Internet Interventions 17 (2019) 100243

Contents lists available at ScienceDirect

Internet Interventions

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

Availability, readability, and content of privacy policies and terms of agreements of mental health apps

Julie M. Robillard[a,*], Tanya L. Feng[a], Arlo B. Sporn[a], Jen-Ai Lai[a], Cody Lo[a], Monica Ta[a], Roland Nadler[b]

[a] Division of Neurology, Department of Medicine, The University of British Columbia, B404 - 4480 Oak Street, Vancouver, BC V6H 3N1, Canada
[b] University of Ottawa Centre for Health Law, Policy and Ethics, Common Law Section, Faculty of Law, University of Ottawa, 57 Louis Pasteur (Fauteux Hall), Ottawa, ON K1N 6N5, Canada

ARTICLE INFO

Keywords:
Apps
Mental health
Smartphone
Mobile health
Privacy

ABSTRACT

Objective: To assess the availability, readability, and privacy-related content of the privacy policies and terms of agreement of mental health apps available through popular digital stores.
Materials and methods: Popular smartphone app stores were searched using combinations of keywords "track" and "mood" and their synonyms. The first 100 apps from each search were evaluated for inclusion and exclusion criteria. Apps were assessed for availability of a privacy policy (PP) and terms of agreement (ToA) and if available, these documents were evaluated for both content and readability.
Results: Most of the apps collected in the sample did not include a PP or ToA. PPs could be accessed for 18% of iOS apps and 4% of Android apps; whereas ToAs were available for 15% of iOS and 3% of Android apps. Many PPs stated that users' information may be shared with third parties (71% iOS, 46% Android).
Discussion: Results demonstrate that information collection is occurring with the majority of apps that allow users to track the status of their mental health. Most of the apps collected in the initial sample did not include a PP or ToA despite this being a requirement by the store. The majority of PPs and ToAs that were evaluated are written at a post-secondary reading level and disclose that extensive data collection is occurring.
Conclusion: Our findings raise concerns about consent, transparency, and data sharing associated with mental health apps and highlight the importance of improved regulation in the mobile app environment.

1. Introduction

The majority of North Americans today own a smartphone (Pew Research Center, 2017) and these devices are playing an increasingly influential role in day-to-day activities. As smartphones begin to play a more important role in the health of end-users in the new era of mobile health (mHealth) (The World Health Organization, 2011) a growing number of health apps becoming available. As of 2015, there were over 60,000 health-related apps available in the Google Play and Apple app stores collectively (Xu and Liu, 2015) and over half of mobile phone users had downloaded a health-related app, highlighting the popularity of using smartphones as a health tool (Krebs and Duncan, 2015).

Within the group of health-related apps, a major subcategory is apps aimed at supporting users' mental health: nearly one-third of disease-specific apps have a mental health focus (Anthes, 2016). These apps have been developed to offer support for a variety of mental illnesses, including depression (Ly et al., 2012), anxiety (Lindner et al., 2013), schizophrenia (Ben-Zeev et al., 2014), addiction (McTavish et al., 2012), and eating disorders (Juarascio et al., 2015).

The availability and use of these apps has been linked to major potential benefits. Mobile-based mental health resources may reduce barriers to accessing necessary mental health services, such as cost, distance, wait-times, and the stigma surrounding receiving treatment or support for mental health issues (Bakker et al., 2016; Price et al., 2014). The use of mental health apps may also improve the portability of mental health support for users and allow for novel advantages not available through traditional mental health care, such as real-time monitoring (Donker et al., 2013). Furthermore, these apps help to promote user autonomy by facilitating an increase in self-awareness and self-efficacy skills (Prentice and Dobson, 2014).

However, the use of mental health apps is not without risks. Apps may be vulnerable to technical issues that may disrupt the availability

* Corresponding author at: BC Children's and Women's Hospital, B404 - 4480 Oak Street, Vancouver, BC V6H 3N1, Canada.
E-mail addresses: jrobilla@mail.ubc.ca (J.M. Robillard), tanyafeng@alumni.ubc.ca (T.L. Feng), arlosporn@alumni.ubc.ca (A.B. Sporn), jlai@alumni.ubc.ca (J.-A. Lai), codylo@alumni.ubc.ca (C. Lo), monicata@alumni.ubc.ca (M. Ta), rnadler@uottawa.ca (R. Nadler).

https://doi.org/10.1016/j.invent.2019.100243
Received 2 March 2018; Accepted 18 February 2019
Available online 06 March 2019

of the services (Burns et al., 2011). In addition, the quality of the services varies considerably from app to app, and only a small proportion of publicly available apps have undergone any formal testing (Donker et al., 2013). Many apps offer resources and services that are not evidence-based and may provide inaccurate information that could result in harm to the user (Price et al., 2014). Price et al. (2014) also point out that these apps may discourage users from seeking professional treatment because they believe the app alone can replace other forms of treatment. Finally, the use of these apps often requires the input of sensitive information, including the user's name, contact information, and data regarding their mental health, posing a significant risk to the user's privacy if the data were to be shared, leaked or breached (Jones and Moffitt, 2016; Luxton et al., 2011). Dehling et al. (2015) found among 18,000 health apps available on the Apple and Android App stores, the large majority (96%) were associated with potential security and privacy risks.

