Internet Interventions 15 (2019) 110–115

Contents lists available at ScienceDirect

Internet Interventions

journal homepage: www.elsevier.com/locate/invent

Reviewing the data security and privacy policies of mobile apps for depression

Kristen O'Loughlin[a,b,*], Martha Neary[b,c], Elizabeth C. Adkins[b], Stephen M. Schueller[b,c]

[a] Virginia Commonwealth University, Department of Psychology, United States of America
[b] Northwestern University, Feinberg School of Medicine, Department of Preventive Medicine, Center for Behavioral Intervention Technologies, United States of America
[c] University of California, Irvine, Department of Psychological Science, United States of America

ARTICLE INFO

Keywords:
Depression
Mental health
Mobile apps
mHealth
Review
Data privacy

ABSTRACT

Background: Mobile apps have become popular resources for mental health support. Availability of information about developers' data security procedures for health apps, specifically those targeting mental health, has not been thoroughly investigated. If people are to use and trust these tools for their mental health, it is crucial we evaluate the transparency and quality around the data practices of these apps. The present study reviewed data security and privacy policies of mobile apps for depression.

Methods: We reviewed mobile apps retrieved from iTunes and Google Play stores in October 2017, using the term "depression", and evaluated the transparency of data handling procedures of those apps.

Results: We identified 116 eligible mobile phone apps. Of those, 4% (5/116) received a transparency score of acceptable, 28% (32/116) questionable, and 68% (79/116) unacceptable. Only a minority of the apps (49%) had a privacy policy. The availability of policies differed significantly by platform, with apps from iTunes more likely to have a policy than from the Google Play store. Mobile apps collecting identifiable information were significantly more likely to have a privacy policy (79%) compared to those collecting only non-identifiable information (34%).

Conclusion: The majority of apps reviewed were not sufficiently transparent with information regarding data security. Apps have great potential to scale mental health resources, providing resources to people unable or reluctant to access traditional face-to-face care, or as an adjunct to treatment. However, if they are to be a reasonable resource, they must be safe, secure, and responsible.

1. Introduction

The increasing use and integration of mobile apps into our daily lives provides opportunity for public health innovation and community benefit. As of 2017, five million mobile phone applications were available through iTunes and Google Play (Statista, 2017), and over 10,000 are for mental health (Torous and Roberts, 2017). These mental health apps provide an array of supportive services. These features include: inputting and organizing user data, accessing or transmitting that information, receiving didactic material to promote psychoeducation, and using interactive tools to promote self-management (BinDhim and Trevena, 2015b). These features impact users' ability to understand, communicate, and treat their mental health symptoms.

People appear willing and interested to use mobile apps for mental health support. Both community samples and out-patient psychiatric patients report positive attitudes towards the use of apps to monitor their mental health symptoms and conditions (Proudfoot et al., 2010; Torous et al., 2014). Indeed, the number of downloads for mental health apps has doubled over the course of just four years (Research2guidance, 2016). Many apps target common mental health conditions that are widespread and undertreated. Depression, for example, affects 8.1% of Americans at any given time (Brody et al., 2018); however, only 21% of those affected receive effective treatment (González et al., 2010). Mobile health app developers reported that as of 2017, depression was in the top three health conditions with the best market potential for digital health apps (Research2guidance, 2017). This is matched by development, with reportedly 18% of mental health apps targeting depression (IMS Institute for Healthcare Informatics, 2015). As such, examining depression apps is likely an important cross-section of currently available mental health apps.

Due to user acceptability and demand, new mental health apps are being developed rapidly, though with limited regulatory oversight.

