International Journal of Law and Psychiatry 64 (2019) 198–204

Contents lists available at ScienceDirect

International Journal of Law and Psychiatry

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

How private is your mental health app data? An empirical study of mental health app privacy policies and practices

Lisa Parker[a,*], Vanessa Halter[b,1], Tanya Karliychuk[c], Quinn Grundy[a,2]

[a] The University of Sydney, School of Pharmacy, Charles Perkins Centre, D17, Level 6 The Hub, NSW 2006, Australia
[b] Australian Digital Health Agency, Level 25, 56 Pitt Street, Sydney, NSW 2000, Australia
[c] Australian Communications Consumer Action Network (ACCAN), PO Box 639, Broadway, NSW 2007, Australia

ARTICLE INFO

Keywords:
Mobile health
mHealth
Privacy
Qualitative research
Mental health

ABSTRACT

Digital mental health services are increasingly endorsed by governments and health professionals as a low cost, accessible alternative or adjunct to face-to-face therapy. App users may suffer loss of personal privacy due to security breaches or common data sharing practices between app developers and third parties. Loss of privacy around personal health data may harm an individual's reputation or health. The purpose of this project was to identify salient consumer issues related to privacy in the mental health app market and to inform advocacy efforts towards promoting consumer interests. We conducted a critical content analysis of promotional (advertising) materials for prominent mental health apps in selected dominant English-speaking markets in late 2016-early 2017, updated in 2018. We identified 61 prominent mental health apps, 56 of which were still available in 2018. Apps frequently requested permission to access elements of the user's mobile device, including requesting so-called 'dangerous' permissions. Many apps encouraged users to share their own data with an online community. Nearly half of the apps (25/61, 41%) did not have a privacy policy to inform users about how and when personal information would be collected and retained or shared with third parties, despite this being a standard recommendation of privacy regulations. We consider that the app industry pays insufficient attention to protecting the privacy of mental health app users. We advocate for increased monitoring and enforcement of privacy principles and practices in mental health apps and the mobile ecosystem, more broadly. We also suggest a re-framing of regulatory attention that places consumer interests at the centre of guidance.

1. Introduction

Digital mental health services are increasingly endorsed by governments and health professionals as a low cost, accessible alternative or adjunct to face-to-face therapy (Australian Government, 2015; Christensen & Petrie, 2013; Donker et al., 2013; Hollis et al., 2015; World Health Organization (WHO), 2013). These digital services include the integration or endorsement of mobile applications (apps) for promotion, prevention, and self-management of mental health conditions. The Australian Department of Health, for example, has recently launched its new Head to Health program, which provides links to apps and online programs to help people with mental health conditions (Department of Health, 2017). Similarly, the United Kingdom's National Health Service has released a beta list of mental health apps as resources for addressing mental health difficulties and seeking a meaningful life (NHS, 2018).

At the same time, there is growing awareness and concern about potential loss of privacy resulting from the use of health apps. A user's privacy may be breached by malign hacking and poorly secured products (Huckvale, Prieto, Tilney, Benghozi, & Car, 2015). However, app user privacy may also be lost due to commercial data-sharing practices. The collection and sharing of user data is a common (and legal) monetisation strategy for apps (Australian Communications and Media Authority (ACMA), 2013). Health apps commonly share data with multiple third parties for app functionality but also for commercial purposes that may be unrelated to use of the app. For example, the Australian medical appointment booking app, HealthEngine, was recently found to be routinely sharing users' health information with law firms to assist them with identifying potential clients for personal injury claims (McGrath, Blumer, & Carter, 2018). Other purposes of data

Abbreviations: Apps, mobile applications; GDPR, General Data Protection Regulation (European Union)

* Corresponding author.
E-mail addresses: lisa.parker@sydney.edu.au (L. Parker), tanya.karliychuk@accan.org.au (T. Karliychuk), quinn.grundy@utoronto.ca (Q. Grundy).
[1] Present address: Healthdirect Australia, Level 7, 222 Pitt Street, Sydney, NSW, 2000, Australia.
[2] Present address: Faculty of Nursing, University of Toronto, Suite 130, 155 College St, Toronto, ON M5T 1P8, Canada.

https://doi.org/10.1016/j.ijlp.2019.04.002
Received 28 November 2018; Accepted 2 April 2019
Available online 28 April 2019
0160-2527/

sharing include delivering targeted advertising and commercialising aggregated individual or population profiles (Pasquale, 2015; Razaghpanah et al., 2018). There is little transparency about exactly what data is being shared, with whom and for what purposes (Razaghpanah et al., 2018). The available information about data sharing may be shrouded in verbose legalistic or technical terminology, making it difficult for the average consumer to be properly informed before deciding to use an app.

