. From the 497 diabetes apps included in our final analysis, a substantial number of them—297 (59.8%)—required dangerous permissions. Table 3 shows, in decreasing order, which dangerous permissions were most frequently requested by the apps.

Table 3. Summary results of apps with the requested privacy-related permissions.

Dangerous permission	Diabetes apps that requested it (N=497), n (%)
Write external storage	272 (54.7)
Read external storage	169 (34.0)
Access coarse location	103 (20.7)
Access fine location	95 (19.1)
Camera	89 (17.9)
Get accounts	82 (16.5)
Read phone state	81 (16.3)
Record audio	39 (7.8)
Call phone	23 (4.6)
Read contacts	22 (4.4)
Others (the sum of the remaining dangerous permissions)	28 (5.6)

In addition, Figure 2 illustrates the number of apps that required each of the top 14 dangerous permissions, arranged by category. The four quadrants represent each of the four categories to which the apps belonged: education, health and fitness, medical, and lifestyle. In addition, the "Advertising" tag indicates whether an app contained advertising: the ones in blue contained advertising, while the ones in red did not. The x-axis shows the number of apps, while the y-axis lists the 14 most requested dangerous permissions.

Figure 2. The top 14 dangerous permissions by app category (lifestyle, medical, education, and health and fitness) and type of privacy-related permission requested, as well as whether they included advertising (“True”) or not (“False”).



Discussion

Principal Results and Comparison With Previous Work

Although we identified the apps requesting access to the camera (89/497, 17.9%), we need to study the actual usage of apps in order to fully understand the context before we consider that access to be a potential risk. For instance, in the case of diabetes, it is very common to use the camera for food logging. On the other hand, except for advertising or fitness tracking (eg, calorie counting), the need for the user’s geolocation data seems difficult to justify. In this sense, what might be acceptable in one app might not be reasonable in others. Similar studies found that 77 of 186 (41.4%) permissions requested by 58 popular German mHealth apps were not related in any way to the apps’ functionalities [38]. Moreover, 15 of 42 (35.7%) Android health and well-being apps accredited by the UK’s NHS Health Apps Library requested critical permissions for unjustifiable reasons [12]. Similarly, other research concluded that several popular mental health apps and mHealth apps requested permissions that were not aligned with the apps’ stated purposes [14,21]. One of the consequences of requesting unnecessary dangerous permissions is a decrease in users’ trust, acceptance, and use of these apps.

Another finding of this study was that 95.4% of the apps were free of charge. The business model of free apps is, in most cases, based on advertising (through services such as Google AdMob), resulting in the disclosure of users’ critical data, either directly (through the app itself) or indirectly (through Google’s commercial advertising platforms).

The reliance on advertising of some of the studied apps might be linked to the high number of apps requesting geolocation, since location can increase advertisement revenue. A study on

NHS-accredited apps found some evidence that patients' data were information for advertisers [12]. Other studies also found that users' information was shared in 19 of 24 popular medication-related apps in the United Kingdom, the United States, Canada, and Australia [39]. Research of privacy in the top 36 mental health and smoking cessation apps also found a lack of compliance with disclosing or sending data to third-party providers [40]. Although app developers usually claim that they do not collect or share personally identifiable data, users can be easily identified by correlating advertising services using data analytics [39].

In addition, 28.4% of the studied apps did not provide a privacy policy website, which corroborates results from other research that demonstrated that 48% of 17,991 free Android apps did not have a privacy policy [18]. Building on this finding, 81% of 154 Android apps related to hypertension and diabetes did not refer to a privacy policy [33]. In addition, a privacy policy was missing in 417 of 600 (69.5%) prominent mHealth apps [41]. Most likely, had we not discarded less reliable apps in our research, the percentage of apps that did not provide a link to a website with their privacy policy would have been higher [34]. The lack of a privacy policy is a critical fault, as it prevents users from properly understanding how apps treat their very sensitive personal information. Further, the discrepancy between apps' privacy policies and their actual features has been reported in several studies [12,18]. This issue might be partially attributed to the fact that app developers have insufficient knowledge about privacy best practices [42].

