Privacy is not the problem with the Apple-Google contact-tracing toolkit

Michael Veale
July 1 2020
The Guardian (available at https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights)

In April, Apple and Google announced a partnership. They would take research into how to undertake Bluetooth-powered Covid-19 contact tracing in a privacy-preserving manner, with no central database, and make it available as a toolkit inside their operating systems for public health authority–sanctioned apps. Before they did this, all such apps had effectively been doomed to fail. At least on iPhones, they were crippled by the same baked-in Bluetooth restrictions that stop normal apps secretly tracking you.

The firms' contact-tracing toolkit has been both praised and condemned. Its "decentralised" approach, with no sensitive central database of who-saw-who, has been supported by hundreds of privacy, security and human rights scholars. The concerns are understandable. The history of passports – which were introduced as a seemingly temporary measure during the first world war, but were retained in response to fears about spreading the Spanish flu – shows that pandemics can significantly influence our social infrastructure. And so they should be designed to minimise future misuse.

Through a software update, Apple and Google loosened privacy restrictions enough to allow public health authorities to run decentralised contact-tracing apps, but did not engineer new functionality to let apps send the unique Bluetooth identities of phones they encountered to a central server. Data had to remain secretly on phones: which was not a problem for decentralised systems, but left centralised apps – such as those favoured by France and the tech wing of NHS England, NHSX – continuing to struggle to use Bluetooth.

Reasons for preferring centralised systems differed. NHSX wanted individuals to trigger self-isolation alerts based on self-reported symptoms, and said it needed centralised fraud analysis to weed out the inevitable hypochondriacs and trolls. The French minister for the digital sector, Cédric O, said that self-reporting was a no-no, and instead wanted to use centralisation to try to lower the risk of a particular snooping attack from a tech-savvy neighbour. (This is a risk that can never be fully removed from any Bluetooth contact-tracing system.)

Tensions grew as it became clear that the firms did not intend to engineer a further global change to their operating systems to specifically accommodate these countries. In the French parliament, O stated that it was no coincidence that the UK and France were going against the grain, given that they were "the only two European states with their own nuclear deterrent". However, it is worth noting

that no country, nuclear-armed or not, even attempted to use the first tool of a sovereign nation against the firms — the ability to make binding laws. Instead, they continued the bizarre path, seen in recent years from politicians around the world, of treating these firms like sovereign nations, hoping that they recognised each other's legitimacy and that their "officials" could come to some agreement.

They did not, and the saga of the demise of NHSX's centralised app in a mid-June U-turn is well-documented. NHSX piloted an app relying on fragile workarounds to avoid the privacy restrictions built into operating systems, despite warnings from many outside the project — myself included — that it was likely to encounter problems. In June, the government admitted that its workarounds left its system unacceptably poor at detecting either iPhones or Androids at all.

What can we learn from NHSX's encounter with these tech giants? One key lesson requires distinguishing the problem of privacy from that of platform power. It is possible to be strongly in favour of a decentralised approach, as I am (as a co-developer of the open-source DP-3T system that Apple and Google adapted), while being seriously concerned about the centralised control of computing infrastructure these firms have amassed.

It's commonly said that in the digital world, data is power. This simple view might apply to a company collecting data through an app or a website, such as a supermarket, but doesn't faithfully capture the source of power of the firms controlling the hardware and software platforms these apps and websites run on. Using privacy technologies, such as "federated" or "edge" computing, Apple and Google can understand and intervene in the world, while truthfully saying they never saw anybody's personal data.

Data is just a means to an end, and new, cryptographic tools are emerging that let those firms' same potentially problematic ends be reached without privacy-invasive means. These tools give those controlling and co-ordinating millions or even billions of computers the monopolistic power to analyse or shape communities or countries, or even to change individual behaviour, such as to privately target ads based on their most sensitive data — without any single individual's data leaving their phone. It's not just ad targeting: privacy technologies could spotlight the roads where a protest is planned, the areas or industries likely to harbour undocumented migrants, or the spots in an oppressive country most likely to be illegal LGBT clubs — not personal data, but data with serious consequences nonetheless.

This approach is effectively what underpins the Apple-Google contact-tracing system. It's great for individual privacy, but the kind of infrastructural power it enables should give us sleepless nights. Countries that expect to deal a mortal wound to tech giants by stopping them building data mountains are bulls charging at a red rag. In all the global crises, pandemics and social upheavals that may yet come, those in control of the computers, not those with the largest datasets, have the best visibility and the best – and perhaps the scariest — ability to change the world.

Law should be puncturing and distributing this power, and giving it to individuals, communities and, with appropriate and improved human-rights protections, to governments. To do so, we need new digital rights. Data protection and privacy laws are easily dodged or circumvented by technical assurances of confidentiality: we need something more ambitious to escape the giants' walled gardens.

A "right to repair" would stop planned obsolescence in phones, or firms buying up competitors just to cut them off from the cloud they need to run. A "right to interoperate" would force systems from different providers, including online platforms, to talk to each other in real time, allowing people to leave a social network without leaving their friends. These interventions need strong accompanying oversight to maintain security and privacy, and stop unwanted side-effects or government abuse, such as the outlawing of end-to-end encryption to oppress dissidents and whistle-blowers. It all starts from realising that deflating digital power isn't just about governing data: it's the walls of the underlying systems we have to tear down.

Michael Veale is a lecturer in digital rights and regulation in the faculty of laws, University College London