The privacy of personal information submitted to the apps is indeed a major concern of app users. For example, one survey showed that 60% of app downloaders have chosen not to install an app because of how much personal information was required to use the app, while 43% uninstalled an app after downloading it for the same reason (Olmstead and Atkinson, 2015). Proudfoot et al. found that participants believed privacy concerns were a key consideration in the design of mental health apps as well as a major reason why some would not be interested in using an app of this sort (Proudfoot et al., 2010).

Despite the increasing popularity health-related apps, there is a lack of empirical research into issues of privacy in the context of apps targeting mental health. Therefore, the purpose of this study was to assess the content and readability the privacy policies (PP) and terms of agreement (ToA) of apps designed to track mental health variables in order to characterize how developers handle users' data.

2. Material and methods

2.1. Sampling

The Apple app store and the Google Play store, the most popular app providers on iOS and Android smartphones respectively, were searched using combinations of keywords “track” and “mood” and their synonyms. To capture search results across a range of devices, the same keyword searches took place on the following mobile phone models: iPhone 5c, iPhone 5 s, iPhone 6, Samsung Note 3, Oneplus One, and Samsung GS6 (see Appendix 1 for the keywords). The first 100 apps that were returned from each search were evaluated for inclusion and exclusion criteria. Inclusion criteria were that the app: 1) is in English; 2) can be downloaded for free; 3) requires the input of personal information (including fingerprints) over time; 4) has a title or description that mentions “mood”, “mental health”, “mental illness”, “depression”, “anxiety” or a synonym of one of those words; and 5) has the general public as its target user group rather than clinicians. Exclusion criteria were that the app: 1) is specific to a mental health condition that is not anxiety or depression; 2) has a primary focus on a condition other than mental health; and 3) only requires the input of personal information at one time point (e.g., no tracking feature). Duplicates were removed. For the apps that met these criteria, we established the availability of PPs and ToAs by searching the app itself and associated online content and, when available, collected their associated PPs and ToAs. In cases where the PPs and ToAs only applied to the developer's website and not the app itself, these were excluded.

2.2. Readability analysis

Grade-level readability of the PPs and ToAs was assessed using an online readability calculator (Readability Calculator [online], n.d.). Consistent with previous studies, readability was reported as an average of scores from the Gunning Fog, Flesh Kincaid, and SMOG formulas (Sunyaev et al., 2015).

2.3. Content analysis

For both PPs and ToAs, a coding guide focused on privacy-related content was developed based on a pilot analysis of a random sample of 10% of the data set. The unit of analysis was defined as each PP or ToA and we employed a rich coding strategy to allow for multiple categorizations of individual documents. The entire sample of PPs and ToAs was coded by one investigator (TF) and a second coder (JL for the PPs, AS for the ToAs) coded 20% of the documents to ensure inter-rater reliability. Reproducibility was originally 94% for PPs and 89% for ToAs and disagreements were settled through discussion until consensus was achieved. The samples were characterized using descriptive statistics.

3. Results

3.1. Sample and readability analysis

The final data set consisted in 319 unique iOS apps (210 free), and 69 unique Android apps (63 free). Of the free Android apps, 20 also appear in the iOS sample, resulting in a total sample of 369 unique apps. For the free iOS apps, 56 PPs (18%) and 47 ToAs (15%) were collected, and 37 apps (12%) had both a PP and ToA. For the free Android apps, 13 (4%) and 12 (3%) were associated with a PP and a ToA, respectively, and 9 (2%) of these apps had both.

The average grade-level readability was 13.78 (13.77 iOS, 13.66 Android) for PPs and 15.24 (15.50 iOS, 13.87 Android) for ToAs.

3.2. Content analysis

3.2.1. Privacy policies

Thirty-nine percent of PPs stated that users' use of the services would be considered implied consent to the PP (38% iOS PPs, 46% Android). The majority (92%) of PPs mentioned some form of information collection (91% iOS, 100% Android). The remaining 8% of PPs explicitly stated that the developer does not collect information (9% iOS, 0% Android). Fig. 1A details the nature of information collected in the apps. Among the total sample of PPs, 29% did not describe the nature of the information collected (28% iOS, 23% Android). Of the specific types of information collected, information about mood or emotions was collected in 13% of the total sample (14% iOS, 15% Android). Users' thoughts or journal entries submitted to the app were collected in 6% of the sample (7% iOS, 8% Android). Fig. 1B summarizes the types of information collected.

One-third (33%) of the sample of PPs included a statement that the developer would not sell users' personal or personally identifiable information without their permission (35% iOS, 31% Android). 5% of PPs (4% iOS, 8% Android) mentioned that the developer may sell aggregate or non-personal information. The most frequently mentioned purposes for collecting information included contacting the user (58%), improving the app (56%), and providing services (44%; see Fig. 2 for full summary)

Over two-thirds (68%) of PPs stated that users' information may be shared with third parties (71% iOS, 46% Android). 10% of PPs (11% iOS, 0% Android) mentioned that users' consent would be obtained before the information was shared. The nature of information shared with the third parties ranged from personally identifiable to aggregated information (Fig. 3A). Service providers were the most frequently specified third party (56%; see Fig. 3B for a summary of the third parties mentioned).