In our study, 59.8% of apps required at least one dangerous permission, the two most requested being write external storage (54.7%) and read external storage (34.0%). This finding confirms the results from previous research. For instance, the most common dangerous permissions requested by the most popular freeware mHealth apps were write external storage (90%) and read external storage (50%) [34]. For prominent mental health apps in the Google Play Store, the most frequently requested permissions were also write (73%) and read (73%) external storage. In addition, these two permissions were the most requested (79%) in medicine-related apps in the Google Play Store in the United Kingdom, the United States, Canada, and Australia [38]. These permissions may indeed jeopardize users' privacy because they allow developers to access users' data, photos, and videos stored on the device [33,34]. Another relevant finding was that health and fitness apps usually requested more dangerous permissions than apps belonging to other categories [21].

Apps' ever-changing functionality and privacy policies, as well as their complexity, do not facilitate matters, either. Moreover, having to manually accept dangerous permissions when using an app poses an additional challenge that can have detrimental consequences, particularly for less knowledgeable users. For instance, individuals with low literacy rates or the elderly would require adequate training to truly understand what they are consenting to before using diabetes apps. Existing tools to evaluate eHealth literacy skills [43] do include security awareness as one of their dimensions. However, the complexity of potential security issues is increasing, and it might be necessary to develop new tools and training methods for both patients and health care providers.

Practical Implications

These findings have very important practical implications for users, physicians, developers, and policy makers [44,45]. To select an appropriate mobile app for diabetes, end users should be aware of what type of personal data is collected, used, and shared by a certain app by carefully reading the app's description, terms of use, and privacy policy.

In addition, it is imperative to emphasize the need for training so that users are able to understand complex privacy policies and terms of service and are fully aware of the privacy risks derived from the sharing of their data with third parties. Users should also be knowledgeable about the different types of dangerous permissions so that they can discern how each particular permission may jeopardize their data. The ultimate goal is to empower users so that they can autonomously and proficiently deny access to any unjustifiable dangerous permission.

To minimize the privacy risks derived from using diabetes apps, savvy users should use AdBlock or encryption apps [33]. Moreover, health care providers should ensure that the apps they recommend to patients adhere to a strict privacy code, and they should assist users in selecting suitable apps by explaining both the apps' benefits and their risks.

App developers should enforce their apps' full compliance with internationally recommended standards and practices [46-49]. Specifically, developers must ensure that their apps' privacy policies are always readily available, very simple to read, and able to be understood by any user. Further, their apps should never request dangerous permissions not directly related to the apps' declared purpose. Developers should not—without the users' explicit consent—collect, use, or share user data for any purpose outside of the predefined scope of the app, and all data sharing practices should be transparently disclosed to users. Last but not least, developers should be aware of diverse privacy laws and data protection legislation, which differ greatly depending on the country or region of use.

In terms of privacy laws, apps tend to adhere to the data protection legislation in the developers' country of origin but not in the apps' country of use. Therefore, regulators around the world should collaborate to establish a specific international accreditation program for diabetes apps. Such a program should be based on unified privacy best practices in which user privacy is the main priority. Because app developers reserve the right to change their privacy policies at any given time and modify their apps' declared purpose and functionalities, regulators should regularly monitor developers' adherence to the recommended privacy practices. As well, regulators should emphasize developers' responsibility and accountability for protecting user data. In addition, app stores should mandate stringent principles and standards that actually compel developers to provide simple and intelligible privacy policies in their apps, especially taking into consideration untrained or illiterate users.

Limitations

We opted to use the free version of the commercial platform 42Matters instead of the Google Play Store because the Google Play Store had a limit of 250 apps per query.

Another limitation was that the developed module exclusively searched for all diabetes apps that contained the root words diabet or mellitus in the title field. There are some diabetes apps in which the aforementioned root words appear in the app's description but not in the app's name. Therefore, some diabetes-related apps may have been excluded from the study. However, this criterion was selected for two principal reasons: (1) to ensure that only truly diabetes-related apps were retrieved, and (2) to make the best use of limited resources (there was neither enough time nor enough labor to thoroughly screen 4700+ apps, many of which bore no relation whatsoever to diabetes). In this sense, our research was not intended to be exhaustive. Rather, we wanted to quantify and evaluate the overall privacy characteristics of the most representative sample of diabetes-related apps. A broader search (ie, to query for all apps that contained the root words diabet or mellitus in the apps' descriptions) would certainly have yielded many false positives of apps unrelated to diabetes and hence required a very resource-intensive manual screening of the apps, which would have been an unnecessary complication of the overall analysis process.