Loss of privacy for app users can have significant consequences for the individual and the public. Developers may share users' data with third parties that provide services to the developer, such as advertising, analytics or customer service support (Razaghpanah et al., 2018). While user data is generally provided to third parties in a de-identified format, (e.g. linked to an Android ID rather than a user's name), app user data can be cross-linked with data from other sources (e.g. social media, public records) such that users are easily re-identifiable. Third parties may draw on this data to deliver targeted advertising to an individual, both within an app and across platforms, such as to a person's geographic place of residence or social media accounts (Ebeling, 2011). Less obvious but arguably more serious consequences may arise when third parties aggregate many people's consumer data from apps and other digital sources for insights into societal patterns and behaviours (Binns et al., 2018; Watkin, 2018). For example, aggregated data may be commercialised by third parties in the form of proprietary algorithms which they claim can be used to predict future behaviour and risk in relation to specific individuals (Pasquale, 2015, p 216). A third party may insert individualised data into their employment algorithm to generate an “employability score” for that individual, which can be bought and used by employers in a preliminary assessment of job applicants. They may also offer “credit ratings” and “rental scores” for use by banks and landlords respectively. Health data, which is classed by privacy regulators as particularly sensitive, may be very influential within such algorithms: even having a mental health app on one's phone could be used to make inferences about an individual's suitability for employment or promotion, for example. Aggregated data sets may also impact society, as in, for example, recent claims that data mining from social media was used to predict and manipulate voting preferences (Watkin, 2018).

Loss of privacy may also have health implications for individuals. An unmediated forum for sharing ideas about mental health and illness may be harmful, especially to those with a serious mental illness (Perry, Werner-Seidler, Calear, & Christensen, 2016) More broadly, concerns about privacy breaches may deter consumers from using mental health apps, meaning that this promising health service fails to reach its potential (Dehling, Gao, Schneider, & Sunyaev, 2015).

1.1. Aims and objectives

The purpose of this project was to identify salient consumer issues related to privacy in the mental health app market and to inform advocacy efforts towards promoting the safety and quality of mental health apps through a partnership with an Australian consumer advocacy organisation. This paper reports on the key finding that apps lacked transparency about the collection, retention, sharing and use of consumers' personal data, while simultaneously promoting to users the value of sharing one's data with an online community.

2. Materials and methods

We conducted a critical analysis of privacy-related information contained within the promotional (advertising) materials of prominent mental health apps available in a selection of major English-speaking markets. These materials included app store listings and linked websites. We defined health apps as software that was intended to be downloaded onto a smartphone, tablet, or other mobile platform, and run with or without internet (Torous & Powell, 2015). We used the term mental health apps to mean apps that focused on one or more of mental health symptoms, behaviours, diagnoses, monitoring and treatment, including mental wellness (Christensen & Petrie, 2013).

2.1. Sampling

We searched for prominent and widely promoted mental health apps in Australia and other major app markets in the English-speaking world (USA, Canada, UK). We used two sampling strategies: an app store crawling program and purposive sampling from the websites of high-profile organisations, and have published the details previously (Parker et al., 2018). In summary, we included: top-ranked Health and Fitness and Medical apps within Google Play and iTunes app stores between 18 August – 9 September 2016; and apps endorsed by Australian government entities, peak mental health bodies and selected media outlets.

Our inclusion criteria were that apps must be:

- designed for a mobile platform;
- available in Australia, USA, Canada or the UK;
- in English;
- pertaining to mental health and wellness symptoms (e.g. suicidal ideation), behaviour (e.g. meditation, mindfulness) or diagnosis (e.g. depression); AND
- providing at least one of: a diagnosis, guidance, recommendation (e.g. following a specific program; general lifestyle advice was not sufficient) *OR* monitoring/tracking of user-generated data *OR* a mental health claim.

We performed initial data collection between October 2016 and February 2017 (hereafter referred to as ‘2017’). We extracted data within app promotional materials using a tool developed with a privacy lawyer (VH) and a consumer advocate (TK) that related to the app developers' self-reported data collection and sharing practices in the form of developer “permissions”, privacy policies, and promotional messages on data sharing. Two researchers extracted the data independently and we discussed and resolved any discrepancies within team meetings. In September–October 2018, after requirements of the new European Union General Data Protection Regulation (GDPR) came into effect (Office of the Australian Information Commissioner (OAIC), 2018), we re-collected data related to app availability, developer “permissions”, and privacy policies in order to assess the policy impact on the sample and analyses.

We evaluated our findings against national and international policies relevant to health app privacy, with particular attention to local guidance as set out in the Australian Privacy Principles (Office of the Australian Information Commissioner (OAIC), 2014a, 2014b, 2018).

3. Results

We identified 61 prominent mental health apps; 56 (92%) were still available in 2018 (see Appendix 1). Most of the apps were available in both Google Play and iTunes (45/61, 74%; 40/56, 71%, in 2018) with slightly more available for iOS in iTunes (55/61, 90%; 50/56, 89% in 2018) than for the Android platform in Google Play (51/61, 84%; 46/56, 82% in 2018). We identified 45 unique developer companies behind the 61 apps (41 behind the 56 apps still available in 2018), half of which were based in North America (23/45, 51%). Others were based in Europe (9/45, 20%) and Australia or New Zealand (13/45, 29%). Most developers were commercial (34/45, 76%) with the remainder being not-for-profit, including university and government departments. The most common mental health issue mentioned in the app promotional materials was anxiety, including panic or stress (34/61, 56%), followed by depression and mood disorders (16/61, 26%). Apps offered a limited range of tools in pursuit of their promised mental health outcomes. Many apps (24/61, 39%) provided relaxation facilitators