Sixty-one percent of the sample (63% iOS, 69% Android) discussed the disclosure of users' information. This is included for reasons such as complying with legal process (56%), the sale or acquisition of the company (40%), or in the case of a merger (39%; see Fig. 4 for full

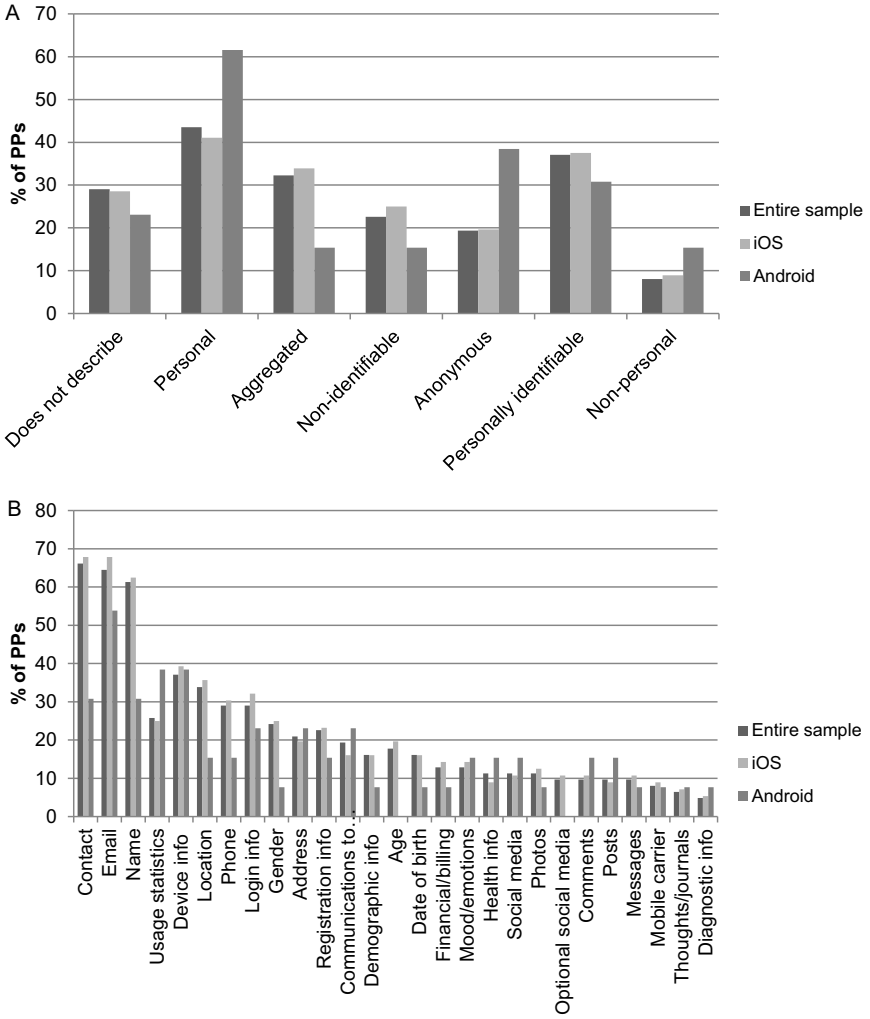

Fig. 1. A) Nature of information described in privacy policies (sample: $n = 62$, iOS: $n = 56$, Android: $n = 13$). B) Types of information described in privacy policies (sample: $n = 62$, iOS: $n = 56$, Android: $n = 13$).

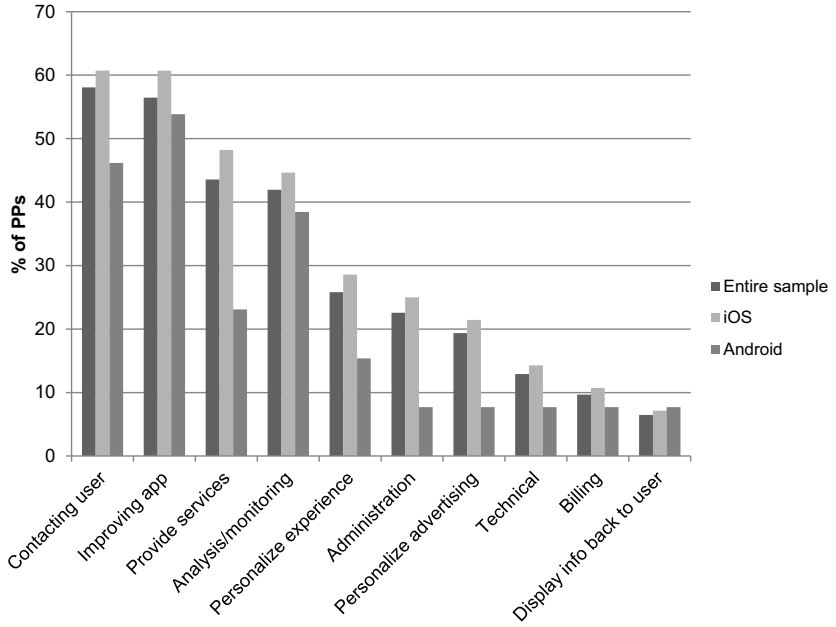

Fig. 2. Uses of information described in privacy policies (sample: $n = 62$, iOS: $n = 56$, Android: $n = 13$).

