thebmj

FEATURE

Alarm bells ring for patient data and privacy in the covid-19 goldrush

Patient data are being used on an unprecedented scale by governments and healthcare bodies to stop the pandemic in its tracks. But what of the long term effects of accessing such sensitive information, asks **David Cox**

David Cox *freelance journalist*

Cambridge

Among the few success stories of the covid-19 pandemic has been how South Korea remarkably stopped its outbreak at just under 11 000 cases and with no lockdown. Its mass testing has been lauded, but equally key was extensive tracing—and surveillance—of its citizens that would prove uncomfortable in other nations.

Korea's containment is in part thanks to a sophisticated network of GPS trackers linked to people's smartphones, as well as access to electronic records such as credit card purchases that allowed the tracking and tracing of every individual's movements, right down to what buses they rode or shops they visited. The system issues alerts to the public, phones buzzing whenever an infectious person is in the area or a citizen has crossed the path of someone who has tested positive, urging them to get tested themselves and to self-isolate.[1] The government even started issuing tracking wristbands to stop people dodging quarantine by leaving their phones at home.[2]

In Asia, bad memories of the SARS, H1N1, and MERS outbreaks have influenced public perspectives on how the government uses and shares their data. "The social shock of MERS in Korea was intense because the Middle East is quite a distant place psychologically as well as geographically," says Youngkee Ju, who researches the dynamics of risk perception at Hallym University in Chuncheon, South Korea.

Ju said that, in one unpublished survey his team conducted between February and April 2020, 68.2% of the respondents preferred maintaining the current level of information sharing even if it sacrificed individual right to privacy. A similar trend was seen in a survey of 1000 people he published in February, which found that most respondents supported the Korean government sharing the travel details of people with covid-19.[3]

The importance of data in tracing, tracking, and preventing transmission has seen governments around the world turn to the expertise of private technology companies in gathering, storing, and processing information. In China, public transport networks in Wuhan have introduced contactless fever detection technology, which uses thermal imaging cameras to scan a passenger's face and take their temperature remotely. The software then silently triggers an alarm if a temperature above 37°C is identified.[4]

In Europe and the US, concerns about privacy and civil liberty abound. A recent survey from health policy analysts KFF found that 68% of Americans would be willing to share coronavirus test results via an app with public health officials; 53% said that they would not be willing to allow the government to use their data to conduct contact tracing.[5]

Everyone wants to save lives, end lockdowns, and escape the pandemic. But doubts linger about the trade-off between individual privacy rights and public health that's been brushed over amid the crisis. After furores over the European Union's General Data Protection Regulation (GDPR) and data breaches involving Facebook and Google, among others, are we now voluntarily giving private corporations access to our sensitive personal data via governments and healthcare bodies?

The ghost of data breaches past

In the UK, the NHS has partnered with Amazon, Google, Microsoft, and the data analytics firm Palantir to create a data store—ranging from the contents of calls to NHS 111 to covid-19 test results and clinical information about patients in intensive care—for use in predictive computer simulations of the outbreak. Critics have expressed concern about a lack of transparency, particularly around Palantir's data mining activities [6] For some in the media, it was an uncomfortable reminder of 2015 when London's Royal Free Hospital transferred 1.6 million confidential medical records to Google DeepMind without the knowledge or consent of those patients.[7]

"An area of concern, which we've seen for a few years, is the involvement of big tech companies providing data infrastructure, software, or analysis to healthcare bodies," says Stephen Roberts, a global health policy researcher at London School of Economics. In the past, there have been security oversights in these data sharing projects, he says.

dcwriter89@gmail.com

"When engaging with big tech, I think there needs to be explicit terms that the data will not be used for additional research purposes or any type of commercial exchange or development. And ultimately the patients themselves have the right to be told if their data is being used."

Governments have sought to play down concerns surrounding data privacy and security by insisting that all patient data gathered and used in these projects is anonymised. But in many cases, there is little explanation of how exactly this is done. Cybersecurity experts point out that merely stating the data are anonymous is insufficient to satisfy GDPR requirements.

Keeping medical records truly anonymous is extremely difficult—even if names and identifier codes are removed from the data—because of the amount of personalised information they contain. To illustrate this, scientists at Imperial College London's computational privacy research group conducted a study showing that just 15 demographic variables could correctly re-identify someone in an anonymised dataset of 300 million people.[8] As such, keeping identities secret in hospital records that typically contain dozens of variables is a nearly impossible task.

As a result, legal experts think that there is an urgent need for new legislation to cover exactly how patient data should be used during crisis scenarios, a need that has been brought to the forefront by covid-19.

Trust and tracking

Ongoing contact tracing initiatives, such as the new NHSX app currently in testing on the Isle of Wight, have shown the importance of gaining public trust in a crisis. These apps—which use Bluetooth technology to detect and alert people who might have come into contact with those infected with the virus—require at least 60% of the population to report their health status to be effective.[9]

But they have also exacerbated concerns over data privacy. The NHSX app uploads the data gathered to a centralised server, in a similar manner to Singapore's TraceTogether app, which launched in March. But just 12% of Singapore's population downloaded the app, in part due to privacy concerns.[10] Some countries, such as Bahrain, have instead introduced compulsory GPS tracking electronic bracelets to track the movements of people who are infected and self-isolating.

