Written evidence from Member of the public (COV0118)

Contact Tracing App

The comments that you made on TV and the report on the tracing app have aligned with my tension over mixed feelings - the advent of a safely managed release from lockdown version the concern of overlooked weaknesses in a speedily developed and launched app.

My background covers anti-fraud and data breaches including in the telecommunications sector. I would not call myself an expert but have experience that underpins my thinking, coupled with an aviation safety background where we question where there is doubt.

1. You raise a crucial point about the collection of data, in whatever form, and its use for the current COVID purpose as well as any potential future use.
2. My concern is where the data is stored - solely on UK servers, within the EU which is a similar standard under GDPR, or more widely such as the US where there are lower standards? Once outside of the UK, applying our data rights becomes harder with some apps declaring foreign legal jurisdictions; one uses the courts in Fulton County in the US State of Georgia!.
3. Whilst I could argue that the collection of the data is a legitimate national security and/or law enforcement purpose under DPA18, I fail to see any reason beyond statistical purposes for its retention beyond the pandemic and clearing up. We need to be completely and simply transparent on current and future use with clear opt-in/out.
4. I have a concern that there will be a move to monetise the data, perhaps by selling to pharma and other companies overseas, thereby likely breaching DPA18 and HRA98 principles.
5. It has been stated that the app has been approved as secure by JCSC but the potential weakness is that when we open Bluetooth, we open a door that anybody can try enter so an opportunity that fraudsters will try exploit through any Bluetooth enabled app on board a device.
6. When using Bluetooth, we often use generic devices where a common password is use to start; in some cases it cannot be changed at all. This offers parallel routes to access the device.
7. I am unclear of what part the location service on a device will be used. We use that for a wide range applications - supermarket queues during COVID, star gazing, and exercises monitoring. There is a well known example of US military personnel punding the perimiter of their base leaving a very clear circuit as well as times of use as a public record until they were forced to go dark and change their routes.
8. When rolling out GDPR with schools, I used to switch my Bluetooth then run through the device I could see - often embarrassment but point clealry made. On one occasion, a teacher told of a couple he knew who were out cycling when their garage was broken into and a haul of around £25,000 of bikes and equipment was stolen because they were being tracked on their exercise app.
9. What will the public habit be when using the app - walking around with a device in our hands? If so, will that lead to a rise in theft and subsequent fraud, the risk of data harm being greater as the device will likely be unlocked.

10. Overall device and personal security needs to be rethought, not as a panic but rather a case of reviewing and ensuring the least risks through sensible actions.
11. Opening a Bluetooth connection uses more power and slows other services down on a device. The plan is a fail if the vital service cannot be accessed due to battery drain and no place to recharge when out.
12. What other risks are we exposed to across a wide range of devices, operating systems, applications and more?

I've committed a range of thoughts, some outside the likely remit of JCHR, but have tried to take a holistic view of what needs to be considered in order to bring the population on board and trust the app which has a real purpose for the benefit of all.

Thanks for what you and JCHR are doing in a challenging time.

29/05/2020