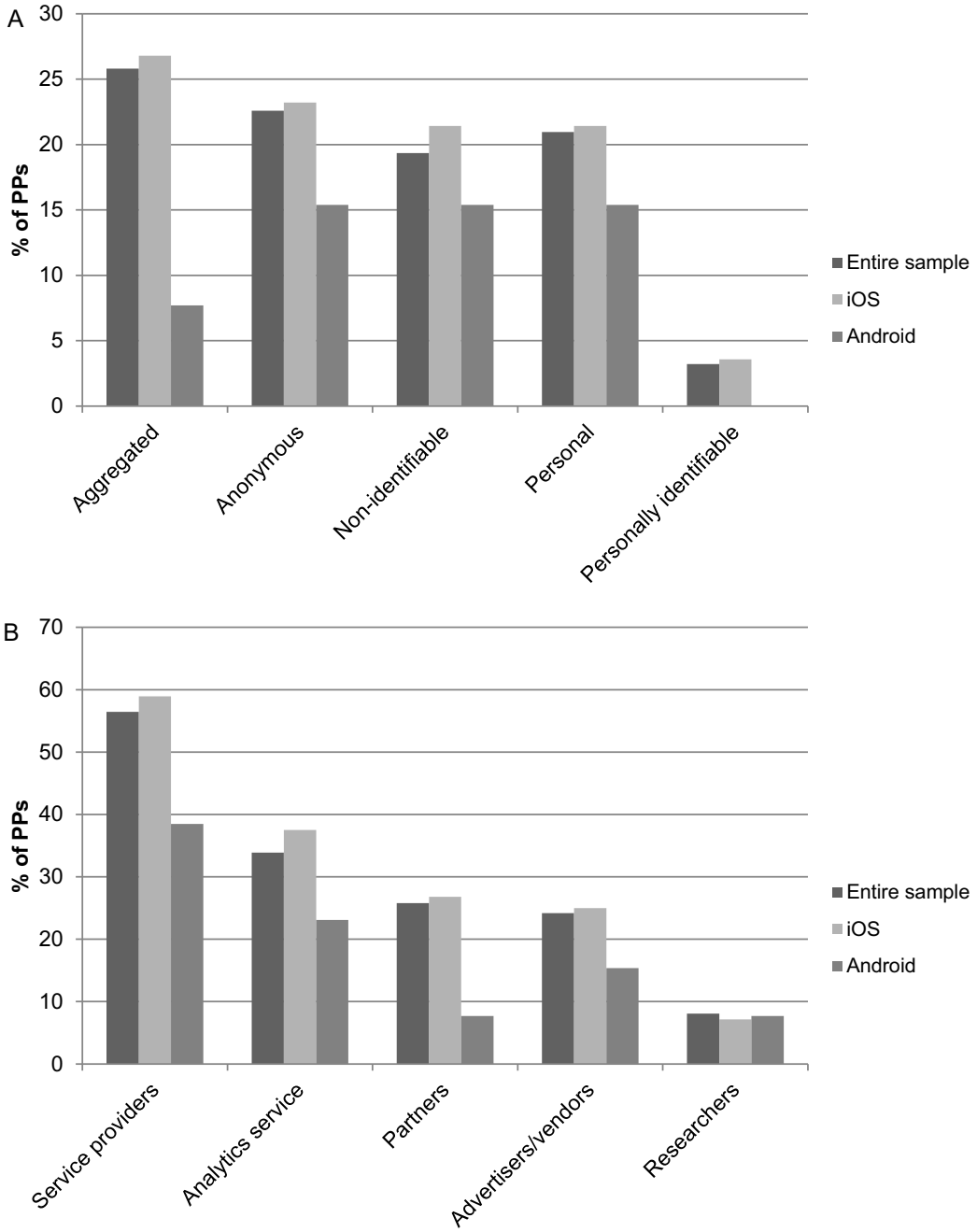

Fig. 3. A) Nature of information shared with third parties described in privacy policies (sample: $n = 62$, iOS: $n = 56$, Android: $n = 13$). B) Types of third parties described in privacy policies (sample: $n = 62$, iOS: $n = 56$, Android: $n = 13$).

summary).

Over half (56%) of PPs mentioned security measures to protect users' information (59% iOS, 31% Android). Thirty-seven percent of the sample (38% iOS, 15% Android) specified that the developer cannot guarantee the security of users' information.

Fifteen percent of the PPs stated that users' could opt-out of having their information collected by the developer (16% iOS, 8% Android). Sixteen percent of PPs (18% iOS, 15% Android) stated that the user can have their collected information deleted. Another 25% (25% iOS, 23% Android) mentioned that the user may be able to have their information deleted but with caveats.

3.2.2. Terms of agreement

Two-thirds (66%) of the ToAs stated that users' use of the app constituted their consent to the ToA (72% iOS, 50% Android). Forty-one (41%) of ToAs (49% iOS, 25% Android) describe a license granted to the developer for regarding the user content on the app (Fig. 5A, B). Sixty-six percent of the sample (72% iOS, 58% Android) specified the federal, state, or provincial laws governing the agreement.