* Corresponding author at: Virginia Commonwealth University, Department of Psychology, 806 W. Franklin Street, Richmond, VA 23223, United States of America.
E-mail address: oloughlink@mymail.vcu.edu (K. O'Loughlin).

https://doi.org/10.1016/j.invent.2018.12.001
Received 10 July 2018; Received in revised form 18 October 2018; Accepted 17 December 2018
Available online 20 December 2018

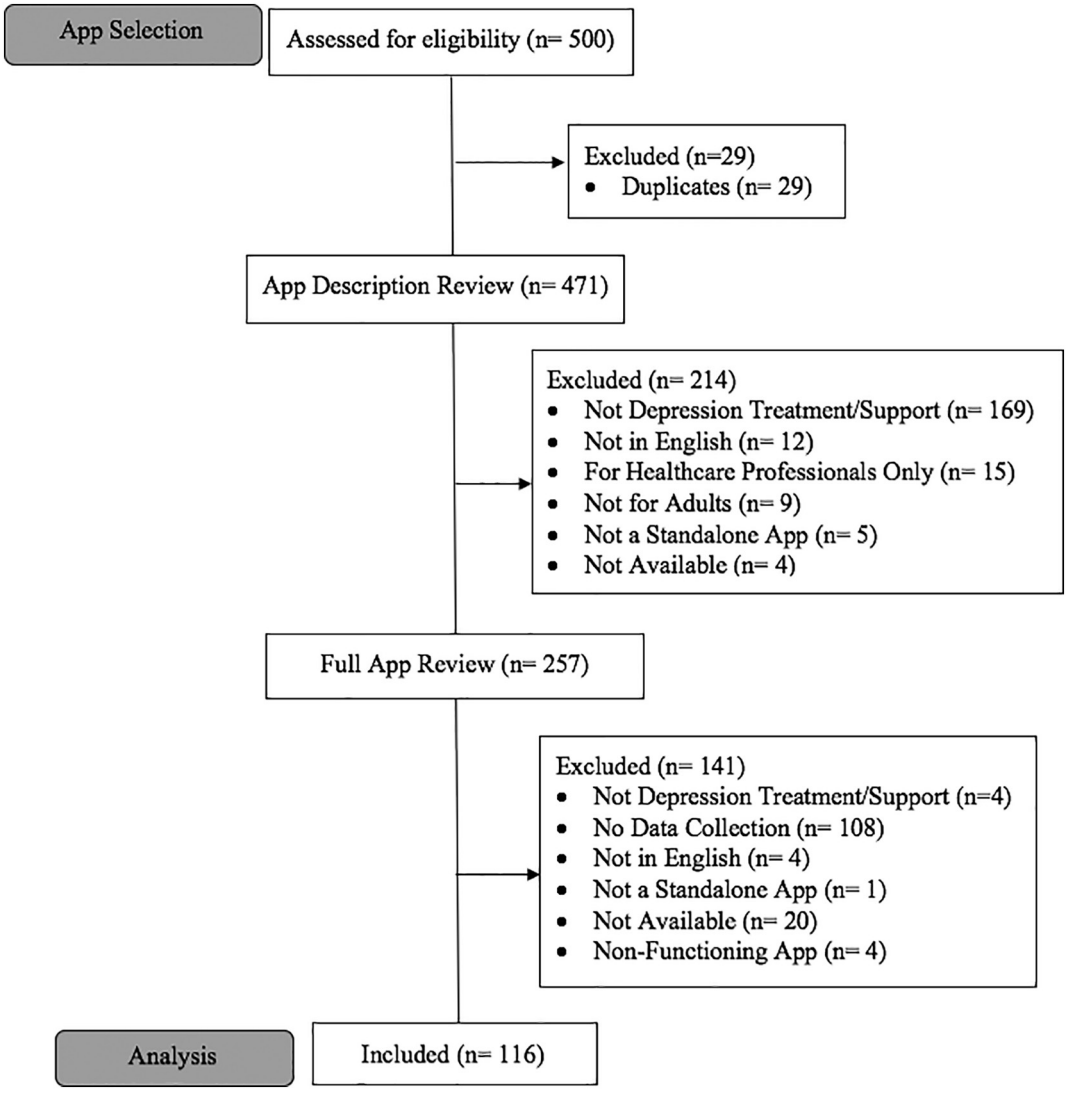

Fig. 1. App inclusion flow diagram.

