People have the AI power

Citizen scientists are empowered by mobile technology to collect data and crowdsource knowledge. Furthermore, automated machine learning tools allow non-experts in AI to analyse data. Ethical and regulatory questions arise, however, as data collection and AI technologies become enmeshed in people's lives.

COVID-19-related data collection on individual citizens, with varying levels of invasiveness, has been introduced by governments around the world. While this has raised privacy and human rights concerns (as we discussed in our April [Editorial](#) from last year), the pandemic has brought the value of health data gathering to everyone's attention. In an alternative, participatory approach, individual citizens voluntarily contribute data with their own smartphones and directly see the benefits of crowdsourcing data in innovative data visualization apps. Multiple citizen science projects have sprung up since the start of the pandemic to gather health data, and flu trackers have been adapted to track COVID-19. In March 2020, the [COVID Symptom Study](#) app was launched, a not-for-profit initiative from health science company ZOE with scientific analysis provided by researchers from King's College London. The app has been used by over 4 million people worldwide who provided regular reports on COVID-19 symptoms. [Analysis](#) of the crowdsourced data from the study helped establish loss of smell and taste as a key symptom of COVID-19 early in the pandemic, and later also delirium as a key symptom in older people.

Such crowdsourcing projects are valuable ways of gathering data and engaging individual citizens in public health science. However, analysing data requires data science experts. Machine learning methods have emerged as powerful analysis tools, but until recently they required substantial hardware resources and machine learning expertise. An empowering step is the development of platforms that provide code-free automated machine learning (AutoML) interfaces. Instead of relying on machine learning experts to decide on hyperparameters and, for instance, the number of layers to use in a specific neural network, these platforms test and choose architectures automatically based on their performance evaluation. AutoML, with the aim of automating the machine learning workflow, has been around for decades. But in recent years, companies such as Amazon, Google and Microsoft have made this approach available and more attractive for a wider group of users, including clinicians and researchers without coding experience.

Credit: Alberto Gordillo

In an [Analysis](#) article in this issue, Korot et al. analysed the performance of six such platforms on medical image classification. AutoML is particularly relevant in medical imaging due to the lack of in-house machine learning expertise within many hospitals and clinical research groups. The authors found that the leading AutoML platforms provide high image classification performance. However, they also cautioned that the ease of AutoML could lead to inadvertent misuse. For example, models could be deployed on differing populations or imaging techniques than those used in the initial validation dataset, potentially yielding unreliable real-world performance. But overall, the authors are optimistic, stating that AutoML has the potential to democratize machine learning for clinicians and researchers. Such frameworks could also lead to the exploration of responsible AI practices, in which the medical community evaluates the safety and efficacy of AutoML and other AI-based devices coming to market.

A related concern about the potential for mis-deployment pertains to predictive or diagnostic medical AI/ML apps designed for personal use. Such apps can, in principle, empower individual users who want to collect and make use of their own medical and health data. An example is the irregular rhythm notification feature of the Apple Watch, which is classified by the Food and Drug Administration as a class II (moderate risk) medical device. In a [Perspective](#) in this issue, Babic et al. argue that the regulatory landscape in the burgeoning industry

of medical AI/ML apps for personal use should be built on an understanding of how consumers interact with direct-to-consumer medical AI apps. In particular, AI/ML predictive or diagnostic devices often require users, the vast majority of whom are not medical experts or trained in statistics, to make sense of probabilistic outputs. For instance, in an example described by the authors, when a skin cancer screening app has 99% sensitivity and 95% specificity and the underlying disease is present in 1% of skin lesions population-wide, a positive outcome of a test means that the Bayesian probability of the user having the disease is 16.7%. In practice, users are likely to repeat the test: if out of five tests, three are positive, a user is likely to interpret this as strong evidence for a positive diagnosis, but the probability to actually have the disease would only be 0.86%. Individual users will be risk-averse, leading to a proliferation of false positives, overdiagnosis and overtreatment, resulting in personal as well as social costs.

Perspicuity is needed on the part of companies that bring AI medical devices to market, and regulatory oversight is warranted as increasingly powerful and fast-developing AI technologies are used by humans whose decision-making is flush with cognitive biases. The authors provide recommendations for regulators in regards to oversight of AI device makers, such as requiring clinical studies or field research to study how consumers actually utilize such devices. The risk of harm from health AI apps needs to be explored in careful risk-benefit evaluations when developing these applications, involving social scientists.

Individual citizens have the power of data and AI at their fingertips, but these developments are taking place more quickly than regulators can keep pace. AI technologies make fast progress, but human nature does not. The pragmatic and ethical space where AI meets human nature requires wisdom and examination. To what extent people can benefit from the power of AI is yet to be determined. □

Published online: 20 April 2021
<https://doi.org/10.1038/s42256-021-00340-z>