4. Discussion

These findings demonstrate that extensive information collection is occurring with the majority of apps available on the Apple and Google Play stores that allow users to track the status of their mental health. Most of the apps collected in the initial sample did not include a PP or ToA, despite the fact that Apple requires that any apps that collect user or usage data include a PP and Google requires developers to link to their PP on the app's store listing page for apps that "request access to sensitive permissions or data" (Apple, n.d.; Google, n.d.). In this present

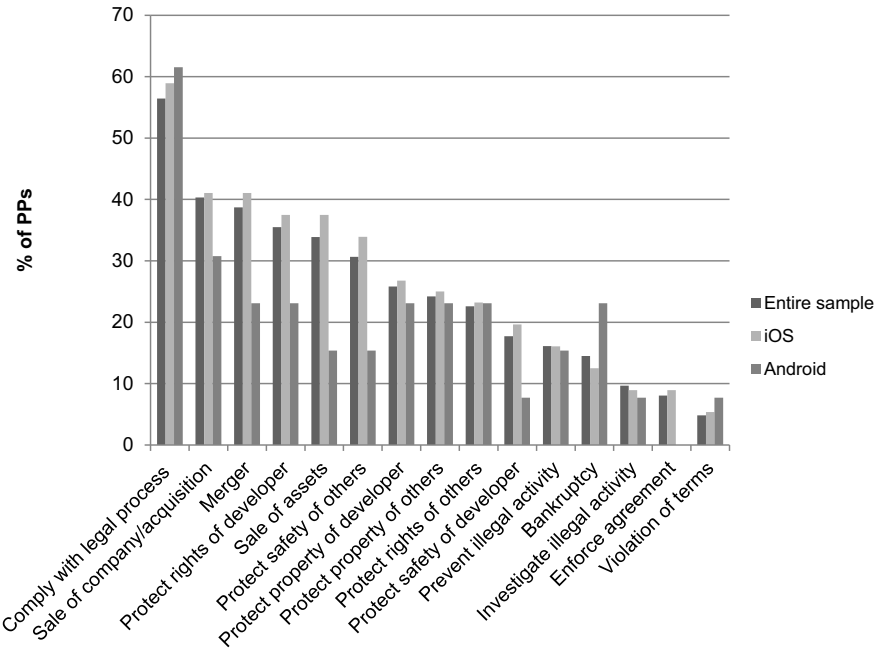

Fig. 4. Reasons for disclosing information described in privacy policies (sample: $n = 62$, iOS: $n = 56$, Android: $n = 13$).

study, a larger proportion of apps found on the Apple store included a ToA or PP compared with those found on the Google store. Jones and Moffitt point out that Apple has stricter guidelines regulating app development than does Google, which may explain this discrepancy (Jones and Moffitt, 2016). The proportion of apps in our sample that were associated with PPs is lower than a previous assessment of mobile health apps, as Sunyaev et al. (2015) found that 31% of the apps in their sample had a PP.

Many PPs and ToAs included statements that users' continued use of the app would constitute their implied consent to these agreements. This is far from the ideal of informed consent used in health care settings (Jones and Moffitt, 2016). As with conventional mental health treatment, it is crucial that users are able to understand the risks and benefits of the app (Prentice and Dobson, 2014), including potential harms to their privacy. However, it may be difficult for users to fully understand these legal documents, as most PPs and ToAs are written at a post-secondary reading level. Previous research also indicates that the average reading grade level of the PPs of health apps far exceeds the reading level of a typical user (Sunyaev et al., 2015). Ploug and Holm describe the “routinisation of informed consent” that occurs when providing consent because a habitual act, which may often be due to users perceiving the conditions and policies of a technology as being too much to read or taking too much time to read (Ploug and Holm, 2013). Simply because a user clicks an “I agree” button, this provides little evidence of the users' competence (Prentice and Dobson, 2014), notwithstanding the legal fiction that ensures these agreements will hold up as valid contractual arrangements.

The content of the PPs and ToAs studied here raises concern regarding the privacy of users' information, including sensitive data pertaining to their mental health. The majority of PPs permitted third party sharing, while ToAs often granted developers broad licenses for the handling of user content. Only one-third of PPs stated that users' personal or personally identifiable information would not be sold without their consent, while small numbers of PPs even indicated that users' non-personal or aggregate information may be sold. The issue of selling users' information was not mentioned in the majority of these documents, highlighting the lack of transparency of these apps. Furthermore, significant proportions of PPs mentioned that users' information may be disclosed during the sale or acquisition of the company, the sale of its assets, or in the case of a merger – hardly a remote possibility in an app economy where acquisition by a larger, more established entity is synonymous with success. App consumers who wish to avoid prominent technology companies they view as untrustworthy may not realize how easily their data could end up in unanticipated hands. This is not a unique case highlighting concerns over the transparency of health apps, as Huckvale et al. (2015) found that a majority of apps in their sample collected or transmitted data that was not discussed in the PP and that some handled information inconsistently with what was described in the PP.

While one quarter of PPs mentioned security measures in place to protect users' data, the majority of these apps stated that they cannot guarantee the security of users' data. Some PPs stated that users can have their information associated with the app deleted; however, in many cases, there were caveats mentioned. A study conducted in Germany which included apps from around the world found that email requests to app vendors to have information deleted were only fulfilled in just over half of the cases (Herrmann and Lindemann, 2016).

Absent, incomplete or overly dense privacy policies can have negative consequences for the end-users of mental health apps. This can range from less serious situations such as targeted advertising within the app to major privacy breaches (Haddadi et al., 2011), during which users' sensitive mental health information may be shared with others, including friends and family, potential employers, and insurance companies, which may result in severe social and financial downstream ramifications (Dehling et al., 2015).

