Contact tracing apps and the law in the COVID-19 epidemic: privacy, protection, politics and power

Lilian Edwards[1]

In the current global pandemic, policy interest has alighted on "contact tracing apps", programs downloaded to smartphones which digitise and speed up long-established manual practices of contact tracing, testing and isolating for control of infection. There has been a flurry of such digital tools proposed all over the world, motivated by early apparent success in countries like South Korea, Singapore and Taiwan[2]. A particular problem with the COVID-19 virus is that it is highly infectious in a period of up to seven days before symptoms show. As a result, contacts cannot arguably be alerted speedily enough by conventional manual tracing, which obviously only starts after symptoms develop. In the UK, NHSX, the recently-conceived digital wing of the NHS, began building an app in early March 2020 and trials began on the Isle of Wight on 5 May[3]. However, despite early plans to have the app out by mid-May, at time of writing no app has yet been rolled out to the general public[4].

Initial enthusiasm for contact tracing apps was tempered by two key worries: privacy and efficacy. In Asia, privacy worries were apparently downplayed, either because of lack of traction in authoritarian regimes or, even in democracies, relatively little history of strong privacy rights. In Europe, privacy considerations were seen however as vital because they might impair trust and confidence and prevent people downloading and using the app. Research had shown that for full efficacy, around 80% of the smart phone owning population had to download and use the app[5] so confidence was vital given assumptions of voluntary not mandated uptake. The use of low energy Bluetooth (BLE) to trace proximity between persons (or actually their phones) as pioneered by Singapore, rather than GPS location, both increased accuracy and reduced privacy worries, but arguably not enough.

The privacy issue became the centre of a heated debate over how to build contact tracing apps; a "centralised" or "decentralised" strategy. In the former, data about infected persons was gathered and stored centrally, with the advantage that it allowed centralised "risk scoring" and hence fewer false alerts to contacts to needlessly isolate, even where, as in the UK, contact tracing was initially based on self-reported symptoms rather than confirmed positive test results[6]. In "decentralised" apps however, minimal data was gathered as proximity data was stored locally on phones rather than made accessible to the state. Mass surveillance beyond the immediate emergency thus looked

---

[1] Professor of Law, Innovation and Society, School of Law, Newcastle University; lilian.edwards@ncl.ac.uk.

[2] The claim that contact tracing apps alone were the foundation of these countries success in fighting the virus has since been widely repelled : see https://www.nature.com/articles/d41586-020-01264-1 .

[3] See https://www.the-scientist.com/news-opinion/uk-launches-trial-of-contact-tracing-app-on-isle-of-wight-67516 ; https://www.bbc.co.uk/news/technology-52532435 .

[4] As of 3 June 2020. During this teething time, the devolved parts of the UK which have control of their own health systems have also gone their own ways. Northern Ireland declared they would build their own app which would be compatible with the decentralised model adopted by the Republic of Ireland (see below) and Scotland has yet to decide if it wants a contact tracing app at all.

[5] See Hinch et al "Effective Configurations of a Digital Contact Tracing App: A report to NHSX", 16 April 2020, link from https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown. The UK, by Ofcom figures, has around 20% population who do not own a smartphone- so this figure becomes around 60% of the total population. In later government pronouncements, this figure mysteriously shrunk to 50%.

[6] Epidemiological advantages such as the identification of recurrent viral "hotspots" were also claimed because more data could be gathered than just pure proximity; however such data can also be delivered voluntarily alongside a decentralised app.

in principle impossible. Unfortunately for the UK, which had been forced by early lack of testing to go for a centralised, self-reported symptoms model, on April 10, Apple and Google in an unprecedented joint move announced they would collaborate to offer a decentralised protocol to states so such apps could be built more efficiently for Android and Apple phones[7]. The soft power of their stranglehold of the smartphone market lead to almost every country in Europe except France, the UK and Norway adopting (or in Germany's case, switching to[8]) the new "Gapple" approach[9].

But did this solve all the problems, even outside the UK? The "Gapple" debate had focused attention on privacy-preserving architectures as technical solutions, at the expense of investigating the wider legal, ethical and social context in which any app would be implemented. It ignored *how* the app would be used, especially given the imperative towards high uptake, combined with known demographics of digital exclusion, poverty and techno-illiteracy among the old. What about those who didn't have smartphones? Would people be compelled to install the app? Who could make them show what notifications they had had? - the state, employers, those who ran spaces like shops or sports stadiums? What groups might suffer most harm and discrimination as a result? Who would provide oversight? In the UK, any such worries tended to be handwaved away with reference to the fact we already had data protection (DP) law. However, many of these worries were covered neither by mandatory DP law nor indeed UK equalities law[10], and issues such as freedom of movement and autonomy only in the most abstract sense by the Human Rights Act 1998 and its "parent" the European Convention on Human Rights.