Indeed, 2016 saw a 57% increase in mental health apps across all major app stores (Research2guidance, 2016). It is unfeasible to completely regulate this enormous and growing volume of apps. To combat this issue, the US Food and Drug Administration (FDA) has made three distinct categories of mobile health apps: (1) apps that are not medical devices, (2) apps that are medical devices but the FDA will exercise enforcement discretion (i.e., will not be regulated), and (3) those which are medical devices and require regulatory oversight. Most mental health apps do not fall into this third category and thus receive little attention (BinDhim and Trevena, 2015a). The second category includes mobile apps that help people with diagnosed mental health conditions maintain their coping skills through regular tips or audio messages. The Federal Trade Commission compiled a list of best practices to advise the development of mental health apps, such as minimizing collection of user data and limiting both access and permissions to the users' phone. However, these practices are not adequately enforced (Federal Trade Commission, 2016). Consequently, many mental health mobile apps fall outside of formal regulation in the US, and therefore, there are few checks on these products before being made available to consumers.

The lack of regulation around the dissemination of mobile health apps raises concern about their quality and practices. One practice that requires careful scrutiny is that of developers' privacy policies and data security practices. Data security for mental health apps is a widespread concern (Powell et al., 2014). A survey of mental health app users found that over 70% rated both the presence of a privacy policy and data encryption as important to them (Schueller et al., 2018). Data security is also a primary concern among mental health professionals when recommending mobile apps to clients (Aguilera and Muench, 2012). Thus, user privacy and data security are of utmost importance. The American Psychiatric Association's App Evaluation model (Torous et al., 2018) has risk, privacy, and security as one of the foundational levels of their review pyramid. This model lists a series of questions that can help users ensure that an app will not cause harm by violating user safety, security, and privacy. However it does not provide guidance as to the relative weighting of each question or the user's perception of potential harm associated with each.

The availability and adequacy of information about developers' data security procedures for apps, specifically those targeting mental health, has not been thoroughly investigated. Rosenfeld et al. (2017) evaluated the data security and privacy of publicly available mobile phone apps targeting dementia. Results showed fewer than half of the apps that collect user information had a privacy policy and the policies were missing important information regarding data handling. This paper sheds important light on the unavailability of privacy policies and deficiency in transparency around developers' practices with data security. However, Rosenfeld et al. (2017) only explored mobile phone apps for dementia, and to this point, more research is needed to understand apps for other clinical issues, especially those that are common

	Yes	ID information No	No-ID information No
Does the app have a privacy policy?			
Does the app provide the option of a pin entry or log-in process to view and enter user data?			
Does the privacy policy state that the app/server encrypts the entered data OR state that user information is stored locally?			
Does the policy describe the information storage and sharing procedures related to user entered information OR state that user information is stored locally			
Does the privacy policy state whether or not users can delete entered information OR state that user information is stored locally?			
Does the privacy policy state whether or not users can edit entered information OR state that user information is stored locally?			
Does the privacy policy state that users can use the app WITHOUT entering identifiable information OR state that user information is stored locally?			

Scoring:
If all white checked→score acceptable
If any dark grey checked→score unacceptable
If any light grey (but no dark grey)→score questionable

ID: identifiable information, which can be used to trace or identify a person, such as full name or e-mail

Fig. 2. Checklist used to evaluate presence and comprehensiveness of privacy and data security policies.

and have a multitude of apps that claim to address them.

Given the widespread use of mobile phone apps as well as their ability to provide support for depression, it is crucial we evaluate the transparency and quality around their data practices. To date, no studies have reviewed data security and privacy policies of publicly available mobile apps for depression. The present study sought to understand the availability and thoroughness of privacy policies for mobile apps targeting depressed users, and if those practices differed based upon which app store they were developed for or the type of data collected. Building on established guidelines, we used a checklist-based approach for evaluation that produced three levels of conclusions similar to those proposed by the American Psychiatric Association's App Evaluation Model. Based upon the findings of Rosenfeld et al. (2017), we anticipated to find a significant number of mobile apps with either no privacy policy or a poor-quality privacy policy. This hypothesized outcome represents a broader problem with developers' communication to users of data security procedures.