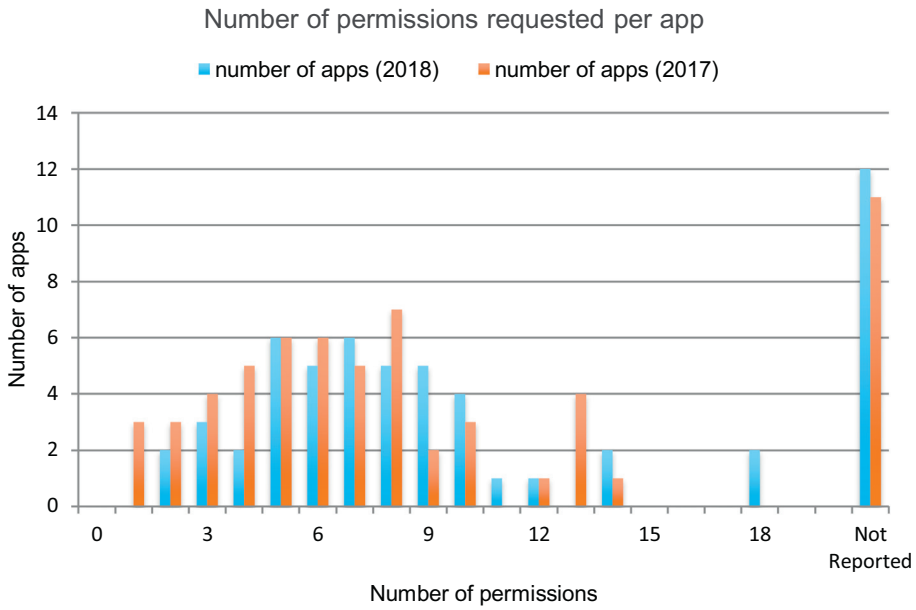

Fig. 1. Total permissions requested (n = 61 in 2017; 56 in 2018).

(e.g. guided recordings or breathing exercises) while others offered variations of cognitive-behaviour therapy exercises (24/61, 39%) or provided track, share and compare services (13/61, 21%).

3.1. Privacy practices: app requests for data collection ('permissions')

Apps available in the Google Play app store allow developers to self-report their data collection practices in the promotional material for prospective app users in the form of "permissions." Developers of apps in the iTunes store do not provide this information. From the 51 apps available in Google Play, 50 (98%) reported permissions data (44/46, 96% in 2018). In 2017, these 50 apps requested an average of 6.4 different permissions (range 1 to 14. The 44 apps available in 2018 requested an average of 7.6 permissions (range 2–18 (see Fig. 1).

Google differentiates between what it calls 'normal' permissions and 'dangerous' permissions', describing the latter as those which pose higher risk. Google's 'dangerous permissions' include, for example, permissions that enable the app to access a user's private information, alter a user's stored data or interfere with operation of other apps (Google Play, 2018). In 2017, apps requested an average of two 'dangerous' permissions (range 0–7). The two most common 'dangerous' permissions, both requested in 73% (37/51) of Google Play apps, were to read, and to modify or delete, the device's USB storage. These permissions are required in order to save any data to the device, and enable developers to read and modify/delete all stored files on the device, including files containing personal information such as photos, contacts and text messages (see Fig. 2). In 2018, these were also the most common 'dangerous' permissions requested, with 31/46 (67%) and 30/46 (65%) apps available in the Google Play store requesting to read and modify/delete USB storage, respectively. Some apps requested permissions which were seemingly unrelated to the app's main purpose as communicated to users. For example, Happify, an app providing "guided relaxation/meditation" audios and "science-based activities & games" requested 18 permissions, including permissions for access to users' text messages and contacts list.

3.2. Privacy practices: promoting the value of sharing

Apps encouraged user interaction and data sharing in their promotional materials. For example, MoodKit – Mood Improvement Tools by Thriveport, LLC, listed links to social media platforms, stating "Email, text, & Facebook sharing of activities," as one of the highlights for app users and OMG! I Can Meditate by OMG! I Can Meditate Inc. endorsed user participation and data sharing in app-based virtual communities it called "serenity circles." Anorexia / Bulimia / Binge Eating Test by PocketShrink urged users to disclose personal information, exhorting them to "share your profile." Another app prompted user sharing by explicitly portraying its forums as emotionally safer spaces compared to traditional social media, telling users they could "talk with people that may be feeling just like you from all around the planet, without worrying about the like/dislike system" [What's Up, by Jackson Tempra].

3.3. Privacy policies

Privacy policies were specific to developers. As noted above, some of the apps in our sample were owned by the same developer 'family' (in 2017 there were 61 apps from 45 unique developers; in 2018 there were 56 apps from 41 developers). Apps in the same developer 'family' shared the same privacy policy or lack of privacy policy. Since we used a consumer facing perspective, we used the app as our unit of analysis when reporting quantitative results.

The Australian Government specifies minimum standards for privacy policies that are pertinent to mobile apps (Office of the Australian Information Commissioner (OAIC), 2014a). These relate to matters such as policy accessibility and readability; provision of information on data collection, use, sharing and security; and details about how and where to complain about privacy practices. During our 2017 data collection period, nearly half of the apps (25/61, 41%) did not have a privacy policy. None of the five apps published or endorsed by a total of three different government entities provided privacy policies (U.S. Department of Defense, Australian Department of Veterans' Affairs and a government-funded health provider). In 2018, 12/56 apps (21%), and one of the five government apps still did not have a privacy policy. In both data sampling periods, only one app's privacy policy met all of the requirements of the Australian Privacy Principles (RR Eating Disorder Management by Recovery Record). In 2017, the majority of apps with a privacy policy met only 6/10 criteria; in 2018, this rose to the majority meeting 7/10 criteria (see Fig. 3).

