Build trust in digital health

The rapid rollout of digital health approaches in the ongoing global COVID-19 pandemic has neglected to prioritize data privacy and is a missed opportunity for building users' trust in these technologies for future outbreaks and quotidian healthcare.

The current COVID-19 pandemic has come at a time during which there are an estimated 3.5 billion smartphone users worldwide, which means four out of ten people are able to generate data relevant to active research and containment of the outbreak. The digital-health-app community was poised to respond, with preliminary analyses from the recent Ebola outbreak acting as a proof of concept. Digital data are now central to the global anti-COVID-19 arsenal, and dozens of COVID-19-related apps are available. However, this rapid deployment, combined with the enactment of emergency powers by governments, has resulted in data privacy's being pushed to the sidelines. In this issue, we present a Focus on Digital Privacy and COVID-19 that explores these new digital technologies, their impact in the context of the COVID-19 pandemic and the gains that must be made around data handling to ensure that users' privacy is protected.

The technological progress that has been made in this field means that with these data, the world has an unprecedented opportunity to understand the outbreak's progression, make sense of the myriad symptoms that are associated with COVID-19 and respond to a flare-up of infections, all in near real time. There is a wide range of potential applications for digital data in the fight against COVID-19, as Rachel McKendry and colleagues discuss in their Review. Symptom-tracking apps, and websites such as those deployed by the National Health Service of the UK and by researchers in Israel, encourage users to input their symptoms for rapid diagnosis, and then these reports are stored in a national database. When combined with maps, these data can be used to track the location of an outbreak. Digital contact-tracing apps notify people when they have come into contact with a person infected with SARS-CoV-2. The expedited anticipated release of remote health-monitoring devices, such as those that measure body temperature, could also

generate more data that could be made available for analysis.

Because many of these digital approaches rely on the good will of those sharing the data, the issue of participant trust is paramount, and several apps have already fallen at that hurdle. For these approaches to work, data of a highly sensitive nature, most often directly linked to the user's health records, need to be shared. A user could reasonably expect these data to be heavily regulated per local health-data laws and for their privacy to be of prime concern to the developers. However, the urgent nature of the task of protecting public health has deprioritized this. In Israel, the government used emergency powers to track peoples' locations from their mobile phones for contact tracing. In the UK, the regulations for the control of patient information were changed mid-March in response to the pandemic's urgency, which means general practitioners in the UK are legally obligated to make health data, including identifiable data, available to NHS Digital and the UK Biobank for research and public-health purposes. A new analysis of 50 COVID-19-related apps in the Google Play store shows that only 16 of the 50 apps sampled explicitly state their intent to anonymize users' data in their policies.

The ways in which data have been collected, stored and accessed in response to COVID-19 have also been controversial. The debate is about whether data should be centralized (i.e., data are kept in a database accessible to the developer and the local government) or decentralized (i.e., data are held in a person's phone, such as in the approach used in Germany). The UK's first iteration of a contact-tracing app was based on a centralized model, which caused the approach to be criticized as being inefficient and possibly illegal, and incited public outrage and cost millions. Norway's contact-tracing app, also based on a centralized model, has been discontinued because of privacy concerns and potential human-rights violations. In this issue of *Nature Medicine*, a new consortium for

sharing COVID-19 symptom data proposes a federated approach to storing peoples' health data in which the data are aggregated for de-identification. However, this is not a cure-all; an app developed by Google using the centralized data approach (and hence Bluetooth, not GPS) has recently come under fire for requiring users to give access to their location data to use the contact-tracing app.

For much of the world's population, COVID-19-linked apps will be their first concrete interaction with digital approaches to healthcare. Trust in these systems should not be presumed. Trust must be earned and maintained. Nor is it universal. Just as the COVID-19 outbreak is distributed unevenly, ravaging communities of color in the United States and the United Kingdom, distrust of governmental institutions in underserved populations is to be expected. Experts have been warning for some time now that ambiguity about the management of data-privacy laws could cause a crisis of public trust. But governments have been sluggish to take concrete action to ensure that laws and policies regulating digital data privacy are transparent and consistent, which has fed into the current mismanagement of digital tools. A counterexample is South Korea, in which discussions around privacy were had after the Middle East respiratory syndrome epidemic and digital privacy laws were loosened in 2015. Singapore anticipated public outcry and consequently built transparency into their contact-tracing app's design, making sure it uses open source code and can be scrutinized by the public.

It is not in a time of crisis that complex issues such as privacy can be effectively addressed, and trust is built on strong foundations. To ensure that the public will continue to welcome digital health approaches, meaningful engagement with the public, transparency and preparedness are direly needed. □

Published online: 7 August 2020
<https://doi.org/10.1038/s41591-020-1032-z>