2. Materials and methods

2.1. App selection process

We used a structured review process to guide the collection of apps. Fig. 1. outlines the inclusion and exclusion of apps during each round of evaluations. Within the iTunes App Store and Google Play Store, we searched for apps using the search term “depression”. We adopted this search strategy in line with other reviews of mental health apps in this space (e.g., Shen et al., 2015; Huguet et al., 2016). We conducted this search on October 15, 2017 in Chicago, IL. As Google Play presents a maximum of 250 results from any search, we also limited apps included from the iTunes App Store to the first 250 apps to make sure results would not be biased towards findings from the iTunes App Store. This resulted in 500 apps for initial review. This seemed like a sufficient number of apps as research shows that most users do not look beyond the top 10 results or even download apps past the top five (Dogruel et al., 2015). It is estimated that 10,000 mental health apps exist (Torous and Roberts, 2017) and 18% target depression (IMS Institute for Healthcare Informatics, 2015). Therefore, we reviewed roughly a quarter of the 1800 available depression apps.

2.2. Inclusion/exclusion

Inclusion and exclusion were determined in two steps by a group of three raters who were the first through third authors. We first identified and eliminated any apps that were duplicates (n = 29). The first step was based on the descriptions within the app stores, and the second step involved downloading and reviewing the app. Certain inclusion and exclusion criteria could only be determined in the second stage of review as they required information only available by downloading and reviewing the app itself. Apps met inclusion criteria if they (1) aim to provide support or treatment for depression; (2) are in English; (3) are designed for adults; and (4) collect data. Apps were excluded if they are (1) for healthcare professionals only; (2) not a standalone app; (3) not available; and (4) did not function. At each stage, each app was reviewed by two of the three raters. Raters obtained an 86.7% initial agreement for the first stage of screening (examining app store descriptions), and 89.5% initial agreement for the second stage (reviewing the downloaded apps). For both stages, each disagreement was discussed as a group and full agreement was met before proceeding. 384 apps were excluded, leaving a total of 116 apps for the final evaluation of the privacy policy and security. All 116 eligible apps were intended for patient use.

2.3. Measurement development & scoring

For the 116 eligible apps, we evaluated the presence and quality of a privacy policy with questions that aim to assess comprehensiveness of an app's documentation in describing data collection and storage practices and policies. Of note, while we evaluated the comprehensiveness of the privacy policies, we did not conduct a technical audit to evaluate if the data handling procedures outlined in the policy are actually implemented.

The list of questions can be seen in Fig. 2. This checklist was developed by adapting questions from Baumel et al.'s (2017) Enlight Evaluation tool, which aimed to be a comprehensive evaluation of mobile and web-based eHealth interventions. We selected items relevant to privacy and basic security with adaptations guided by the American Psychiatric Association's App Evaluation Model. All questions are answered either “Yes” or “No”. “Yes” responses required that the privacy policy explicitly state the content of the question. “No” responses resulted when the information was absent from the privacy policy, thus an end user would not know that aspect of their data's handling. In the Enlight privacy and security checklists, lower scores represent higher quality of data security. This is somewhat counterintuitive because higher scores tend to be interpreted more favorably (as in commercial app stores, for example). To guide interpretation of the checklist, resulting scores were grouped into three categories: Acceptable, Questionable, Unacceptable (for an explanation of scoring, see Fig. 2). The first 23 apps were rated by two of the three raters to establish reliability. Consistency of ratings between raters was considered excellent with intraclass correlation coefficients ranging from 0.923 to 1.00 (Koo and Li, 2016). Given this level of consistency the remaining apps were rated by a single rater. All reviews were completed in a one-month period.

3. Results

Of the 116 eligible apps, 4% (5/116) received a transparency score of acceptable, 28% (32/116) questionable, and 68% (79/116) unacceptable. This was mostly due to the fact that slightly less than half of the apps (49%, 57/116) had a privacy policy. Privacy policies, when available, were found in various places (see Table 1). Most frequently they were available in the app stores (79%), whereas they were least frequently available in the apps themselves (53%). Privacy policies provided in the app were rarely (11%, 13/116) provided to the user before other information was collected.

3.1. Google Play vs iTunes

The availability of privacy policies differed significantly by platform X^2 (1) = 6.07, p = .014. Table 2 details the availability of privacy policy for apps broken down by app platform (e.g., Google Play/Android and/or Apple iTunes/iOS). Single platform apps are those available on either Google Play/Android or Apple iTunes/iOS, multiplatform apps are those available on both. iTunes/iOS apps were more likely to report privacy policies. This was true even for those apps with a corresponding Google Play/Android version. However, there was no significant difference by platform as to whether privacy policies were provided prior to collecting user data X^2 (1) = 2.11, p = .147.