3.3.1. Policy accessibility and readability

Policies were difficult to read and understand. They were, on

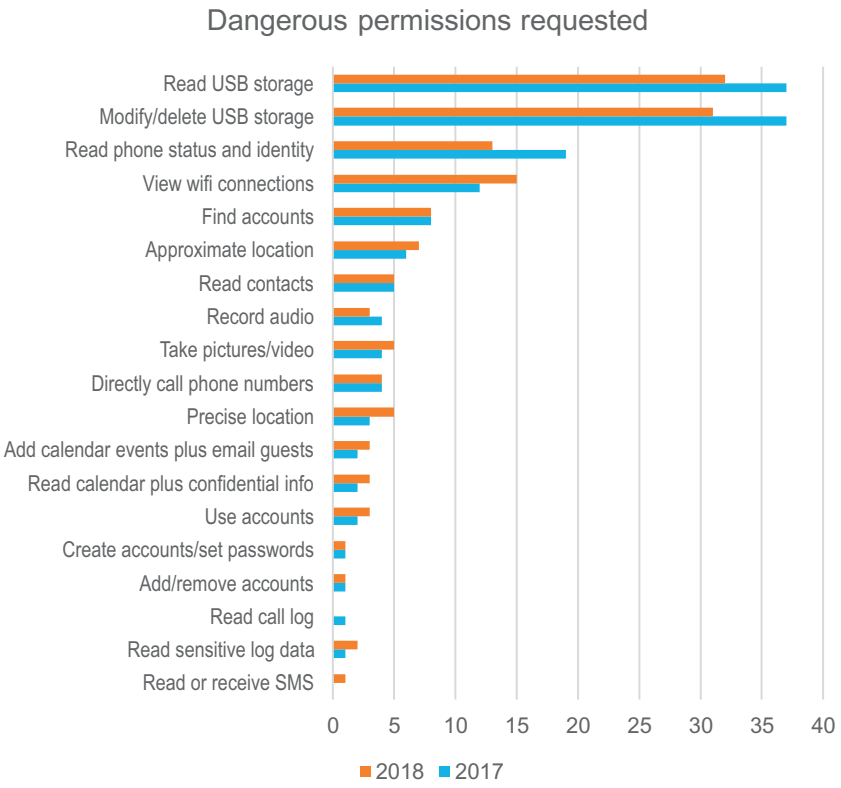

Fig. 2. Dangerous permissions requested (n = 61 in 2017; 56 in 2018).

average, about 2000 words long (2017 mean = 1760 words, SD 1206 words; 2018 mean = 2179 words, SD 1635 words). In 2017, policies ranged from just seven words (e.g. "No data from this application is collected") to over 5000 words; the minimum increased to 21 words in 2018. Few of the privacy policies had features that would facilitate user engagement: for example, in 2017, only three (3/36, 8%) contained a summary with key points, and only four (4/36, 11%) were judged to use lay language, though this increased to 10/44 (23%) and 9/44 (21%), respectively, in 2018. The link to the privacy policy was hard to find in over ¼ of sampled apps with a privacy policy in 2017 (10/36, 27%) and still hard for 11/44, 25% in 2018. Similarly, less than 3/4 used headings to facilitate navigation through the policy in 2017 (25/36, 69%), though this increased to 88% (39/44) in 2018.

3.3.2. Policy information on data collection, use and sharing

Most apps in 2017 (32/36, 89%) and 2018 (39/44, 89%) had policies that mentioned the type of data that was collected and why (Fig. 3). Most also said that data was disclosed to third parties (28/36, 78% in 2017; 39/44, 89% in 2018), and at least half (19/36, 53% in 2017; 22/44, 50% in 2018) mentioned the purposes for which these parties might use data, including, for example, "data processing, data analysis, information technology services and support, fundraising, website maintenance/development, printing, record archiving, data mailing and market research and medical consultants who provide medical services" (Black Dog Snapshot by Black Dog; privacy policy webpage https://www.blackdoginstitute.org.au/privacy/ dated 2018, accessed 17 October 2018). App policies also referred to user data as a

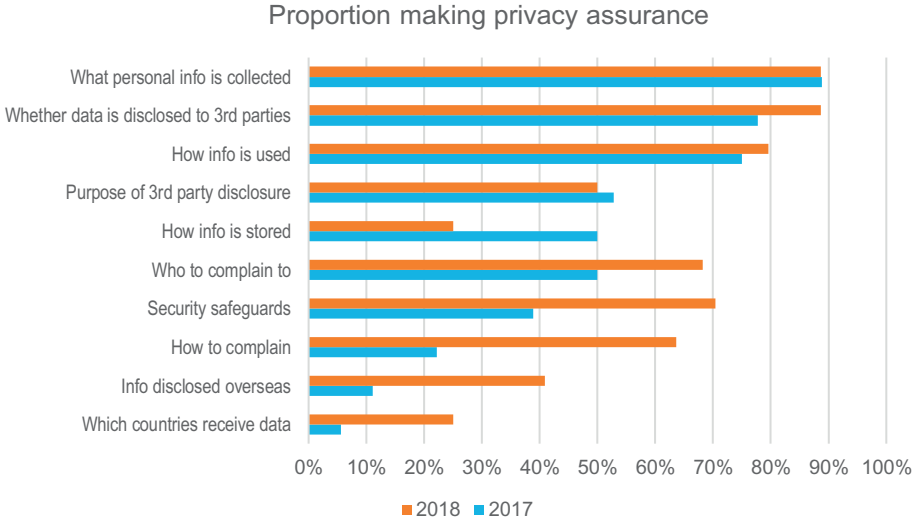

Fig. 3. Proportion of apps with a privacy policy making privacy assurances (2017 n = 36; 2018 n = 44).

