THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Commercial health apps

in the user's interest?

Citation for published version:
Pagliari, C 2019, 'Commercial health apps: in the user's interest?', *British Medical Journal (BMJ)*, vol. 364, 1280. https://doi.org/10.1136/bmj.l1280

Digital Object Identifier (DOI):
10.1136/bmj.l1280

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
British Medical Journal (BMJ)

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 27. Jul. 2024

BMJ 2019;364:l1280 doi: 10.1136/bmj.l1280 (Published 21 March 2019)

EDITORIALS

Commercial health apps: in the user's interest?

Study shows how sensitive data from health apps is finding its way to corporations

Claudia Pagliari *senior lecturer in primary care*

eHealth Research Group, Usher Institute of Population Health Sciences and Informatics, University of Edinburgh, Edinburgh, UK

Excitement about digital health is at an all time high, with innovations in mobile personal computing, robotics, genomics, artificial intelligence, cloud based infrastructure, and more, promising to revolutionise the organisation, quality, cost effectiveness, inclusivity, and personalisation of patient care.[1 2] Amid this celebration, the shadow of privacy risks continues to lurk, like an unwelcome guest at a party.[3-5]

In a linked paper, Grundy and colleagues (doi:10.1136/bmj.l920) examine the surreptitious tracking and profiling of people using medicines related apps, which can generate sensitive health data.[6]

Grundy and colleagues used an "app store crawling program" to identify the top 100 medicines related apps available to Android mobile users in the UK, USA, Australia, and Canada, combined with a search for endorsed apps on a medicines related agency website, a health app library, a systematic review, and their personal networks. Of the 821 apps screened, 24 met the criteria of managing drugs (for example, information, decision support, adherence, engagement), requesting at least one "dangerous" permission, claiming to collect or share user data, or requiring user interaction. These were tested multiple times, using dummy user profiles representing professionals and patients, to create a baseline, then the process was repeated, each time changing one type of user information. Comparing network traffic before and after the profile changes revealed how the new data were being transmitted from the app. Next, the authors used IP Lookup tools to identify the data recipients and analysed their company information, privacy terms, data sharing agreements, and business models. Recipients were classified as first parties (app developers), third parties (external entities receiving data from the app), and fourth parties (organisations that receive and might aggregate data from multiple third parties). Network analysis was then used to map and visualise the pathways through which data are potentially being shared.

"Dangerous" permissions

On average, apps requested four or more "dangerous" permissions for private information held on the user's phone, or which affected the operation of other apps. Most transmitted encrypted data, but several used clear text. Nineteen of the 24 apps shared user data, which were received by 55 unique third parties. Third parties typically reserved the right to hold user information for their own commercial purposes. Some collected data from other apps, along with communications and behavioural information, building detailed user profiles across devices, which could be shared with business affiliates or sold on. Although most third parties were developers, 33% were advertising companies and 8% were investor owned. The fourth party network included 237 entities, including "families" of companies with the same owner. Of these, Alphabet (Google) and Facebook were able to receive the most types of data, either directly from the apps or through third parties, whereas Alphabet, Amazon, and Microsoft received the highest volume of app user data overall.

Although others have convincingly shown vast networks of data leakage by Android apps,[7 8] this study is unique in focusing on apps that can yield highly sensitive information about people's use of or need for medicines. As the authors' note, although many of the data fields collected by these entities can seem innocuous, in combination they can be used to uniquely identify and profile users, effectively bypassing existing data protection and privacy laws.

Such tracking practices differ for apps and online search engines,[7] but the dominant role of global corporations such as Google is evident in both—as was also shown in another study published this week on "ad tech surveillance on the public sector web."[9] With these digital apex predators voraciously consuming other companies and the data they generate, as well as the global talent pool of data scientists able to make best use of them, concepts such as "free market" and "democracy" are beginning to look decidedly 20th century.

Exploitative practices

National Health Service patients may be cushioned from the worst impacts of exploitative health data practices, unlike our US cousins, but we are not immune. A shadow economy of commercial data brokers is silently gleaning, linking, and commoditising behavioural information about our health, spending, political attitudes, movements, time spent online, social networks, and so on, which is already influencing our

Claudia.Pagliari@ed.ac.uk

For personal use only: See rights and reprints http://www.bmj.com/permissions Subscribe: http://www.bmj.com/subscribe

BMJ: first published as 10.1136/bmj.l1280 on 21 March 2019. Downloaded from http://www.bmj.com/ on 21 March 2019 by guest. Protected by copyright.

mortgages, employment, travel, and more. With corporate data brokers and public sector data centres now collaborating to "understand society," it is not overly fanciful to predict future policy scenarios in which these insights affect our access to drugs or place on a surgical waiting list. For now, the threats to our privacy and self determination are arguably the most important.