Table 1
Privacy policy availability (N = 57).

Criteria	Yes (%)	No (%)
App website	38 (68)	19 (32)[a]
App store	45 (79)	12 (21)
In app	30 (53)	27 (47)

[a] 2 apps included did not have a website.

Table 2
Privacy policy availability by platform.

	Single Platform		Multiplatform		Total	
	Google Play only	iTunes only	Google Play	iTunes	Google Play	iTunes
Yes	19	20	15	18	34	38
No	38	18	5	2	43	20

3.2. Identifiable vs non-identifiable

Finally, we compared the availability and comprehensiveness of privacy policies based on whether or not the app collected identifiable information (i.e., information that can be used to trace or identify a person, such as full name or e-mail) or non-identifiable information (e.g., journal entry, mood or symptom rating, etc.). Not surprisingly, mobile apps which collected identifiable information were significantly more likely X^2 (1) = 21.14, $p < .001$ to have a privacy policy (79%) compared to those that collected only non-identifiable information (34%).

Closer examination of the privacy policies for apps collecting identifiable vs. non-identifiable information revealed two points of difference in comprehensiveness, as shown in Table 3. For apps collecting identifiable information, nearly all privacy policies discussed their storage and sharing practices (87%) and included password protection (87%). This was less frequently covered in apps not collecting identifiable information.

Two mobile applications included features to support the user in directly sharing information with a provider through the app. Both had accessible privacy policies, though neither mention HIPAA requirements for safeguarding medical information nor procedures they implement to be in compliance.

4. Discussion

Mobile apps offer tremendous potential to facilitate and enhance mental health care and are increasing in prevalence and use. As technology continues to develop, it is likely that more technologies will emerge as adjuncts or alternatives to traditional treatments for conditions such as depression. However, while these digital tools offer exciting new opportunities for mental health care, they come with significant drawbacks, such as insufficient data security and privacy policies, as highlighted by this paper. Such issues need to be addressed in order to increase consumer and clinician confidence in using mental health apps. Currently, low confidence is a barrier to widespread adoption.

Alarmingly, only 4% of the apps reviewed in this study had privacy policies which we deemed to provide sufficient information regarding their data handling procedures. The majority of apps reviewed (68%) were not sufficiently transparent with this information and received

Table 3
Privacy policy specifications for apps which collect.

Criteria	Non-identifiable info (N = 26)		Identifiable info (N = 31)	
	Yes (%)	No (%)	Yes (%)	No (%)
Storage/share	15 (58)	11 (42)	27 (87)	4 (13)
Password protection	12 (46)	14 (54)	27 (87)	4 (13)
Server encrypts	9 (35)	17 (65)	15 (48)	16 (52)
Delete info	12 (46)	14 (54)	11 (35)	20 (65)
Edit info	11 (42)	15 (58)	15 (48)	16 (52)
Use w/o identifiable info[a]	–	–	11 (35)	20 (65)

[a] Final criteria does not apply to apps which only collect non-identifiable information.

unacceptable scores. Slightly over half of the apps reviewed had no privacy policy at all. Of the apps that did have a policy, they were often only provided after users were asked for information, meaning the apps had collected data before alerting users how that data could be used. The availability of privacy policies varied depending on the type of data collected by the app; apps collecting identifiable data were more likely to have a privacy policy than apps collecting non-identifiable data. This indicates an awareness of the importance of privacy among developers of apps soliciting personal information. Yet, not all apps collecting identifiable data provided policies, and those that did, did not disclose all aspects deemed relevant within our checklist. The availability of privacy policies also varied by platform; apps from iTunes were more likely than Google Play to have a policy, which is likely a reflection of different requirements in app stores. Our results parallel the findings of Rosenfeld et al. (2017), who found that two thirds of apps for dementia included in their review did not have a privacy policy. Seeing this pattern mirrored in our review of depression apps suggests that this may be a recurring pattern in mental health apps as a whole.