business asset that could be transferred to other companies in the event of acquisition:

> *"Hive Brain may disclose your personally identifiable information upon a transfer or sale to another entity of all or substantially all of Hive Brain's stock or assets in Hive Brain's line of business to which this Privacy Policy relates or upon any bankruptcy or other corporate reorganization." [Beat Social Phobia; Positivity with Andrew Johnson; both by Hive Brain; privacy policy webpage http://relaxingapps.com/privacy-policy last updated 27 August 2015, accessed 17 October 2018].*

App policies informed consumers that the privacy practices could change at any time and did not necessarily promise to alert current users to material alterations. RR Eating Disorder Management, for example, put responsibility entirely on users to check the policy regularly for any updates:

> *"We may revise this Privacy Policy, so review it periodically … If you are concerned about how your information is used, bookmark this page and read this Privacy Policy periodically." [RR Eating Disorder Management by Recovery Record; privacy policy webpage https://www.recoveryrecord.com/privacy_policy last updated 23 June 2018, accessed 17 October 2018].*

Similarly, apps did not necessarily take responsibility for the data management practices of linked third parties. SuperBetter's policy, for example, explicitly instructed app users to find and understand this information:

> *"You should review the privacy policies of other sites you visit or link to from the Site to understand how these other sites use Cookies and how they use the information they collect through the use of Cookies or Web Beacons on their own sites." [SuperBetter by SuperBetter LLC; privacy policy webpage https://www.superbetter.com/terms dated 2018, accessed 17 October 2018].*

3.3.3. Security and complaints about loss of privacy

App policies commonly delivered disclaimers stating they were not responsible for any harm to the user resulting from loss of personal privacy and/or poor security. For example, Rise Up Eating Disorder Help's policy stated:

> *"You are responsible for maintaining the security of your Health-Related Information derived from your use of Recovery Warriors Services … We are not responsible for any third-party's access of your Health Related Information that you entered through the use of the Recovery Warriors Services." [Rise Up: Eating Disorder Help by Recovery Warriors; privacy policy webpage https://www.recoverywarriors.com/privacy-policy/ last updated 28 June 2018, accessed 17 October 2018].*

We found a range of detail about security within the app policies. At the more informative end, for example, SuperBetter's privacy policy told users that the app had "Secure Socket Layer encryption" which required users to "have an Internet browser which supports 128-bit encryption." (https://www.superbetter.com/terms dated 2018, accessed 17 October 2018) Other apps provided much less information about their security practices. For example:

> *"Excel at Life, LLC has put in place appropriate measures to safeguard and help prevent unauthorized access, maintain data security, and correctly use the information we collect on our site." [Stop Panic and Anxiety Self-Help by Excel at Life; privacy policy webage https://www.excelatlife.com/privacy_policy.htm dated 2017, accessed 17 October 2018].*

Policies did not always contain information about where or how to make a complaint about the app's privacy practices. Information about who to complain to was absent in 50% (18/36) of the policies (14/44, 32% of the policies available in 2018). Information about how to complain was absent in 78% (28/36) of policies (16/44, 36% in 2018). When information was provided, it tended to be in the form of responding to questions, rather than specifically mentioning the concept of complaints, for example: "Please contact us at support.calm.com if you have any questions about our practices or this Privacy Policy "(Calm – Meditate, Sleep, Relax; privacy policy webpage https://www.calm.com/privacy last updated 25 May 2018; accessed 7 November 2018). Five apps (5/56, 9% in 2018) provided information about where and how to complain to an external regulator about an app's privacy practices.

3.4. Impact of GDPR regulations on privacy policies

We identified a range of ways in which the new European Union GDPR privacy regulations (European Commission, 2018a; European Union, 2016) were mentioned and referenced in apps' privacy policies. In some cases, apps changed privacy practices to comply with the GDPR. For example, WellMind, an NHS branded app by Blue Step Solutions, had no privacy policy in 2017, but in 2018 provided a link to privacy policy Version 1.0, which was completed on 10 May 2018 as a "completely new document to comply with changes to data protection law, GDPR" (privacy policy webpage https://bluestepsolutions.com/privacy-policy/ accessed 17 October 2018). In another example, the policy of a United States app spelled out specific privacy rights available to EU app users, including rights to access and erase personal data held by the company:

> *"If you are within the European Union, you are entitled to certain information and have certain rights under the General Data Protection Regulation." [Rise Up: Eating Disorder Help by Recovery Warriors; privacy policy webpage https://www.recoverywarriors.com/privacy-policy/ last updated 28 June 2018, accessed 17 October 2018].*

