SCL
Society for Computers & Law
The leading educational charity
for the tech law community
www.scl.org

SCL Tea and Tech report:
Ada Lovelace Institute's COVID-19 Rapid Evidence Review: Exit through the App Store?

The Ad Lovelace Institute, whose mission is “to ensure that data and AI work for people and society” has published a rapid review of evidence for “whether, and how, the UK government should use technology to transition from the COVID-19 global public health crisis.”

According to the review, the significant technical limitations, and deep social risks, of digital contact tracing outweigh the value offered to the crisis response.

The tea and tech session discussed the review and the wider implications of a contact tracing app with key contributions from Mark O’Conor and Patricia Shaw.

The main question is how we use technology to assist with a return to work (more) normally. There are a number of preconditions for any app to be successful: you need a device with Bluetooth which excludes quite a lot of people. You need to download an app and then comply with what it tells you to do, and according to the government, so do around 60% of the UK population for it to work.

Any app needs to be understood in the context that it can only augment other measures such as testing. There needs to be a validation system so if you self-certify that you have the virus a health professional confirms that, and also when you do not have it anymore. There is an argument that financial support measures need to be in place if people are stopped from working.

Various other issues were discussed during the meeting. For example, as mentioned above, not everyone has a smartphone – would there be a social and a digital divide? Would people be stigmatised for not signing up – indeed, would they be prosecuted for not signing up? And even if you do have the app and it is found that you gave the virus to other people, could you be prosecuted for that?

It was also discussed whether the app is solving the wrong problem. It is not yet 100% clear how the virus spreads and the right way of stopping it needs to be found. Guidance will need to be provided to employers about how to deal with employees who may have or have had the virus, and this will differ from sector to sector – the requirements for a restaurant are very different to a professional services firm. Questions were raised as to whether these uncertainties are being built into the design of the app.

The implications of a centralised versus decentralised model were also discussed. Germany and Switzerland are reportedly following a decentralised model while the UK and France are following a centralised model. The model chosen affects the storage and purposes of storage, of the data. A centralised model holds more data and would be more vulnerable to a hack. Questions arise as to who would see your social grouping – ie who are you seeing, how often, and for how long? It would be a very powerful dataset, especially when combined with location data. How much data is too much? What goes beyond the data minimisation principle?

The Ada Lovelace report considered the mental health issues – for example if you know from the data who gave you the virus, or to whom you gave it and you know that one of you had it far worse than someone else. Although the data is anonymised, if you move in small circles it could be easy to identify someone.

The distinction between data rights and human rights was also discussed, and the fact that the right to a private life does not necessarily mean the same as a right to privacy. Not all data is personal data and therefore it might not be covered by the GDPR.

Solutions in other countries such as Australia were briefly discussed and it is clear that nobody really has all the answers and it is difficult to balance all the competing issues.

In conclusion: the following key questions need to be posed when considering using tech in any exit strategy:

- There needs to be a very clear understanding of the purposes for which the app will be used.
- There needs to be evidence of its effectiveness.
- Contingencies and preconditions need to be considered.
- There needs to be protection against mission/scope/function creep.
- If the public effectively become used to this and voluntarily relinquish their rights to privacy what is the exit strategy to the exit strategy – that is, when and how do we stop using the app when the public health emergency is over – right away or after some sort of grace period?
- What will happen to the data collected?
- What happens if there is another flare-up in the virus – when/how would measures be reintroduced?