Among the privacy policies we did find, many policies were vague and lacked important information, such as details on encryption of data, password protection, and the ability to edit or delete entered information. In addition to being vague, many privacy policies are convoluted. Das et al.' (2018) conducted a readability analysis of privacy policies are determined most are not comprehensible to the general population. This mirrors previous findings that most app privacy policies require college-level literacy (Sunyaev et al., 2015). This lack of clarity might limit people's ability to understand the content of privacy policies.

Improving data security standards is not only in the interest of clinicians and consumers, but has a commercial advantage too. Uptake of apps will likely increase if users are more confident that their entered information is secure. Indeed, clinicians report they would use and recommend apps if privacy and security issues could be overcome (Schueller et al., 2016). Higher standards and increased regulation might improve clinician confidence in such products, thus increasing their comfort in recommending such tools. In Schueller et al.'s (2018) study of consumer interest in mental health apps, 74.2% (N = 602) of survey respondents said that encryption of data was important or very important to them, and 70.5% (N = 572) rated the availability of a privacy policy as important or very important. However, only 10.7% (N = 87) said that privacy and data security concerns would prevent them from using or downloading an app. In relation to the findings from this study, consumers have few available choices of apps with adequate disclosure and quality of their data security and privacy practices, thus making it challenging to incorporate this into decision making.

4.1. Limitations

Our study has several limitations. We excluded apps that did not appear to collect user information. However, we cannot be certain that these apps do not collect background data or information such as location. If so, the data security and privacy policies of these apps should be evaluated with similar rigor. Additionally, while we reviewed app policies, we did not audit data handling practices. Thus, we cannot ascertain that apps which have policies deemed “acceptable” are actually following the practices they outline. It is possible, therefore, that our findings overestimate the quality of privacy and data security of these apps. This is worrisome given that our potentially “best case” scenario was still quite grim. A recent paper which conducted static and dynamic analyses of mobile health apps privacy and data security found that few followed well-established practices and guidelines (Papageorgiou et al., 2018). In addition, a previously established app certification group, Happtique, faced challenges and shut down after several of the apps that it certified as having acceptable level of privacy and security were demonstrated to not be secure by a group of hackers. Lastly, while we evaluated the presence or absence of key pieces of information in the privacy policies we reviewed, we did not evaluate the comprehensibility of policies. Das et al. (2018) explored this within youth-focused apps, and found policies had high literacy demands. Based on our experience, we suspect evaluating the reading comprehension level required to understand privacy policies within apps designed for adults would produce similar findings.

4.2. Future directions

It is likely that this pattern of lack of transparency around data handling is repeated with mobile apps targeting other mental health conditions. Future research could review the policies of other mental health apps to obtain a broader picture of the state of the field of mental health apps. It is also worth noting that our study used an independent rating tool for privacy policies that draws from consensus from the research literature and expert opinions. Another approach would be to evaluate assessments or privacy policies from potential end users, for example clinicians or patients. One could even directly compare the adoption of apps on the basis of those that include privacy policies or not, or with privacy policies of varying quality. The rating tool itself, could also be evaluated based on clinician or patient feedback to determine if it reflects the concerns of these key stakeholder groups. These directions would help align these findings with the needs and interests of those who would use mental health apps in their practice and/or lives.

Formal regulation of data handling procedures within apps will likely remain lax. Many of the mental health apps included in our review would fall within the subset of which the FDA has decided to exercise enforcement discretion. Thus, we strongly encourage developers, and potentially app stores, to raise their standards. If people are to trust apps with their mental health information and hope that those apps might be useful for them, they should have confidence that their information is going to be used in ways that protects their safety, security, and privacy. Recent data security breaches have gained considerable media attention, such as Cambridge Analytica obtaining and misusing the private information of more than 50 million Facebook users, bringing issues of data privacy and security into public conscience. This may result in skepticism or hesitation around the use of digital health tools which collect personal information. The onus is on developers and app stores to be clear about the extent, and limitations, of privacy protections in order to increase public confidence in using tools. There may also be a role for third-party reviewers to help raise the bar.