An EU ePrivacy regulation[10] that extends the General Data Protection Regulation (GDPR)[11] to web trackers and profiling is under development, although it has been described as "sitting in the sidings, being mobbed by lobbyists."[12] As the study reported by Grundy and colleagues illustrates, issues of consent and legitimate interest are muddied in the multiparty data ecosystem of digital health apps. Meanwhile, the capacity of regulators such as the Information Commissioner's Office (https://ico.org.uk) to enforce the rules on privacy is severely constrained by lack of manpower.[13] Penalties for exploitative data practices are typically applied only after incidents have occurred, been spotted, and been reported, and it is likely that the majority slip under the radar.

Nevertheless, there is a good news story hidden in this work—for one thing, Grundy and colleagues showed that companies were more likely to declare their data sharing partnerships after the GDPR had come into force, albeit with an eye on the back door. More importantly, all the studies mentioned here show the value of digital forensic research methods, for uncovering the illicit practices and business relations underlying fine words about regulatory compliance. With advances in technologies such as bots[9] and AI,[13] regulators could soon have an effective dashboard of suspect apps and websites. How they choose to respond to it is another matter, but without more effort to tackle the problem, public trust in digital health will continue to hold back its future.

CP leads the Interdisciplinary Research Group in eHealth, the MSc in Global eHealth, and the consumer informatics theme of the NHS Digital Academy.

Competing interests: *The BMJ* has judged that there are no disqualifying financial ties to commercial companies. The author declares the following other interest: The author holds one industry sponsored research grant, from the WhatsApp Foundation, for a study of disease outbreak misinformation in India. Further details of The BMJ policy on financial interests is here: https://www.bmj.com/sites/default/files/attachments/resources/2016/03/16-current-bmj-education-coi-form.pdf.

Provenance and peer review: Commissioned; not externally peer reviewed.

1 NHS England. The future of healthcare: our vision for digital, data and technology in health and care (policy document). 17 October 2018. www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care
2 White A. Turning health data into knowledge to improve lives. Open Access Government, 18 June 2018. www.openaccessgovernment.org/turning-health-data-into-knowledge-to-improve-lives/46716/
3 Gostin LO, Halabi SF, Wilson K. Health data and privacy in the digital era. *JAMA* 2018;320:233-4. https://jamanetwork.com/journals/jama/fullarticle/2686001. 10.1001/jama.2018.8374 29926092
4 Smith DW. GDPR runs risk of stifling healthcare innovation. *Eureka (Asunción)* 2018;30. https://eureka.eu.com/gdpr/gdpr-healthcare/.
5 Duggal R, Brindle I, Bagenal J. Digital healthcare: regulating the revolution. *BMJ* 2018;360:k6. 10.1136/bmj.k6 29335296
6 Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ* 2019;364:l920.
7 Binns R, Lyngs U, Van Kleek M, Zhao J, Liber T, Shadbolt N. Third Party Tracking In The Mobile Ecosystem. *WebSci '18 Proceedings of the 10th ACM Conference on Web Science* 2018. https://dl.acm.org/citation.cfm?id=3201089
8 Privacy International. How apps on Android share data with Facebook (even if you don't have a Facebook account). December 2018. https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf
9 Cookiebot. Ad tech surveillance on the public sector web. A special report on pervasive tracking of EU citizens on government and health service websites. 18 March, 2019. www.cookiebot.com/media/1121/cookiebot-report-2019-medium-size.pdf
10 Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.
11 Regulation(EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
12 Lomas N. ePrivacy: An overview of Europe's other big privacy rule change. *TechCrunch* 7 October 2018. https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/
13 Compliance meets artificial intelligence. *Compliance Week* [undated] https://www.complianceweek.com/glossary/compliance-meets-artificial-intelligence

Published by the BMJ Publishing Group Limited. For permission to use (where not already granted under a licence) please go to http://group.bmj.com/group/rights-licensing/permissions

BMJ: first published as 10.1136/bmj.l1280 on 21 March 2019. Downloaded from http://www.bmj.com/ on 21 March 2019 by guest. Protected by copyright.