Accordingly, a team lead by the author drafted a model Bill in early April 2020[11] which sought to propose key legal safeguards not covered by DP law and in a technology neutral way. The five main planks of the Bill were:

1. *Digital exclusion*. No compulsion to own smartphone.
2. *Non-compulsion*. No compulsion to install or use app, or to display data sent to or from the app to any party.
3. *Retention/deletion***.** Personal data collected by apps must be deleted or securely anonymised within 28 days
4. *Oversight* : Coronavirus Safeguarding Commissioner to review safeguards across entirety of COVID-19 emergency laws
5. *Immunity passports*. No discrimination on basis of having, or not having, such a certificate unless justified by and proportionate to a public, legitimate goal.

---

[7] See https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[8] See Reuters https://uk.reuters.com/article/uk-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUKKCN22807X, 26 April 2020.

[9] It should be noted that the decentralised model was pioneered by the European academic DP3-T consortium who were at least partially responsible for the Apple uptake. See https://github.com/DP-3T/documents .

[10] The Equality Act 2020 does not include health, and certainly not contagious disease status , as a protected characteristic. One suggestion of the Coronavirus Safeguards Bill was that COVID-19 status became a protected characteristic : see s 6.

[11] "The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates", lead drafter Lilian Edwards, Professor of Law, Innovation and Society, Newcastle Law School. A team assisted including Michael Veale, Orla Lynskey, Rachel Coldicutt, Nóra Loideain, Frederike Kaltheuner, Marion Oswald, Rossana Ducato, Burkhard Schafer, Elizabeth Renieris, Aileen McHarg and Elettra Bietti. First version April 13, 2020; v 9 May 6 2020. Available at https://osf.io/preprints/lawarxiv/yc6xu/.

Such choices are political and contentious, especially 2 and 5. If social good requires maximum uptake of an app, can coercion be justified? Anecdotally, it seemed those groups already fearful of state surveillance – ethnic minorities, religious groups, those anxious about immigration or self-employed status - were most likely to worry about installing the app; while those already disempowered in the workplace , such as gig workers , were most likely to suffer discrimination if apps were abused. In some jobs, refusing to install or display the app might give employers reason to sack or exclude disliked workers or groups that would otherwise be illegal. Compelling use of the app might fatally impair trust and encourage users to supply false and partial data as well as infringe basic human rights.

The issues became even more controversial as we looked at the future technology of "immunity passports" whose very purpose was to discriminate. Should law not prevent the happenstance implementation of what would be effectively a new digital ID card and internal passport? Our answer, drawn from human rights scrutiny, was not to ban the immunity passport in *toto*, but to turn to legally familiar transparency, legitimacy, necessity and proportionality tests. We felt uncertain in our choices, and it was affirming as actual legislatures such as Australia[12] and Italy[13] began themselves to pass "non-compulsion" clauses.

As of early June 2020, the contact tracing narrative remains unresolved. It is still quite likely that in the UK (and other countries) the uptake necessary to make apps useful will not be achieved, in which case , legal safeguards would at least prevent a damp squib technology from becoming an actively harmful vehicle for discrimination and future mass surveillance. In the UK, despite support from the cross-party Joint Human Rights Committee who drafted their own COVID-19 safeguards Bill[14], the government remains firmly opposed to any new laws[15]. Speculatively, this might be not because of any evil intent but because a parliamentary debate would expose the early failures in testing provision which lead to the centralised app design adopted by NHSX, as well as the later failure after Gapple to reconsider it as, eg, Germany did. Much of this story in the UK at least, has been about what decisions made in political expediency can be justified later, and less about pure jurisprudential debates about the balance between public good and private rights. Framed globally, the story is about how sovereign power in nation states could be diverted by the soft technology power of the two most powerful technology companies on the planet. The story is also not over yet.

---

[12] Enacted in the temporary Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020 ; see now Privacy Amendment (Public Health Contact Information) Act 2020 at https://www.legislation.gov.au/Details/C2020A00044 .

[13] See tweet thread by Silvia de Conca at https://twitter.com/SilviaPetulante/status/1267775151334133760?s=20 . Liberty have also spoken out against coercion , see https://www.theguardian.com/law/2020/apr/26/dont-coerce-public-over-coronavirus-contract-tracing-app-say-campaigners .

[14] See news item and link to draft Bill, 15 May 2020, at https://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/news-parliament-2017/covid-contact-tracing-app-draft-bill-19-21/.

[15] See 22 May 2020, https://www.computerweekly.com/news/252483536/Hancock-to-Harman-No-contact-tracing-privacy-law .