The study did not comprehensively address either the fact that the number of permissions an app requests does not necessarily reflect how risky the app may be. For instance, an app requesting, unnecessarily, a single dangerous permission, could seriously endanger users' personal data by collecting and illegitimately sharing them. On the other hand, an app requesting multiple dangerous permissions, but for valid technical or functional needs, could be considered safe. Therefore, the amount of personal information that users are putting at risk depends on many factors, such as the app's functionality, the permissions it requests, and the context in which these permissions are being used [50]. To perform a more complete assessment of apps' privacy risks, additional technical, human, and contextual research (eg, analysis of the skills of patients using diabetes apps) should be conducted. For example, when dealing with privacy issues in health apps, an important factor to be considered would be the legitimacy of the request, as highlighted in a recent publication on mHealth apps for cancer in which the authors evaluated a new scale to assess the privacy policies of mHealth apps [51]. Tracking users' location might be fair in the case of reporting a medical emergency (eg, hypoglycemic crisis).

Although the methodology employed in this research was robust and Google is continuously improving Android and the Play Store's security policy, this study found evidence that it is extremely difficult to prove whether diabetes apps actually comply with their privacy policies. In fact, even Google cannot control the many malicious apps that are frequently uploaded by hackers in its Play Store and is consequently forced to periodically remove massive numbers of these fraudulent apps [52-54]. Further, a recently published two-year study discovered 2040 potential counterfeit apps that contained malware in the Google Play Store [55].

This study did not cover all of the elements related to the privacy and security of diabetes apps. Privacy protection cannot be guaranteed solely by controlling permissions; for instance, unsecure internet connections can also jeopardize the privacy of mobile app users. Finally, our study only evaluated the apps on one app store; the privacy policies and the requested dangerous permissions in other app stores, such as Apple's App Store or Samsung's Galaxy Store, might have yielded different outcomes. However, Android's Google Play Store was also chosen due to its popularity.

Future Research

A possible expansion of the research could include investigating those diabetes apps that were excluded from this research, either because they belonged to nonrelevant categories or because the developed module did not search for the root words in the apps' description field. Future research could also focus on analyzing the taxonomy of app categories and match them to officially recognized and standardized clinical categories, such as the Systematized Nomenclature of Medicine Clinical Terms or Medical Subject Headings. Related to that, there is a new trend emerging toward the creation of machine learning approaches to identify privacy issues in mobile apps [56,57]. However, to the best of our knowledge, those methods have unfortunately not yet been applied to health apps. Further, there is a need for homogenous approaches for the assessment of privacy in health apps, as was highlighted recently in a scoping review addressing the issue [58].

Finally, from a legal perspective, although many diabetes apps are available worldwide, their privacy policies usually only comply with the specific national data protection regulations of the developers' country or region of origin. For instance, the BeatO SMART Diabetes Management app claims that both its privacy policy and its terms of use fully adhere to Indian law, but if this app were to be used in the Middle East or the European Union, it would be unclear whether it would also comply with data protection laws in the country or region of use. This could indeed be another matter of study.

Conclusions

If privacy issues in diabetes mobile apps are not dealt with carefully, users may unwillingly and unknowingly share very sensitive private data. Therefore, it is crucial that all stakeholders are involved in the development of diabetes apps from the very beginning of the process in order to ensure apps' absolute compliance with data protection regulations and user privacy.

As the economic value of personal data increases [59], a completely new business model for apps has emerged: users pay for the usage of an app with their data, which is then sold to third parties, such as advertising clients [60]. The lesson to be learned is that there is a price to pay in exchange for free apps, usually at the expense of privacy. Consequently, new control measures are needed to enable users to decide which personal information they are willing to disclose in return for a certain service [61].

The importance of personal data protection laws and their endorsement are of utmost importance. Well-designed privacy policies may protect individuals by requiring consent for the collection, use, disclosure, or retention of sensitive personal and health information, and they may regulate the use of these extremely sensitive data, allowing users to modify their information as well as to revoke their previous consent.

Therefore, we recommend proper training for users, enforcement of strict data protection laws by governments and regulatory bodies, much tougher security policies and protocols in both Android apps and the Google Play Store, and the implication and supervision of all stakeholders in the app development process.