In contrast, other apps' policies made a point of stating that their practices would not provide GDPR-level protection to its users but would adhere to local privacy regulations even if app users were 'visiting' the app from other jurisdictions:

> *"International Visitors and Customers: The Website is hosted in the United States. If you are visiting from the European Union (EU) or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal data to the United States which does not have the same data protection laws as the EU." [Beat Social Phobia; Positivity with Andrew Johnson, both by HiveBrain; privacy policy webpage http://relaxingapps.com/privacy-policy last updated 27 August 2015, accessed 17 October 2018].*

> *"INTERNATIONAL USERS By choosing to visit the Services or otherwise provide information to us, you agree that any dispute over privacy or the terms contained in this Privacy Policy will be governed by the law of the state of California." [RR Eating Disorder Management by Recovery Record; privacy policy webpage https://www.recoveryrecord.com/privacy_policy last updated 23 June 2018, accessed 17 October 2018].*

4. Discussion

Mental health apps and other digital health services have been promoted by health services and researchers partly because they appear to offer a discreet, accessible and affordable alternative to face-to-face therapy (Australian Government, 2015; Cotton, Irwin, Wilkins, & Young, 2014; Proudfoot, 2013). However our findings are adding to the emerging body of empirical work that suggests apps, including health apps, are not particularly private or secure (Blenner et al., 2016; Grindrod et al., 2017; Papageorgiou et al., 2018; Razaghpanah et al., 2018; Vallina-Rodriguez et al., 2016).

We indicate how mental health apps might threaten the privacy of users, including by actively encouraging users to share information online without warning them about the risks associated with normal

app data-sharing practices, and about the risk of malign security breaches. Normal data-sharing practices of app developers are often a means of monetising the app. For example, many developers offer their app free to users, but embed an advertising library in the application, which displays ads to the user while interacting with the app. However, third party ad libraries are granted the same permissions as the developers, and may share or on-sell the information they collect with other entities in the mobile ecosystem (Grace, Zhou, Jiang, & Sadeghi, 2012). Malign security breaches are always a possibility, and may be more likely if an app's security processes are poor. A study by Huckvale and colleagues found that none of the 79 apps in the UK NHS Health Apps Library encrypted user data stored on the phone, though they commonly used password security, which could lead a user to believe their data were secure (Huckvale et al., 2015).

Our data show that app developers are becoming more careful about whether and how they communicate data collection, use and sharing practices, although like others (Papageorgiou et al., 2018) we show that many apps still lack a readily accessible privacy policy, or any privacy policy at all. The new GDPR has been part of the impetus for this trend, having prompted some improvements in app transparency around privacy practices. However, given that other developers claim not to fall under GDPR jurisdiction, despite the GDPR clearly stating its provenance over all organisations that offer goods or services to EU persons regardless of their location (European Commission, 2018b), there remains some confusion around its provenance, and its overall impact on companies who hold data outside the EU remains unclear (Razaghpanah et al., 2018).

Despite these small improvements, we show that some apps still appear to request permission for access to user data that is unrelated to the stated app purpose, and some explicitly claim to absolve their developers of responsibility for protecting consumer information. This is done without providing guidance to consumers on how they could protect themselves (e.g. don't share really personal details, have strong banking passwords in case of identity theft) or where they could complain or seek redress about poor privacy practices. These practices are particularly problematic given that current evidence shows the public still has little understanding about the privacy risks associated with app use. There is low awareness amongst consumers about what kind of personal data is collected, used and shared by apps; people using health apps may particularly assume their data is kept private by app developers because health data is sensitive information. Consumers also have low awareness about the implications of developers' data sharing practices within the larger mobile ecosystem (Razaghpanah et al., 2018; Van Kleek et al., 2018).

4.1. Implications and recommendations

Personal health information, particularly mental health information, is highly sensitive. Breaching privacy may have significant repercussions, including exploitative, targeted advertising and negative impacts on an individual's employability, credit rating, or ability to access rental housing. It may result in emotional harm, particularly amongst those mental health app users who already have high levels of anxiety. Privacy breaches are also associated with identity theft and health system fraud (Dehling et al., 2015; Pasquale, 2015).

Our recommendations to improve protection of app user privacy are targeted at multiple stakeholders throughout the global mobile app ecosystem. Government regulators around the world should work in harmony to ensure global uptake of the GDPR as the exemplary data protection standard. This EU legislation protects consumer and personal data through several key requirements, such as opt-in user consent, alerting users to data transfer outside borders, anonymising data, enforcing data breach notification and user rights to data erasure (European Commission, 2018a). Widespread uptake and enforcement of this legislation would substantially improve privacy issues with apps, but there are other areas that can also be improved. Governments should place an immediate and high priority on supporting innovation in app security (Department of Industry, Innovation, and Science, 2017; Huckvale et al., 2015;). We suggest that consumers take every opportunity to improve their technological literacy (Torous & Roberts, 2017), including being aware that data sharing is common, may be hidden, and may change at any time (and without notice).

