[1] Lawrence S. Bloomberg Faculty of Nursing, University of Toronto, Toronto, ON, Canada

[2] Hospital for Sick Children (SickKids), Toronto, ON, Canada

[3] Mommy Monitor, Toronto, ON, Canada

Correspondence to: Q Grundy
quinn.grundy@utoronto.ca

Cite this as: *BMJ* 2021;373:n1429
http://dx.doi.org/10.1136/bmj.n1429
Published: 16 June 2021

Health apps are designed to track and share

We must advocate for greater scrutiny, regulation, and accountability

Quinn Grundy, [1] Lindsay Jibb, [2] Elsie Amoako, [3] Geoffrey Fang[2]

Mobile health apps have generated substantial investment and enthusiasm for their potential to personalise interventions using real time user data. However, user data are not only invaluable for creating engaging and effective apps. Health apps are just one source of user data that is collected, transmitted to third parties, then aggregated to create detailed impressions about users and people such as them. These sources of big data are commercialised, often as consumer insights or algorithms, and used to deliver microtargeted adverts, influence political behaviours, or make decisions about health insurance, employment, and housing,[1 2] sometimes with exploitive or discriminatory effects.[3]

Even so, users might reasonably assume that apps advertised for health purposes would treat health and personal information with greater care. To question this assumption, Tangari and colleagues (doi:10.1136/bmj.n1248) analysed more than 15 000 free Android apps in the "medical" and "health and fitness" categories of the Google Play store and compared their privacy practices with a random sample of more than 8000 apps from store categories unrelated to health.[4] They examined the apps' code to understand what kind of user data might be shared and with whom, and then during network traffic analysis which data were actually shared. Finally, they assessed users' awareness of privacy failings as expressed in app store reviews.

The authors found that mobile health apps were designed for tracking and sharing information.[4] Developers had programmed most health apps (88%) to enable tracking capabilities. About two thirds of apps could collect advert identifiers or cookies, which can be used to uniquely identify users across different apps and websites, even if not by name. One third could collect a user's email address, and about a quarter could identify the mobile phone tower to which a user's device is connected, potentially providing information on the user's geolocation.

Health apps then shared user data within the wider, commercial mobile ecosystem, which includes developers, their parent companies, cloud storage providers, and a host of services that developers use to monetise, improve, or learn about use of their app.[5-7] In 63% of apps, developers had embedded at least one third party service such as an advert library, analytics service, or social media provider, which most commonly were a small number of tech corporations, including Google, Facebook, and Yahoo!.[4]

Mobile health apps appeared to be somewhat more reticent about sharing user data with third parties than non-health apps, having fewer interactions with advert and tracking services.[4] This could reflect what users expect from health apps: users rated health apps with adverts or tracking more negatively.[4] Tangari and colleagues found that only 4% of health apps actually transmitted data; however, they measured data transmission for only 180 seconds while automatically running the app,[4] finding a much lower prevalence of data sharing than recent small, in-depth analyses, which fully explored apps' functions.[5 8]

Data protection

May 2021 marked the third anniversary of the General Data Protection Regulation (GDPR), which has improved transparency around apps' data collection and sharing practices[5 9] and requires specific measures to ensure active consent to data sharing.[10] Privacy regulation such as the GDPR continues to distinguish between sensitive and non-sensitive data, requiring more stringent controls for sensitive or personal data.[11] However, a user's health status can increasingly be inferred—accurately or not—on the basis of diverse data points such as self-reported mood, the name of the health app, postal code, search history, and race or ethnicity, calling into question whether all data, and especially aggregated data, should be treated as sensitive.

Privacy regulation also still largely relies on the idea that an "informed consumer" can choose apps with adequate privacy assurances.[11] However, 29% of the apps sampled by Tangari and colleagues failed to provide a privacy policy and another 24% collected and transmitted user data in ways that violated the terms set out in their privacy policy.[4] There is no assurance that users will know how apps track and share data, and regulators continue to place the greatest responsibility on those with the least ability to prevent harm.[12 13]

The status quo regarding health apps' privacy practices means that it is difficult and even irresponsible to offer tips to busy clinicians or consumers about how to choose a health app that protects their privacy. Consumers can, however, make it more difficult to be tracked by disabling advert identifiers, adjusting app permissions, and using advert blockers.[14] We must also advocate for greater scrutiny, regulation, and accountability on the part of key players behind the scenes—the app stores, digital advertisers, and data brokers—to address whether these data should exist and how they should be used, and to ensure accountability for harms that arise.[15]

Competing interests: The BMJ has judged that there are no disqualifying financial ties to commercial companies. The authors declare the following other interests: QG and LJ have received research funding from the New Frontiers in Research Fund (government of Canada) through the Hospital for Sick Children for research

on data sharing practices of children's health apps. Mommy Monitor receives funding from the government of Ontario.

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

1 Pasquale F. *The black box society: The secret algorithms that control money and information.* Harvard University Press, 2015doi: 10.4159/harvard.9780674736061.
2 Ebeling M. *Healthcare and big data: Digital specters and phantom objects.* Palgrave Macmillan US, 2016doi: 10.1057/978-1-137-50221-6.
3 Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. *Science* 2019;366:447-53. doi: 10.1126/science.aax2342 pmid: 31649194
4 Tangari G, Ikram M, Ijaz K, Kaafar MA, Berkovsky S. Mobile health and privacy: cross sectional study. *BMJ* 2021;373.
5 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. doi: 10.1136/bmj.l920 pmid: 30894349
6 Vallina-Rodriguez N, Sundaresan S, Razaghpanah A, et al. Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem. 1st Data and Algorithm Transparency Workshop; New York, NY. 2016.
7 Razaghpanah A, Nithyanand R, Vallina-Rodriguez N, et al. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. Proceedings 2018 Network and Distributed System Security Symposium. 2018.
8 Huckvale K, Torous J, Larsen ME. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA Netw Open* 2019;2:e192542. doi: 10.1001/jamanetworkopen.2019.2542 pmid: 31002321
9 Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Assessment of the fairness of privacy policies of mobile health apps: Scale development and evaluation in cancer apps. *JMIR Mhealth Uhealth* 2020;8:e17134. doi: 10.2196/17134 pmid: 32720913
10 General Data Protection Regulation, (2018).
11 Marelli L, Lievevrouw E, Van Hoyweghen I. Fit for purpose? The GDPR and the governance of European digital health. *Policy Stud* 2020;41:447-67doi: 10.1080/01442872.2020.1724929.
12 Parker L, Bero L, Gillies D, Raven M, Grundy Q. The "hot potato" of mental health app regulation: A critical case study of the Australian policy arena. *Int J Health Policy Manag* 2019;8:168-76. doi: 10.15171/ijhpm.2018.117 pmid: 30980633
13 Ferretti A, Ronchi E, Vayena E. From principles to practice: benchmarking government guidance on health apps. *Lancet Digit Health* 2019;1:e55-7. doi: 10.1016/S2589-7500(19)30027-5 pmid: 33323230
14 Thompson SA, Warzel C. The privacy project: Twelve million phones, one dataset, zero privacy. The New York Times. 2019 December 19, 2019.
15 Zuboff S. *The age of surveillance capitalism.* PublicAffairs, 2019.