Data sharing by popular health apps is routine and far from transparent, warn experts

March 20 2019

Credit: CC0 Public Domain

Sharing of user data by popular mobile health applications (apps) is routine, yet far from transparent, warn experts in a study published in

The BMJ today.

They say regulators should emphasise the accountabilities of those who control and process [user data](#), and [health](#) app developers should disclose all data sharing practices and allow users to choose precisely what data are shared and with whom.

App developers routinely, and legally, share user data. But evidence suggests that many health apps fail to provide privacy assurances around data sharing practices, and pose unprecedented risk to consumers' privacy, given their ability to collect sensitive and personal health information.

So researchers led by Assistant Professor Quinn Grundy at the University of Toronto, set out to investigate whether and how user data are shared by popular medicines related mobile apps and to characterise privacy risks to app users, both clinicians and consumers.

They identified 24 top rated medicines related apps for the Android mobile platform in the United Kingdom, United States, Canada, and Australia.

All apps were available to the public, provided information about medicines dispensing, administration, prescribing, or use, and were interactive.

First, they downloaded each app onto a smartphone and used four dummy user profiles to simulate real world use.

They ran each app 14 times and found baseline traffic relating to 28 different types of user data. They then altered one source of user information and ran the app again to detect any privacy leaks ([sensitive information](#) sent to a remote server, outside of the app). Companies

receiving sensitive user data were then identified by their IP address, and their websites and privacy policies were analysed.

Most (19 out of 24; 79%) of the sampled apps shared user data outside of the app.

A total of 55 unique entities, owned by 46 parent companies, received or processed app user data, including developers and parent companies (first parties) and service providers (third parties).

Of these, 18 (33%) provided infrastructure related services such as cloud services and 37 (67%) provided services related to the collection and analysis of user data, including analytics or advertising, suggesting heightened privacy risks.

Network analysis revealed that first and third parties received an average of three unique transmissions of user data. Both Amazon.com and Alphabet (the parent company of Google) received the highest volume of user data (24 unique transmissions), followed by Microsoft (14).

Third parties also advertised the ability to share user data with 216 "fourth parties" including multinational technology companies, digital advertising companies, telecommunications corporations, and a consumer credit reporting agency.

Only three of these fourth parties could be characterised predominantly as belonging to the health sector.

Several companies, including Alphabet, Facebook, and Oracle, occupied central positions within the network with the ability to aggregate and re-identify user data

The researchers point to some limitations that may have influenced the

results. For example, it is unknown whether iOS apps share user data and whether these apps share user data more or less than other health apps, or apps in general.

Nevertheless, they say their findings suggest that health professionals "should be conscious of privacy risks in their own use of apps and, when recommending apps, explain the potential for loss of privacy as part of informed consent."

Privacy regulators should also consider that loss of privacy is not a fair cost for the use of digital health services, they conclude.

More information: Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis, *BMJ* (2019). DOI: 10.1136/bmj.l920 , www.bmj.com/content/364/bmj.l920

Provided by British Medical Journal