Authors' Contributions

JJF-S was the principal investigator. He designed the majority of the work, supervised the research, and took over most of the data interpretation and writing of the manuscript. In addition, he was responsible for developing the software module for extracting apps' metadata. MH and AA-A significantly contributed to the results and discussion sections of the paper. JV-A contributed to the overall manuscript and study by providing a clinical perspective. LF-L conceived the original research idea and greatly assisted with the design of the methodology and with the discussion section. Finally, CLS-B's contribution to the analysis and interpretation of the results was fundamental. All of the authors contributed to and approved the manuscript.

Conflicts of Interest

LF-L is co-founder of Adhera Health Inc (USA), a digital health company that provides digital therapeutic solutions for people with chronic conditions

Multimedia Appendix 1

Qualitative results of case studies.
[DOCX File , 5315 KB-Multimedia Appendix 1]

Multimedia Appendix 2

Top 10 Android's dangerous permissions identified.
[DOCX File , 16 KB-Multimedia Appendix 2]

Multimedia Appendix 3

Comma-separated values files.
[DOCX File , 14 KB-Multimedia Appendix 3]

References

1. Global report on diabetes. In: World Health Organization. Geneva: WHO Library; 2016:1-88.
2. Forbes J, Fotheringham A. Vascular complications in diabetes: old messages, new thoughts. Diabetologia 2017 Nov;60(11):2129-2138. [doi: 10.1007/s00125-017-4360-x] [Medline: 28725914]
3. Bourne RRA, Stevens GA, White RA, Smith JL, Flaxman SR, Price H, et al. Causes of vision loss worldwide, 1990–2010: a systematic analysis. The Lancet Global Health 2013 Dec;1(6):e339-e349. [doi: 10.1016/S2214-109X(13)70113-X]
4. Hanyu H. Diabetes-Related Dementia. Adv Exp Med Biol 2019;1128:147-160. [doi: 10.1007/978-981-13-3540-2_8] [Medline: 31062329]
5. Klonoff DC. The current status of mHealth for diabetes: will it be the next big thing? J Diabetes Sci Technol 2013 May 01;7(3):749-758 [FREE Full text] [doi: 10.1177/193229681300700321] [Medline: 23759409]
6. mHealth App Developer Economics 2015. Research 2 Guidiance. Berlin; 2015. URL: http://research2guidance.com/product/mhealth-developer-economics-2015/ [accessed 2019-09-08]
7. Jia Z, Gavriel S, editors. Human Aspects of IT for the Aged Population. Social Media, Games and Assistive Environments. In: International Conference on Human-Computer Interaction. Switzerland: Springer, Cham; 2019.
8. Arnhold M, Quade M, Kirch W. Mobile applications for diabetics: a systematic review and expert-based usability evaluation considering the special requirements of diabetes patients age 50 years or older. J Med Internet Res 2014 Apr 09;16(4):e104 [FREE Full text] [doi: 10.2196/jmir.2968] [Medline: 24718852]
9. Jeon E, Park H. Experiences of Patients With a Diabetes Self-Care App Developed Based on the Information-Motivation-Behavioral Skills Model: Before-and-After Study. JMIR Diabetes 2019 Apr 18;4(2):e11590 [FREE Full text] [doi: 10.2196/11590] [Medline: 30998218]
10. Giunti G, Giunta DH, Guisado-Fernandez E, Bender JL, Fernandez-Luque L. A biopsy of Breast Cancer mobile applications: state of the practice review. Int J Med Inform 2018 Feb;110:1-9 [FREE Full text] [doi: 10.1016/j.ijmedinf.2017.10.022] [Medline: 29331247]