The current paper focuses on understanding the existing state of privacy policies within mental health apps for depression, but stops short of exploring what would be the desired state of privacy policies for those apps. Such an exploration would require further input from stakeholders as previously noted not just in comprehensiveness and sufficiency of information, but also in terms of its' capabilities to be easily read and understood. It would also be worth considering from a regulatory perspective what is required of developers. This is an evolving landscape with new regulations emerging, such as the General Data Protection Regulation (GDPR), which impacts what data can be collected and how that collection needs to be disclosed. Nevertheless, future work could be more aspirational to further help developers determine how to create effective practices for data security and privacy and effectively convey those practices to end users.

5. Conclusion

Currently app developers are provided considerable latitude in their data security and privacy practices within health apps and how they explain these practices to users. Some developers are acting responsibly; for example, providing this information to consumers prior to obtaining any user information. However, as we found in the case of

apps for depression, this is the exception rather than the rule. The app marketplaces continue to have relatively few checks for developers who wish to disseminate a product. Apps advertising uses for mental health issues do not have any additional checks to validate their claims nor their data security and privacy. Apps have great potential to scale mental health resources, to provide them to people who are unable or reluctant to access traditional face-to-face care. If digital mental health resources are to be a reasonable option; however, it is not sufficient to show that they are effective, they must also be safe, secure, and responsible. Just as therapists are held to standards of responsible practice and confidentiality, mental health app developers should be held to standards of safety, security, and privacy. Enforcing such standards could also raise clinicians' confidence in recommending such products to their patients. We suggest that before clinicians recommend a mobile app to their client, they first obtain its privacy policy and evaluate it for the criteria listed in Fig. 2. Overall, our findings suggest the field has a long way to go in regards to transparency around data handling, however, and it is unlikely practices will change without calling attention to this large need.

Declaration of interest

Dr. Schueller receives funding from One Mind to direct and lead PsyberGuide, a non-profit project focused on identifying and evaluating mental health apps. Dr. Schueller is supported by a career development award from the National Institute of Mental Health (K08MH102336) and is an investigator with the Implementation Research Institute (IRI), at the George Washington University in St. Louis; through an award from the National Institute of Mental Health (5R25MH08091607) and the Department of Veterans Affairs, Health Services Research & Development Service, Quality Enhancement Research Initiative (QUERI).

References

Aguilera, A., Muench, F., 2012. There's an app for that: information technology applications for cognitive behavioral practitioners. Behav. Ther. 35 (4), 65–73.

Baumel, A., Faber, K., Mathur, N., Kane, J.M., Muench, F., 2017. Enlight: a comprehensive quality and therapeutic potential evaluation tool for mobile and web-based eHealth interventions. J. Med. Internet Res. 19 (3), e82.

BinDhim, N., Trevena, L., 2015a. Health-related smartphone apps: regulations, safety, privacy and quality. BMJ Innovations 1, 43–45.

BinDhim, N., Trevena, L., 2015b. There's an app for that: a guide for healthcare practitioners and researchers on smartphone technology. Online J. Public Health Inform. 7 (2), e218. https://doi.org/10.5210/ojphi.v7i2.5522.

Brody, D., Pratt, L., Hughes, J., 2018. Prevalence of Depression Among Adults Aged 20 and Over: United States, 2013–2016. Centers for Disease Control and Prevention, Center for Disease Control Retrieved from. www.cdc.gov/nchs/products/databriefs/db303.htm.

Das, G., Cheung, C., Nebeker, C., Bietz, M., Bloss, C., 2018. Privacy policies for apps targeted toward youth: descriptive analysis of readability. JMIR mHealth and uHealth 6 (1), e3.

Dogruel, L., Joeckel, S., Bowman, N.D., 2015. Choosing the right app: an exploratory perspective on heuristic decision processes for smartphone app selection. Mob. Media Commun. 3 (1), 125–144. https://doi.org/10.1177/2050157914557509.

Federal Trade Commission, 2016, June 24. Mobile Health App Developers: FTC Best Practices. Federal Trade Commission Retrieved from. www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

González, H.M., Vega, W.A., Williams, D.R., Tarraf, W., West, B.T., Neighbors, H.W., 2010. Arch. Gen. Psychiatry 67 (1), 37–46.

