Android OS in Health Services

By Gabriel Ruiz, Craig Pitout, Corey Hilton, Tom Prusher, Codie Springer

Table 1

Showing 10 Apps and the permissions they need or do not need

APP	Need	Not Needed
Facebook	Phone, Photos/Media/Files, Camera, Microphone, Wifi, Identity, Calendar, Contacts, Location*	Bluetooth connection information, Device ID & call information
Instagram	Photos/Media/Files, Phone, Camera, Wifi, Identity, Contacts, Location, Microphone	Bluetooth connection information, Device ID & call information, change audio settings
YouCut- Video Editor	Photos/Media/Files, Microphone, Other- access to Google Photos	Read google service config
Audible	Identity, Photos/Media/Files, Wifi connection information	Device ID & Call Information, auto run on boot, contact info,
Period Tracker Clue: Ovulation & Period		Photos/Media/Files, Identity, Wifi connection information

Table 1

APP	Need	Not Needed
 Calorie Counter My Fitness Pal	Photos/Media/Files, Camera, Identity, Location, Bluetooth connection information	Wifi (enable/disable & change network), Contacts, auto-run on boot, control vibration settings
 Terraria	Photos/Media/Files, Wifi, Identity, Device ID & call information	
 Dash Tag		Device & app history, Photos/Media/Files, Wifi
 The Warehouse	Location, Wifi	Photos/Media/Files, Camera, Microphone, Bluetooth connection information
 Trade Me	Location, Photos/Media/Files	

Table 1

Table 2

Showing 10 Apps and the potential personal privacy breaches for each Android App

APP	Potential Personal Privacy Breach
Facebook	IPP3: potential breach through '*Intended recipients of information*' and '*Rights of access and correction*'. Lastly '*Fact information is being collected*' with the way FB embeds tracking across multiple apps/sites IPP4 & 9: indefinitely holding information, messages, 'likes' and page views etc IPP5: Cambridge Analytica & (Silverstein, 2019)
Instagram	IPP1: Device ID and call information is not necessary for the functioning of the application IPP6:It is not easy to see where you can access or request the information that Instagram has on you and therefore they may be in breach of IPP6. IPP6: As per the point above, it is not easy to access your own information and I have found no information around the duration that they keep a users information. Therefore they could be keeping information longer than necessary.
YouCut- Video Editor	IPP 1, 6 & 9: not easy to see where you can access your personal information, how long they may/not store it and what information they do keep and how that is pertinent to the functioning of the app
Audible	IPP 1: Device ID and call information is not necessary for the functioning of the application IPP 6 & 9: Access to personal information and storing this information for longer than required
Period Tracker Clue: Ovulation & Period	IPP1: Access to a users media and photos is not necessary for the functioning of the application

Table 2

APP	Potential Personal Privacy Breach
 Calorie Counter My Fitness Pal	IPP1 – photos/media/files, camera and contacts are not being collected lawfully as they are not necessary for the operation of this app. This app does not need this information to provide you with its service. IPP4 – The way this information is being collected is lawful as the user accepts to use it. It does however have the possibility to intrude unreasonably on the personal affairs of the individual through photos, contacts, camera and location. IPP5- (Newcomb, 2019) impact potentially 150m user accounts through data breach, largely concerned with users who re-use passwords across accounts IPP6 – The app does not make it easy to access information that has been collected. The nature of the information collected does not give them grounds to refuse disclosure. Data regarding exercise/eating can be exported but a premium subscription is required. Putting up a paywall to access information (Under Armour, Inc, 2019).
 Terraria	IPP1 – photos/media/files, identity and device ID & call information is not necessary for this app. This app does not need this information to provide you with its service making it unlawful. IPP4 – The way this information is being collected is lawful as the user accepts to use it. It does however have the possibility to intrude unreasonably on the personal affairs of the individual through photos, identity and device ID & call information.

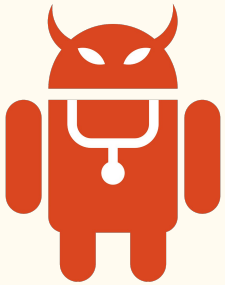
Table 2

APP	Potential Personal Privacy Breach
 Dash Tag	IPP1 – Photos/media/files is not a required permission for this app to operate. IPP3 – This app contains advertisements and will pass information to third parties while doing so. This may mean that the user is not aware of who is holding information on them. IPP4 – The collection of this information has not been made clear to the user and is required to use the app. This makes it an unfair means of collection of personal data. IPP6 – The app does not give the ability for the user to access information about them. The nature of the information collected does not give them grounds to refuse disclosure.
 The Warehouse	IPP1 – This app does not require location, photos/media/files, camera and microphone to carry out its services. This does not make the collection of this information lawful. IPP 6, 7, 9: there is no way to view, review or change the information held about the user. Also no information as to how long they would store the information
 Trade Me	IPP1 – Location data is not needed for this app to provide its services. IPP 6, 7, 9: no way to view, review or change the information held about the user. Also no information about how long they would store the information

Is Android safe?

In general, for casual use Android mobile devices that access and manage electronic healthcare information are not safe. (“Apple,” 2019).

- Multiple IPP potential violations:
  - Storage (IPP 1, 5)
  - Access (IPP 6, 7, 8, 10, 11)
  - Duration (IPP 9, 12)
- Outside intrusions: (Raphael, 2019)
  - Malware
  - Crypto attacks



There are steps that can be taken to secure a Android device for use in healthcare industry (Hussain et al., 2018)

- Professionally managed devices:
  - Use Security Services
  - Google Admin Service
  - Use a permission manager application
- Compartmentalize:
  - Use device only for work
  - Keep confidential data on secure cloud
  - Be diligent (Brown, 2019)
  - Research apps
  - Update device and apps
  - Secure with VPN, antiVirus, etc.

Can it be secured?

References:

Apple vs. Android: Which device offers the best healthcare data security? (2019) Retrived from https://www.mobius.md/blog/2019/01/apple-vs-android-which-device-offers-the-best-healthcare-data-security/

Rafael, J. R. (2019) *7 mobile security threats you should take seriously in 2019*. Retrieved from https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html

Hussaina, M., Zaidanb, A.A., Zidanb, B.B., Iqbala, S, Ahmedc, M.M., Albahrib, O.S., Albahrib, A.S. (2018) A security framework for mHealth apps on Android platform. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404818300798

Newcomb, A. (2019). Hacked MyFitnessPal Data Goes on Sale on the Dark Web—One Year After the Breach. Retrived from https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/

Silverstein, J (2019). *Hundreds of millions of Facebook user records were exposed on Amazon cloud server* Retrieved From https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

Under Armour, Inc. (2019) *Data Export FAQs* Retrieved From https://myfitnesspal.desk.com/customer/portal/articles/2457070-data-export-faqs-premium-feature

Brown, Shelby (2019) *7 security tips to keep people and apps from stealing your data.* Retrieved from https://www.cnet.com/how-to/7-security-tips-to-keep-people-and-apps-from-stealing-your-data/