11. Giunti G, Kool J, Rivera Romero O, Dorronzoro Zubiete E. Exploring the Specific Needs of Persons with Multiple Sclerosis for mHealth Solutions for Physical Activity: Mixed-Methods Study. JMIR Mhealth Uhealth 2018 Feb 09;6(2):e37 [FREE Full text] [doi: 10.2196/mhealth.8996] [Medline: 29426814]
12. Huckvale K, Prieto JT, Tilney M, Benghozi P, Car J. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med 2015 Sep 25;13(1):214 [FREE Full text] [doi: 10.1186/s12916-015-0444-y] [Medline: 26404673]
13. Yom-Tov E, Fernandez-Luque L, Weber I, Crain SP. Pro-anorexia and pro-recovery photo sharing: a tale of two warring tribes. J Med Internet Res 2012 Nov 07;14(6):e151 [FREE Full text] [doi: 10.2196/jmir.2239] [Medline: 23134671]
14. Parker L, Halter V, Karliychuk T, Grundy Q. How private is your mental health app data? An empirical study of mental health app privacy policies and practices. Int J Law Psychiatry 2019 May;64:198-204. [doi: 10.1016/j.ijlp.2019.04.002] [Medline: 31122630]
15. Zhou L, Parmanto B, Alfikri Z, Bao J. A Mobile App for Assisting Users to Make Informed Selections in Security Settings for Protecting Personal Health Data: Development and Feasibility Study. JMIR Mhealth Uhealth 2018 Dec 11;6(12):e11210 [FREE Full text] [doi: 10.2196/11210] [Medline: 30538088]
16. Fougerouse P, Yasini M, Marchand G, Aalami OO. A Cross-Sectional Study of Prominent US Mobile Health Applications: Evaluating the Current Landscape. AMIA Annu Symp Proc 2017;2017:715-723 [FREE Full text] [Medline: 29854137]
17. Stoyanov SR, Hides L, Kavanagh DJ, Zelenko O, Tjondronegoro D, Mani M. Mobile app rating scale: a new tool for assessing the quality of health mobile apps. JMIR Mhealth Uhealth 2015 Mar 11;3(1):e27 [FREE Full text] [doi: 10.2196/mhealth.3422] [Medline: 25760773]
18. Parker L, Karliychuk T, Gillies D, Mintzes B, Raven M, Grundy Q. A health app developer's guide to law and policy: a multi-sector policy analysis. BMC Med Inform Decis Mak 2017 Oct 02;17(1):141 [FREE Full text] [doi: 10.1186/s12911-017-0535-0] [Medline: 28969704]
19. Wang Y, Min J, Khuri J, Xue H, Xie B, A Kaminsky L, et al. Effectiveness of Mobile Health Interventions on Diabetes and Obesity Treatment and Management: Systematic Review of Systematic Reviews. JMIR Mhealth Uhealth 2020 Apr 28;8(4):e15400 [FREE Full text] [doi: 10.2196/15400] [Medline: 32343253]
20. Wu Y, Yao X, Vespasiani G, Nicolucci A, Dong Y, Kwong J, et al. Mobile App-Based Interventions to Support Diabetes Self-Management: A Systematic Review of Randomized Controlled Trials to Identify Functions Associated with Glycemic Efficacy. JMIR Mhealth Uhealth 2017 Mar 14;5(3):e35 [FREE Full text] [doi: 10.2196/mhealth.6522] [Medline: 28292740]
21. Pustozerov E, von Jan U, Albrecht U. Evaluation of mHealth Applications Security Based on Application Permissions. Stud Health Technol Inform 2016;226:241-244. [Medline: 27350515]
22. Quevedo Rodríguez A, Wägner AM. Mobile phone applications for diabetes management: A systematic review. Endocrinol Diabetes Nutr 2019 May;66(5):330-337. [doi: 10.1016/j.endinu.2018.11.005] [Medline: 30745121]
23. iTunes Search API Internet. Apple Inc. URL: https://affiliate.itunes.apple.com/resources/documentation/itunes-store-web-service-search-api/ [accessed 2019-09-04]
24. Mobile App Intelligence | 42matters Internet. 42matters. URL: https://42matters.com/ [accessed 2019-07-02]
25. App Manifest Overview. Android Developers. URL: https://developer.android.com/guide/topics/manifest/manifest-intro [accessed 2019-06-30]
26. Zhang M, Ying J, Song G, Fung DS, Smith H. Attention and Cognitive Bias Modification Apps: Review of the Literature and of Commercially Available Apps. JMIR Mhealth Uhealth 2018 May 24;6(5):e10034 [FREE Full text] [doi: 10.2196/10034] [Medline: 29793899]
27. Mendiola MF, Kalnicki M, Lindenauer S. Valuable features in mobile health apps for patients and consumers: content analysis of apps and user ratings. JMIR Mhealth Uhealth 2015 May 13;3(2):e40 [FREE Full text] [doi: 10.2196/mhealth.4283] [Medline: 25972309]
28. car A, Kinne J, Resch B. Generating Big Spatial Data on Firm Innovation Activity from Text- Mined Firm Websites. giforum 2018;1:82-89. [doi: 10.1553/giscience2018_01_s82]
29. 42Matters extraction script. GitHub. 2019. URL: https://github.com/jose-javier-flors-sidro/42Matters-webcrawler [accessed 2020-01-28]
30. Google's categories description. Play Console Help. 2019. URL: https://support.google.com/googleplay/android-developer/answer/113475?hl=en-419 [accessed 2019-06-18]
31. Permissions on Android. Android Developers. URL: https://developer.android.com/guide/topics/permissions/overview [accessed 2019-09-04]
32. Xu W, Zhang F, Zhu S. Permlyzer: Analyzing permission usage in Android applications. 2013 Presented at: IEEE 24th International Symposium on Software Reliability Engineering (ISSRE); 2013; Pasadena, CA p. 400-410. [doi: 10.1109/ISSRE.2013.6698893]
33. Nora CB, Frédéric C, Sushil J, Anas Abou EK, Thierry S, editors. ICT Systems Security and Privacy Protection. In: IFIP International Information Security Conference. Berlin, Heidelberg: Springer; 2014.
34. Papageorgiou A, Strigkos M, Politou E, Alepis E, Solanas A, Patsakis C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. IEEE Access 2018;6:9390-9403. [doi: 10.1109/ACCESS.2018.2799522]