While the Isle of Wight trial is ongoing, reports indicate that the NHS might instead partner with Google and Apple to develop a decentralised contact tracing app.[11] The solution proposed by the two tech giants means that all data gathered via Bluetooth would be stored locally on people's phones rather than government servers and would be automatically erased every 15 minutes after alerts have been sent to those potentially exposed to the virus.

But it would still require considerable public uptake to succeed. Based on figures released in 2019, 21% of the UK population do not own a smartphone, meaning that 76% of all smartphone users would need to participate to meet the 60% efficacy threshold.

Legislation needed

The Ada Lovelace Institute, an independent research body looking at data and artificial intelligence, thinks that primary legislation could increase public trust in the use of their data in crisis scenarios. Such legislation would enforce the deletion of all personal information used by the government or private sector partners when the crisis has passed. This would help reassure the public that engagement with such apps will not lead to permanent surveillance

If people share their health status for the purpose of contact tracing, could these data later be required by employers, for example, or by private sector outlets, asks Carly Kind, director of the Ada Lovelace Institute. "Is it possible that, at some point, delivery services will require that you disclose your covid-19 immunity status before you're able to place an order? How do we make sure that we don't allow that kind of creeping scope for health data to be shared beyond the strictest purpose necessary? We think primary legislation would be one way to do that."

One idea is the creation of data trusts to govern how data are used and accessed during public emergencies. These would be managed by independent non-governmental organisations under a strict and legally binding charter. The Open Data Institute—which has conducted government funded studies into whether access to data can increase while retaining public trust—says that any trustees would have legally binding responsibilities to make decisions aligned with the purpose of the data trust.[12] Kind thinks this could be a way of ensuring that patient data are used only for the public good, and the current crisis could accelerate the use of these trusts.

"It doesn't always have to be a trade-off between privacy and safety," she says. "There are now ways of facilitating data sharing with lots of protections in place, so when information is shared, people can feel confident that it will be handled in the right way."

Competing interests: I have read and understood BMJ policy on declaration of interests and have no relevant interests to declare.

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

1 Kim N. "More scary than coronavirus": South Korea's health alerts expose private lives. *Guardian* 2020 Mar 6. https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives

2 Bostock B. South Korea deploys wristbands to catch people dodging state tracking app. *Business Insider* 2020 Apr 11. https://www.businessinsider.com/south-korea-wristbands-coronavirus-catch-people-dodging-tracking-app-2020-4?r=US&IR=T

3 Ju Y, You M. The outrage effect of personal stake, dread, and moral nature on fine dust risk perception moderated by media use. *Health Commun* 2020;1-11. 10.1080/10410236.2020.1723046 32024391

4 Glover C. China to roll out infrared fever screening cameras on public transport. *Comput Bus Rev* 2020 Mar 31. https://www.cbronline.com/news/china-to-roll-out-temperature-taking-infrared-cameras

5 Kirzinger A, Hamel L, Muñana C, Kearney A, Brodie M. KFF health tracking poll—late April 2020: coronavirus, social distancing, and contact tracing. Kaiser Family Foundation. 2020 Apr 24. https://www.kff.org/global-health-policy/issue-brief/kff-health-tracking-poll-late-april-2020/

6 Hall K. The tech firms getting their hands on NHS patient data to fight coronavirus. The Bureau of Investigative Journalism. 2020. https://www.thebureauinvestigates.com/stories/2020-05-07/the-tech-firms-getting-their-hands-on-nhs-patient-data-to-fight-coronavirus

7 Hern A. Royal Free breached UK data law in 1.6m patient deal with Google's DeepMind.*Guardian* 2017 https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act

8 Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* 2019;10:3069. 10.1038/s41467-019-10933-3 31337762

9 Sample I. NHS contact-tracing app ready for use in three weeks, MPs told. *Guardian* 2020 Apr 28. https://www.theguardian.com/technology/2020/apr/28/nhs-coronavirus-contact-tracing-app-ready-for-use-in-three-weeks-mps-told

10 Lee A. If Bluetooth doesn't work for contact-tracing apps, what will? *Wired* 2020 Apr 17. https://www.wired.co.uk/article/bluetooth-contact-tracing-apps

11 Hern A, Proctor K. UK may ditch NHS contact-tracing app for Apple and Google model. *Guardian* 2020 May 7. https://www.theguardian.com/technology/2020/may/07/uk-may-ditch-nhs-contact-tracing-app-for-apple-and-google-model

12 Open Data Institute. Huge appetite for data trusts, according to new ODI research. 2020 Apr 15. https://theodi.org/article/huge-appetite-for-data-trusts-according-to-new-odi-research/