Concerns have been raised over the absence of laws governing mental health apps, both at the federal level and internationally. Specifically, these regulations may be out of date, based on older technologies, and may not be specific to mobile health apps (Martínez-Pérez et al., 2014). For example, in the United States, a 2016 report released by the United States Department of Health and Human Services emphasizes that laws in place to protect traditional health information, such as the Health Insurance and Portability and Accountability Act of 1996, do not apply to health information submitted on mobile apps (U.S. Department of Health and Human Services, 2016). The report highlights that, “large gaps in policies around access, security, and privacy continue, and…confusion persists among both consumers and innovators.” This emphasizes that the absence of PPs

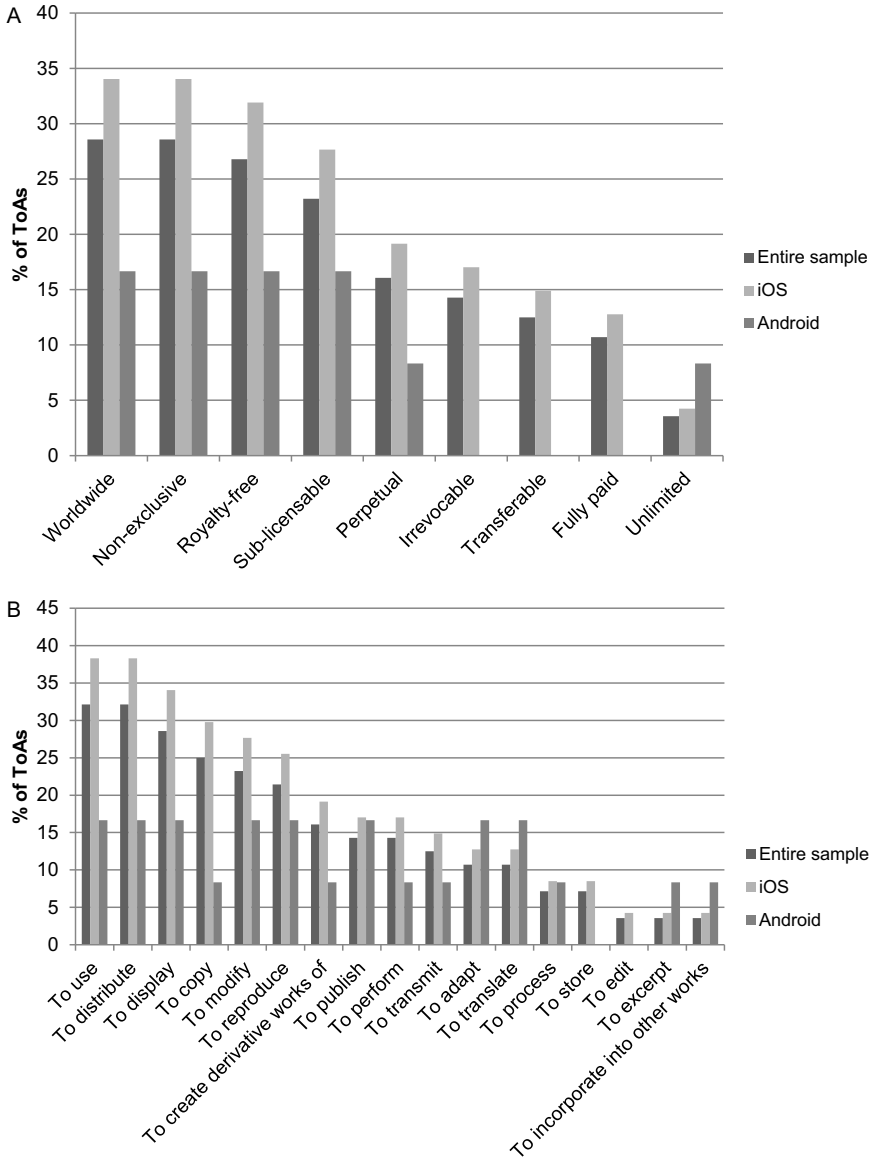

Fig. 5. A) Description of license granted to developer described in terms of agreements (sample: $n = 56$, iOS: $n = 47$, Android: $n = 12$). B) License privileges granted to developer described in terms of agreements (sample: $n = 56$, iOS: $n = 47$, Android: $n = 12$).

and ToAs for mental health apps may not be solely indicative of negligence or intentional lack of transparency; rather, not all developers may have the legal knowledge to create effective legal documents for their apps. Indeed, findings from surveys and interviews with app developers demonstrate that developers themselves find PPs difficult to read (Balebako and Cranor, 2014). Furthermore, working in a competitive and dynamic industry with limited resources, developers do not always consider privacy as a priority.

We appreciate the limitations of this present study. While we analyzed both the PPs and ToAs of the apps, findings were only discussed in the document category they were more frequently mentioned in to avoid redundancy. For example, while disclosure of information was mentioned in both the PP and ToA sample, we reported mentions of disclosure in the context of PPs as it was discussed far more often in PPs than ToAs. In addition, while there were some apps that included both a PP and ToA, we did not consolidate the information in these documents for the app. Therefore, it is possible that information not captured in the app's PP may be found in the ToA and vice versa.