35. Grundy Q, Held FP, Bero LA. Tracing the Potential Flow of Consumer Data: A Network Analysis of Prominent Health and Fitness Apps. J Med Internet Res 2017 Jun 28;19(6):e233 [FREE Full text] [doi: 10.2196/jmir.7347] [Medline: 28659254]
36. Chen J, Zhao Z, Shi J, Zhao C. A New Approach for Mobile Advertising Click-Through Rate Estimation Based on Deep Belief Nets. Comput Intell Neurosci 2017;2017:7259762-7259768 [FREE Full text] [doi: 10.1155/2017/7259762] [Medline: 29209363]
37. Cha Y, Pak W. Protecting contacts against privacy leaks in smartphones. PLoS One 2018 Jul 11;13(7):e0191502 [FREE Full text] [doi: 10.1371/journal.pone.0191502] [Medline: 29995881]
38. Hoppe A, Knackmuß J, Morgenstern M, Creutzburg R. Privacy Issues in Mobile Health Applications - Assessment of Current Android Health Apps. Electronic Imaging 2017 Jan 29;2017(6):76-83. [doi: 10.2352/ISSN.2470-1173.2017.6.MOBMU-302]
39. Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ 2019 Mar 20;364:l920 [FREE Full text] [doi: 10.1136/bmj.l920] [Medline: 30894349]
40. Huckvale K, Torous J, Larsen ME. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. JAMA Netw Open 2019 Apr 05;2(4):e192542 [FREE Full text] [doi: 10.1001/jamanetworkopen.2019.2542] [Medline: 31002321]
41. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. J Am Med Inform Assoc 2015 Apr;22(e1):e28-e33 [FREE Full text] [doi: 10.1136/amiajnl-2013-002605] [Medline: 25147247]
42. Balebako R, Marsh A, Lin J, Hong J, Faith CL. The Privacy and Security Behaviors of Smartphone App Developers. In: Internet Society. 2014 Presented at: NDSS Symposium 2014; 2014; San Diego, California. [doi: 10.14722/usec.2014.23006]
43. Chan CV, Matthews LA, Kaufman DR. A taxonomy characterizing complexity of consumer eHealth Literacy. AMIA Annu Symp Proc 2009 Nov 14;2009:86-90 [FREE Full text] [Medline: 20351828]
44. Wicks P, Chiauzzi E. 'Trust but verify'--five approaches to ensure safe medical apps. BMC Med 2015 Sep 25;13:205 [FREE Full text] [doi: 10.1186/s12916-015-0451-z] [Medline: 26404791]
45. Wyatt JC. How can clinicians, specialty societies and others evaluate and improve the quality of apps for patient use? BMC Med 2018 Dec 03;16(1):225 [FREE Full text] [doi: 10.1186/s12916-018-1211-7] [Medline: 30501638]
46. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: a review and recommendations. J Med Syst 2015 Jan;39(1):181. [doi: 10.1007/s10916-014-0181-3] [Medline: 25486895]
47. Shaping Europe’s digital future. Privacy Code of Conduct on mobile health apps. European Commision. URL: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps [accessed 2019-06-30]
48. Mobile Health App Developers: FTC Best Practices. Federal Trade Commission. URL: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices [accessed 2019-06-30]
49. Mobile privacy A better practice guide for mobile app developers. Office of the Australian Information Commissioner. 2013. URL: https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/
50. Atkinson M. Apps Permissions in the Google Play Store. Pew Res Cent - Internet Technology. 2015 Nov 10. URL: http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/ [accessed 2019-09-04]
51. Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Assessment of the Fairness of Privacy Policies of Mobile Health Apps: Scale Development and Evaluation in Cancer Apps. JMIR Mhealth Uhealth 2020 Jul 28;8(7):e17134 [FREE Full text] [doi: 10.2196/17134] [Medline: 32720913]
52. Telecom. Google removing 100 apps by Chinese developer from Play Store. Telecom.com. URL: https://telecom.economictimes.indiatimes.com/news/google-removing-100-apps-by-chinese-developer-from-play-store/69089407 [accessed 2019-06-30]
53. Androidauthority. BeiTaAd adware infects 238 apps on Google Play Store. URL: https://www.androidauthority.com/beitaad-google-play-store-994796/ [accessed 2019-06-30]
54. Adware-Ridden Apps in Google Play Infect 30 Million Android Users. Threatpost. URL: https://threatpost.com/google-play-adware-30-million/144098/ [accessed 2019-06-30]
55. Rajasegaran J, Seneviratne S, Jourjon G. A Neural Embeddings Approach for Detecting Mobile Counterfeit Apps. arXivLabs 2018 Apr 26:1-11 [FREE Full text]
56. Liu B, Gong N. Personalized Mobile App Recommendation?: Reconciling App Functionality and User Privacy Preference. In: Association for Computing Machinery. 2015 Presented at: Eighth ACM International Conference on Web Search and Data Mining (WSDM '15); 2015; New York p. 315-324. [doi: 10.1145/2684822.2685322]
57. Zhu H, Xiong H, Ge Y, Chen E. Mobile app recommendations with security and privacy awareness. In: 20th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '14). 2014 Presented at: Association for Computing Machinery; 2014; New York p. 951-960. [doi: 10.1145/2623330.2623705]
58. Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Privacy Assessment in Mobile Health Apps: Scoping Review. JMIR Mhealth Uhealth 2020 Jul 02;8(7):e18868 [FREE Full text] [doi: 10.2196/18868] [Medline: 32459640]
59. IoT Research – Smartbands. Securelist. URL: https://securelist.com/iot-research-smartbands/69412/ [accessed 2019-09-04]

