Written evidence from Professor Lilian Edwards (COV0121)

I would like to formally submit as evidence the *Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates* (hereafter CSB).

The CSB is periodically updated and the permanent link is at https://osf.io/preprints/lawarxiv/yc6xu/

Although the CSB is primarily aimed at dealing with contact tracing apps, it also refers to symptom trackers and to what may be to come in the form of immunity certificates (or "passports"). I was assisted in drafting this by a number of people who are indicated under Other Contributors. I was however the main drafter and had final responsibility for the contents.

The CSB was designed to raise awareness and clearly does not conform to full Parliamentary style, unlike the draft Bill prepared for the JCHR. However, it has raised considerable interest and the key provision on non-coercion (section 3) has influenced strongly the Australian legislation attached to their app (now the Privacy Amendment (Public Health Contact Information) Bill 2020). The Council of Europe also commented favourably on it.

I would draw the Committee's attention to several points I do not feel are adequately addressed by the JCHR's own bill

A. Key provisions missing from the JCHR Bill

1. **No compulsion to own smartphone (s 1 of CSB)** . No one shall be penalised for not having a phone (or other device), leaving house without a phone, failing to charge phone, turning off Bluetooth, etc.

   This prevents any attempts to penalise those who are economically disempowered, less techno-literate or digitally excluded. There seems no good reason not to include this as a safeguard given basic norms of autonomy and bodily privacy and indeed the government has guaranteed such voluntary uptake: I think it is therefore useful to improve trust and confidence without any loss to public good.

2. **No compulsion to install or use app (s 3 of CSB)**. No one shall be compelled to install a symptom and contact tracing app, or to share messages of their status on such an app on request (eg to an employer or insurer or university) ("non-coercion" principle).

   I realise this is a contentious provision given the obvious aim of COVID-19 apps to protect both the public and other private interests eg the interest of employers or shop owners in having safe workplaces or premises. However, installing the app is not a proxy for good health, and there is a danger it may be perceived this way. It works for the greater good not for the immediate good of the user. Indeed, the person who installs may well never hear any more after installation. From the UK scheme as currently described (28/5/20) it seems more likely a contact may receive guidance to isolate from a manual tracer than from the app itself. There is also likely to be a great margin for error in such notifications, given their origin in self reported symptoms as opposed to confirmed tests, leaving room for individual consideration of whether to isolate. There are worries about malice and fraud eg reporting symptoms so as to get a workplace or school closed down. Taking all these factors into account, coercion to install, use or display messages on the app may serve relatively little advantage to an individual or society, but open up the possibility of covert discrimination eg against employers who want to take the opportunity to discriminate against certain individuals or classes of employees.

   There seems complete uncertainty that employment law will safely protect against this, especially for those who are contractors rather than employees, as in some gig economy jobs.

This is not an abstract worry : I have already heard of several employers including government departments seeking advice on exactly this point. Furthermore, since the government is committed to trying to get uptake of the app to 50% of the population, there may be covert (or indeed overt) pressure on both public and private sector employers and service providers to make such requirements.

Furthermore, there is opportunity for ethnic or other group discrimination buried in any attempt at compulsion. Some groups are more likely than others to resist using the app, for what may seem to them good reason even if the objective truth is different. Ethnic Asian or Muslim groups may fear that they are in some way being surveilled as associates to terrorism , or may fear prejudice to immigration status. The same may be true of the poorest self-employed. There may also be religious groups unwilling to interact with a UK government app. These beliefs may be erroneous but that does not mean they should enable discrimination.

It is also worth noting that the Royal Society have issued a report suggesting that public unwillingness to engage with an app can best be met by incentives, rather than compulsions or exclusions.

Overall therefore it seems vital to remove the possibility for both private and public actors to mandate installation of the app, and worse still, display of its messages to any party other than a public health sector worker, as a condition for access to services, premises, public spaces and especially, workplaces. This was also the choice made by the Australian Act. It is possible to provide as a backstop that the Secretary of State can allow for specific exceptions to this prohibition, by means of delegated legislation which gives opportunity for debate..

3. **Immunity certificates or passports** (section 6 of CSB). The JCHR may understandably have felt that these were too far in the future and uncertain for legislation. However, the government has repeatedly indicated, sometimes rather casually, that these are likely to come and other countries are already, *pace* the absence of hard science, making use of them. Since the entire purpose of an immunity certificate is to discriminate, it seems valuable to put in place top level principles trying to regulate such discrimination, in ways that are conform to human rights principles. The Bill suggests a test whereby the use of an immunity certificate to exclude or discriminate should always be justified by, familiar transparency, legitimacy, necessity and proportionality tests. Furthermore, it suggests in particular that only police or their equivalent should be able to demand sight of an immunity certificate to prevent movement within the UK. This prevents use of the certificate as a proxy privatised internal passport, something the UK has never seen as legitimate. I suggest it would be worth enshrining in law such top level principles sooner rather than later.

B. Overlap with data protection law

Much of the JCHR Bill in essence replicates GDPR and DPA2018 law (security, repurposing, reidentification, etc) ut with greater specificity to the particular case of contact tracing apps. This is a reasonable choice (though s 9(5), in particular, seems redundant). My own view however was that it was better to accept the GDPR (etc) as a given and merely legislate where gaps existed outside that law (coercion, discrimination, freedom of movement) plus suggest points where protection *greater* than standard DP was required.

I would note three points where I feel the JCHR Bill could be improved

(i) **Consent.** There is no reference to the standard of consent as defined in GDPR (see art 4(11)). This effectively reduces protection below not above the level of the GDPR,

especially in relationships where DP law regards consent as intrinsically invalid because of imbalance of power and hence not "freely given". This is especially true of the employment relationship but possibly also of the relationship between individual and state.

(ii) **Retention .** Section 12 of the JCHR Bill in essence takes us no further than existing DP law which already provides that data must be deleted or anonymized as soon as the purposes of processing are fulfilled. Yet, in reality, this may mean indefinite retention. It is interesting to note that the privacy notice recently released for the *manual* contact tracing and tracking regime in fact says that personal data (though it is called "PII") may be retained for 20 years. This seems far too long for such sensitive data and is hard to see how it can be justified even on grounds of research. Other countries such as New Zealand have sought to distinguish between data needed to deal with current infections in identified form, where the appropriate period of retention is 21-28 days, and data to be held for research purposes where anonymization should be necessary after that shorter period. The JCHR refers to anonymisation "as soon as is practicable after it is obtained" but again this might conceivably be a very long and disproportionate time. I would suggest that the "arrangements" section be reviewed to provide much tighter and more relevant controls, in consultation with health experts. In particular a definite "sunset clause" after which all data collected in the emergency situation should be deleted or stringently anonymized should be declared.

(iii) **Oversight**. Like my Bill, the JCHR Bill takes the view that a new regulator is appropriate, the Digital Contact Tracing Human Rights Commissioner. However, the remit of the new Commissioner is very narrow indeed. It does not extend to future immunity certificates, nor to symptom trackers, nor even to manual tracking and tracing databases or dashboards, such as the one being prepared by Palantir. Given the newer governmental emphasis on an integrated strategy in which the app plays a relatively minor part, it seems odd to think the app alone requires a new regulator. On the other hand, the new regulator only has exactly the same powers as the existing ICO, but less experience and (presumably) resources and trained staff. Again therefore it is hard to see quite what the gain is. I think this needs a wider debate and reconsideration of what powers would be useful and what scope. My own suggestion is that the new Commissioner, should in general take a watching brief on all COVID-19 tracking and data mining schemes.

28/05/2020