5. Conclusion

Despite these limitations, our findings demonstrate a general lack of transparency regarding the handling of users' sensitive information submitted to mental health apps, and, in cases of greater transparency, raise concern over developers' use of this information. Many groups have proposed various solutions to this issue. For example, a collaborative effort between the RAND Corporation and the Massachusetts Institute of Technology has resulted in the creation of the DL-FIPPs Tool to assist policymakers in identifying weaknesses and strengths in current and future policies (Yerukhimovich et al., 2016). In addition, others have recommended prompting developers to write privacy notices, such as through policy and regulation (Balebako and Cranor, 2014). Schaub and colleagues also recommend employing a user-centered or participatory design process for the creation of privacy notices in order to ensure the effectiveness of these documents (Schaub et al., 2015). Awareness should also be raised among end-users of the privacy issues surrounding mental health apps. Users can be empowered to choose the apps they use carefully, such as looking for the presence of a PP and ToA and reading these documents in full before submitting any

personal information. Furthermore, efforts have been made to create certification standards for health apps to make it easier for users to select credible apps (Boulos et al., 2014), such as the National Health Service Health Apps Library (National Health Service, n.d.). Moving forward, key action items will include the introduction of new governmental regulation, greater transparency norms, and increased awareness among users and developers alike to create a safer online environment for users' mental health information.

Acknowledgements

None.

Funding

This research was supported by the Canadian Consortium on Neurodegeneration in Aging, the Canadian Institutes of Health Research, the British Columbia Knowledge Development Fund, the Canada Foundation for Innovation, the BC Children's Hospital Foundation and the Vancouver Coastal Health Research Institute. The funding bodies had no role in the design of the study and collection, analysis, and interpretation of data and in writing the manuscript.

Declarations of interest

None.

Appendix 1

	Track	Measure	Monitor	Test	Scale	Check	Diagnose	Trace	Log	Diary	Journal	Record
Mood	Mood track	Mood measure	Mood monitor	Mood test	Mood scale	Mood check	Mood diagnose	Mood trace	Mood log	Mood diary	Mood journal	Mood record
Anxiety	Anxiety track	Anxiety measure	Anxiety monitor	Anxiety test	Anxiety scale	Anxiety check	Anxiety diagnose	Anxiety trace	Anxiety log	Anxiety diary	Anxiety journal	Anxiety record
Depression	Depression track	Depression measure	Depression monitor	Depression test	Depression scale	Depression check	Depression diagnose	Depression trace	Depression log	Depression diary	Depression journal	Depression record
Mental	Mental track	Mental measure	Mental monitor	Mental test	Mental scale	Mental check	Mental diagnose	Mental trace	Mental log	Mental diary	Mental journal	Mental record
Emotion	Emotion track	Emotion measure	Emotion monitor	Emotion test	Emotion scale	Emotion check	Emotion diagnose	Emotion trace	Emotion log	Emotion diary	Emotion journal	Emotion record
Feeling	Feeling track	Feeling measure	Feeling monitor	Feeling test	Feeling scale	Feeling check	Feeling diagnose	Feeling trace	Feeling log	Feeling diary	Feeling journal	Feeling record
Stress	Stress track	Stress measure	Stress monitor	Stress test	Stress scale	Stress check	Stress diagnose	Stress trace	Stress log	Stress diary	Stress journal	Stress record
SAD	SAD track	SAD measure	SAD monitor	SAD test	SAD scale	SAD check	SAD diagnose	Sad trace	SAD log	SAD diary	SAD journal	SAD record
Melancholy	Melancholy track	Melancholy measure	Melancholy monitor	Melancholy test	Melancholy scale	Melancholy check	Melancholy diagnose	Melancholy trace	Melancholy log	Melancholy diary	Melancholy journal	Melancholy record
Worry	Worry track	Worry measure	Worry monitor	Worry test	Worry scale	Worry check	Worry diagnose	Worry trace	Worry log	Worry diary	Worry journal	Worry record
Panic	Panic track	Panic measure	Panic monitor	Panic test	Panic scale	Panic check	Panic diagnose	Panic trace	Panic log	Panic diary	Panic journal	Panic record
Nervous	Nervous track	Nervous measure	Nervous monitor	Nervous test	Nervous scale	Nervous check	Nervous diagnose	Nervous trace	Nervous log	Nervous diary	Nervous journal	Nervous record
Distress	Distress track	Distress measure	Distress monitor	Distress test	Distress scale	Distress check	Distress diagnose	Distress trace	Distress log	Distress diary	Distress journal	Distress record