App developers should educate themselves about relevant privacy legislation and take steps to install better privacy tools into their products. We have previously written a publicly available a developer's guide to Australian privacy legislation and principles of good practice (Parker et al., 2017) and there are resources available to guide developers through internationally recommended practices and tools. (e.g. Federal Trade Commission, 2016; Flick, 2013; Martinez-Perez, de la Torre-Diez, & Lopez-Coronado, 2015; OAIC, 2014a) For example, developers could provide more granular options for users to select increased privacy at the expense of functionality, implement default privacy settings for new apps according to previously expressed user preferences (Van Kleek et al., 2018), and implement “just-in-time” strategies for requesting user consent for information collection (Sunyaev, Dehling, Taylor, & Mandl, 2014). We encourage more research with end-users to assist in the identification of privacy concerns and development of better privacy materials (Van Kleek et al., 2018) and advocate for innovative change that provides users with better privacy and data management control.

Since many apps are monetised through the collection and sharing of user data (Australian Communications and Media Authority (ACMA), 2013), developers may need incentives before they commit to better privacy practices. We recommend consumer advocacy groups lobby governments and industry to prompt the powerful app stores to take a role here (Parker, Bero, Gillies, Raven, & Grundy, 2019). App stores, including iTunes, should enforce the in-store reporting of permissions and should explain permissions and their implications in lay terms. They should also have stricter standards for privacy policies, for example. insisting they be comprehensible to those with lower literacy levels. This would assist users with preferentially choosing apps that have clear, understandable privacy practices and policies and making informed choices about sharing their personal information.

4.2. Limitations

Our purposive sampling of prominent mental health apps means that our app sample is not exhaustive nor representative of all health apps. Nevertheless, mental health app consumers are likely to encounter these targeted apps, and they provide information on a range of privacy practices and policies. Our analysis was restricted to the content of app advertising materials, but this gave us access to information on important privacy practices (i.e. permissions requests) and policies, albeit self-reported ones. Thus, future work should explore the actual nature of data sharing practices such as type of consumer data collected or network traffic analysis. The population of apps changes frequently, as shown by the differences in our updated data. Apps that we included in this study may no longer be available or their practices and policies may have changed.

5. Conclusions

The field of mental health apps is beset by risks to user privacy. Loss of user privacy may have significant ramifications for individuals and may contribute to current societal concerns about malign uses of aggregated data sets. We endorse the values exhibited through the GDPR, that prioritise the interests of individual consumers and the protection of privacy. We advocate for heightened app user protection, and enhanced choice, enabling consumers to enjoy the benefits of health apps with minimised risks of harm.

Funding

This work was supported by the Australian Communications Consumer Action Network (ACCAN). The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers. The funder, represented by co-author TK, informed the study design, data interpretation, and revision of the manuscript, but did not play any role in data collection, analysis or the decision to submit this paper for publication. QG was supported by a Postdoctoral Fellowship from the Canadian Institutes of Health Research.

Acknowledgements

We would like to thank Chris Klochek, MS, for developing the app store searching (crawling) program.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijlp.2019.04.002.

References

Australian Communications and Media Authority (ACMA) (2013). *Mobile apps: Emerging issues in media and communications.* Canberra, ACT: ACMA. Retrieved from http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Mobile%20apps%20Emerging%20issues%20in%20media%20and%20communications%20Occasional%20paper%201.pdf.

Australian Government (2015). *Australian Government response to Contributing Lives, Thriving Communities - Review of mental health programmes and services.* Canberra, ACT: Commonwealth of Australia.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). *Third party tracking in the mobile ecosystem.* 23–31. https://doi.org/10.1145/3201064.3201089.

Blenner, S. R., Kollmer, M., Rouse, A. J., Daneshvar, N., Williams, C., & Andrews, L. B. (2016). Privacy policies of android diabetes apps and sharing of health information. *JAMA, 315*(10), 1051–1052. https://doi.org/10.1001/jama.2015.19426.

Christensen, H., & Petrie, K. (2013). State of the e-mental health field in Australia: Where are we now? *The Australian and New Zealand Journal of Psychiatry, 47*(2), 117–120. https://doi.org/10.1177/0004867412471439.

Cotton, R., Irwin, J., Wilkins, A., & Young, C. (2014). *The future's digital. Mental health and technology.* London: Mental Health Network, NHS Confederation.

Dehling, T., Gao, F., Schneider, S., & Sunyaev, A. (2015). Exploring the far side of mobile health: Information security and privacy of mobile health apps on iOS and android. *JMIR Mhealth Uhealth, 3*(1), e8. https://doi.org/10.2196/mhealth.3672.

Department of Health (2017). Head to health. Retrieved from https://headtohealth.gov.au, Accessed date: 1 November 2017.

Department of Industry, Innovation, and Science (2017). *Cyber security - Capability statement.* Canberra, ACT: Australian Government. Retrieved from https://www.science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx Accessed on 28 February, 2017 .

Donker, T., Petrie, K., Proudfoot, J., Clarke, J., Birch, M. R., & Christensen, H. (2013). Smartphones for smarter delivery of mental health programs: A systematic review. *Journal of Medical Internet Research, 15*(11), e247. https://doi.org/10.2196/jmir.2791.

Ebeling, M. (2011). 'Get with the program!': Pharmaceutical marketing, symptom checklists and self-diagnosis. *Social Science & Medicine, 73*(6), 825–832. https://doi.org/10.1016/j.socscimed.2011.05.054.

European Commission (2018a). *2018 reform of EU data protection rules.* European Union. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#relatedlinks.

European Commission (2018b). *Who does the data protection law apply to?* European Union. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.