Huguet, A., Rao, S., McGrath, P.J., Wozney, L., Wheaton, M., Conrod, J., Rozario, S., 2016. A systematic review of cognitive behavioral therapy and behavioral activation apps for depression. PLoS One 11 (5) Retrieved from. http://search.ebscohost.com.turing.library.northwestern.edu/login.aspx?direct=true&db=psyh&AN=2016-55985-001&site=ehost-live.

IMS Institute for Healthcare Informatics, 2015. Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance. Retrieved from. https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/patient-adoption-of-mhealth.pdf?la=en&hash=B3ACFA8ADDB143F29EAC0C33D533BC5D7AABD689.

Koo, T.K., Li, M.Y., 2016. A guideline of selecting and reporting intraclass correlation coefficients for reliability research. J. Chiropr. Med. 15 (2), 155–163.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C., 2018. Security and privacy analysis of mobile health applications: the alarming state of practice. IEEE Access. 6, 9390–9403.

Powell, A.C., Landman, A.B., Bates, D.W., 2014. In search of a few good apps. JAMA 311 (18), 1851–1852. https://doi.org/10.1001/jama.2014.2564.

Proudfoot, J., Parker, G., Hadzi-Pavlovic, D., 2010. Community attitudes to the appropriation of mobile phones for monitoring and managing depression, anxiety and stress. J. Med. Internet Res. 12, e64.

Research2guidance, 2016. mHealth app development economics 2016: the current status and trends of the mHealth app market. Retrieved from. http://research2guidance.com/r2g/r2g-mHealth-App-Developer-Economics-2016.pdf.

Research2guidance, 2017. Top 3 therapy fields with the best market potential for digital health apps. Retrieved from. https://research2guidance.com/top-3-therapy-fields-with-the-best-market-potential-for-digital-health-apps.

Rosenfeld, L., Torous, J., Vahia, I.V., 2017. Data security and privacy in apps for dementia: an analysis of existing privacy policies. Am. J. Geriatr. Psychiatry 25 (8), 873–877. https://doi.org/10.1016/j.jagp.2017.04.009.

Schueller, S.M., Washburn, J.J., Price, M., 2016. Exploring mental health providers' interest in using web and mobile-based tools in their practices. Internet Interv. 4, 145–151. https://doi.org/10.1016/j.invent.2016.06.004.

Schueller, S.M., Neary, M., O'Loughlin, K., Adkins, E.C., 2018. Discovery of and interest in health apps among those with mental health needs: a survey and focus group study. J. Med. Internet Res. 20.

Shen, N., Levitan, M.-J., Johnson, A., Bender, J.L., Hamilton-Page, M., Jadad, A.R., Wiljer, D., 2015. Finding a depression app: a review and content analysis of the depression app marketplace. JMIR mHealth and uHealth 3 (1), e16. https://doi.org/10.2196/mhealth.3713.

Statista, 2017. Number of apps available in leading app stores as of March 2017. Retrieved from. https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores.

Sunyaev, A., Dehling, T., Taylor, P.L., Mandl, K.D., 2015 Apr. Availability and quality of mobile health app privacy policies. J. Am. Med. Inform. Assoc. 22 (e1), e28–e33.

Torous, J., Roberts, L.W., 2017. Needed innovation in digital health and smartphone applications for mental health transparency and trust. JAMA Psychiatry 74 (5), 437–438. https://doi.org/10.1001/jamapsychiatry.2017.0262.

Torous, J., Friedman, R., Keshavan, M., 2014. Smartphone ownership and interest in mobile applications to monitor symptoms of mental health conditions. JMIR mHealth and uHealth 2 (1), e2. https://doi.org/10.2196/mhealth.2994.

Torous, J., Chan, S., Tan Gipson, S., Kim, J., Nguyen, T., Luo, J., Wang, P., 2018. A hierarchical framework for evaluation and informed decision making regarding smartphone apps for clinical care. Psychiatr. Serv. 69 Retrieved from. https://ps.psychiatryonline.org/doi/pdf/10.1176/appi.ps.201700423.