References

Anthes, E., 2016. Mental health: there's an app for that. Nature 532 (7597), 20–23.
Apple, n.d. App Store review guidelines [online]. URL https://developer.apple.com/app-store/review/guidelines/ (date accessed 7.25.17).
Bakker, D., Kazantzis, N., Rickwood, D., et al., 2016. Mental health smartphone apps: review and evidence-based recommendations for future developments. JMIR Mental Health 3 (1).
Balebako, R., Cranor, L., 2014. Improving app privacy: nudging app developers to protect user privacy. IEEE Secur. Priv. 12, 55–58.
Ben-Zeev, D., Brenner, C.J., Begale, M., et al., 2014. Feasibility, acceptability, and preliminary efficacy of a smartphone intervention for schizophrenia. Schizophr. Bull. 40, 1244–1253.
Boulos, M.N.K., Brewer, A.C., Karimkhani, C., et al., 2014. Mobile medical and health apps: state of the art, concerns, regulatory control and certification. Online J. Public Health Inform. 5, 229.
Burns, M.N., Begale, M., Duffecy, J., et al., 2011. Harnessing context sensing to develop a mobile intervention for depression. J. Med. Internet Res. 13, e55.
Dehling, T., Gao, F., Schneider, S., et al., 2015. Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. JMIR MHealth UHealth 3, e8.
Donker, T., Petrie, K., Proudfoot, J., et al., 2013. Smartphones for smarter delivery of mental health programs: a systematic review. J. Med. Internet Res. 15, e247.
Google, n.d. Upload an app [online]. URL https://support.google.com/googleplay/android-developer/answer/113469#privacy (date accessed 7.25.17).
Haddadi, H., Hui, P., Henderson, T., et al., 2011. Targeted advertising on the handset: privacy and security challenges. In: Pervasive Advertising, Human-Computer Interaction Series. Springer, London, pp. 119–137.
Herrmann, D., Lindemann, J., 2016. Obtaining personal data and asking for erasure: do app vendors and website owners honour your privacy rights? ArXiv16020. 1804.
Huckvale, K., Prieto, J.T., Tilney, M., et al., 2015. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med. 13, 214.
Jones, N., Moffitt, M., 2016. Ethical guidelines for mobile app development within health and mental health fields. Prof. Psychol. Res. Pract. 47, 155–162.
Juarascio, A.S., Manasse, S.M., Goldstein, S.P., et al., 2015. Review of smartphone applications for the treatment of eating disorders. Eur. Eat. Disord. Rev. 23, 1–11.
Krebs, P., Duncan, D.T., 2015. Health app use among US mobile phone owners: a national survey. JMIR MHealth UHealth 3.
Lindner, P., Ivanova, E., Ly, K.H., et al., 2013. Guided and unguided CBT for social anxiety disorder and/or panic disorder via the internet and a smartphone application: study protocol for a randomised controlled trial. Trials 14, 437.
Luxton, D.D., McCann, R.A., Bush, N.E., et al., 2011. mHealth for mental health: integrating smartphone technology in behavioral healthcare. Prof. Psychol. Res. Pract., Telehealth and Technology Innovations in Professional Psychology 42, 505–512.
Ly, K.H., Carlbring, P., Andersson, G., 2012. Behavioral activation-based guided self-help treatment administered through a smartphone application: study protocol for a randomized controlled trial. Trials 13, 62.
Martínez-Pérez, B., de la Torre-Díez, I., López-Coronado, M., 2014. Privacy and security in mobile health apps: a review and recommendations. J. Med. Syst. 39, 1–8.
McTavish, F.M., Ming-Yuan, C., Shah, D., et al., 2012. How patients recovering from alcoholism use a smartphone intervention. J. Dual Diagn. 8, 294–304.
National Health Service, n.d. Digital Apps Library [online]. URL https://apps.beta.nhs.

uk/ (date accessed 8.11.17).
Olmstead K, Atkinson M, 2015. Chapter 1: the majority of smartphone owners download apps [online]. Pew Res. Cent. Internet Sci. Tech. URL http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/ (date accessed 3.23.17).
Pew Research Center, 2017. Mobile fact sheet [online]. URL Pew Res. Cent. Internet Sci. Tech.http://www.pewinternet.org/fact-sheet/mobile/, Accessed date: 23 March 2017.
Ploug, T., Holm, S., 2013. Informed consent and routinisation. J. Med. Ethics 39, 214–218.
Prentice, J.L., Dobson, K.S., 2014. A review of the risks and benefits associated with mobile phone applications for psychological interventions. Can. Psychol. 55, 282–290.
Price, M., Yuen, E.K., Goetter, E.M., et al., 2014. mHealth: a mechanism to deliver more accessible, more effective mental health care. Clin. Psychol. Psychother. 21, 427–436.
Proudfoot, J., Parker, G., Hadzi Pavlovic, D., et al., 2010. Community attitudes to the appropriation of mobile phones for monitoring and managing depression, anxiety, and stress. J. Med. Internet Res. 12, e64.
Readability Calculator [online], n.d. Online Util. URL https://www.online-utility.org/english/readability_test_and_improve.jsp (date accessed 9.8.17).
Schaub, F., Balebako, R., Durity, A., et al., 2015. A design space for effective privacy notices. Eleventh Symposium On Usable Privacy and Security 1–17.
Sunyaev, A., Dehling, T., Taylor, P.L., et al., 2015. Availability and quality of mobile health app privacy policies. J. Am. Med. Inform. Assoc. 22, 28–33.
The World Health Organization. mHealth: New Horizons for Health Through Mobile Technologies, Global Observatory for eHealth Series. 2011.
U.S. Department of Health and Human Services, 2016. Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA.
Xu, W., Liu, Y., 2015. mHealthApps: a repository and database of mobile health apps. JMIR MHealth UHealth 3, e28.
Yerukhimovich, A., Balebako, R., Boustead, A., et al., 2016. Can Smartphones And Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices (No. RR-1393-DARPA). Massachusetts Institute of Technology. In: RAND Corporation.