European Union (2016). General data protection regulation 2016/679. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Federal Trade Commission (FTC) (2016). *Mobile health app developers: FTC best practices.* Washington, DC: Federal Trade Commission. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

Flick, C. (2013). Informed consent in information technology: Improving end user licence agreements. In J. Weckert, & R. Lucas (Eds.). *Professionalism in the information and communication technology industry* (pp. 127–154). Canberra: ANU E Press.

Google Play. (2018), (August 14). Dangerous permissions. Retrieved from https://developer.android.com/guide/topics/permissions/overview#dangerous-permission-prompt accessed on 27 August, 2018.

Grace, M. C., Zhou, W., Jiang, X., & Sadeghi, A.-R. (2012). *Unsafe exposure analysis of mobile in-app advertisements. Paper presented at the Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

Grindrod, K., Boersema, J., Waked, K., Smith, V., Yang, J., & Gebotys, C. (2017). Locking it down: The privacy and security of mobile medication apps. *Canadian Pharmacists Journal (Ott), 150*(1), 60–66. https://doi.org/10.1177/1715163516680226.

Hollis, C., Morriss, R., Martin, J., Amani, S., Cotton, R., Denis, M., & Lewis, S. (2015). Technological innovations in mental healthcare: Harnessing the digital revolution. *The British Journal of Psychiatry, 206*(4), 263–265. https://doi.org/10.1192/bjp.bp.113.142612.

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

Martinez-Perez, B., de la Torre-Diez, I., & Lopez-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems, 39*(1), 181.

McGrath, P., Blumer, C., Carter, J. S., & (Producer) (2018). Medical appointment booking app HealthEngine sharing clients' personal information with lawyers. *ABC News*. 26 June. Retrieved from http://www.abc.net.au/news/2018-06-25/healthengine-sharing-patients-information-with-lawyers/9894114.

NHS. NHS Apps Library, Mental Health. (2018). Retrieved from https://apps.beta.nhs.uk/category/mental_health/ Accessed on 17 October, 2018.

Office of the Australian Information Commissioner (OAIC) (2014a). *Mobile privacy: A better practice guide for mobile app developers.* Canberra, ACT: OAIC. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers.

Office of the Australian Information Commissioner (OAIC) (2014b). *Privacy fact sheet 17: Australian privacy principles.* Canberra: Australian Government. Retrieved from https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.

Office of the Australian Information Commissioner (OAIC) (2018). *Australian businesses and the EU General Data Protection Regulation.* Canberra: Australian Goverment. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.

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.

Parker, L., Bero, L., Gillies, D., Raven, M., & Grundy, Q. (2019). The "hot potato" of mental health app regulation: A critical case study of the Australian policy arena. *International Journal of Health Policy and Management, 8*(3), 168–176.

Parker, L., Bero, L., Gillies, D., Raven, M., Mintzes, B., Jureidini, J., & Grundy, Q. (2018). Mental health messages in prominent mental health apps. *Annals of Family Medicine, 16*(4), 338–342. https://doi.org/10.1370/afm.2260.

Parker, L., Karliychuk, T., Gillies, D., Mintzes, M., Raven, M., & Grundy, Q. (2017). A health app developer's guide to law and policy: A multisector policy analysis. *BMC Medical Informatics and Decision Making, 17*(141), https://doi.org/10.1186/s12911-017-0535-0.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Cambridge, MA: Harvard University Press.

Perry, Y., Werner-Seidler, A., Calear, A. L., & Christensen, H. (2016). Web-based and mobile suicide prevention interventions for young people: A systematic review. *Journal of Canadian Academy of Child and Adolescent Psychiatry, 25*(2), 73–79.

Proudfoot, J. (2013). The future is in our hands: The role of mobile phones in the prevention and management of mental disorders. *The Australian and New Zealand Journal of Psychiatry, 47*(2), 111–113. https://doi.org/10.1177/0004867412471441.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). *Apps, trackers, privacy and regulators. A global study of the mobile tracking ecosystem.* 18–21 February. Paper presented at the Network and distributed systems security (NDSS) symposium, San Diego, CA, USA.

Sunyaev, A., Dehling, T., Taylor, P., & Mandl, K. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association,* e28–e33. https://doi.org/10.1136/amiajnl-2013-002605.

Torous, J., & Powell, A. C. (2015). Current research and trends in the use of smartphone applications for mood disorders. *Internet Interventions, 2*(2), 169–173. https://doi.org/10.1016/j.invent.2015.03.002.

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.

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., & Gill, P. (2016). *Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem.* arXiv preprint arXiv:1609.07190.

Van Kleek, M., Binns, R., Zhao, J., Slack, A., Lee, S., Ottewell, D., & Shadbolt, N. (2018). *X-ray refine: Supporting the exploration and refinement of information exposure resulting from smartphone apps. Paper presented at the Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.

Watkin, W. D. (2018, July 5). Cambridge Analytica used our secrets for profit – The same data could be used for public good. *The Conversation*. Retrieved from https://theconversation.com/cambridge-analytica-used-our-secrets-for-profit-the-same-data-could-be-used-for-public-good-98745.

World Health Organization (WHO) (2013). Mental health action plan 2013–2020. Retrieved from Geneva http://apps.who.int/iris/bitstream/10665/89966/1/9789241506021_eng.pdf?ua=1.