60. Leontiadis I, Efstratiou C, Picone M, Mascolo C. Don't kill my ads! Balancing privacy in an ad-supported mobile application market. In: Twelfth Workshop on Mobile Computing Systems & Applications (HotMobile '12). 2012 Presented at: ssociation for Computing Machinery; 2012; New York p. 1-6. [doi: 10.1145/2162081.2162084]
61. The Security and Privacy of Wearable Health and Fitness Devices. Security Intelligence Logo. URL: https://securityintelligence.com/the-security-and-privacy-of-wearable-health-and-fitness-devices/ [accessed 2019-09-04]

Abbreviations

API: application programming interface
CSV: comma-separated values
DM: diabetes mellitus
mHealth: mobile health

Edited by G Eysenbach; submitted 18.09.19; peer-reviewed by R Zowalla, G Klein, L Zhou; comments to author 19.12.19; revised version received 03.05.20; accepted 29.07.20; published 13.01.21

Please cite as:
Flors-Sidro JJ, Househ M, Abd-Alrazaq A, Vidal-Alaball J, Fernandez-Luque L, Sanchez-Bocanegra CL
Analysis of Diabetes Apps to Assess Privacy-Related Permissions: Systematic Search of Apps
JMIR Diabetes 2021;6(1):e16146
URL: http://diabetes.jmir.org/2021/1/e16146/
doi: 10.2196/16146
PMID: 33439129