Opening Remarks From Academics Briefing Minister on 2ⁿᵈ May 2020.

We understand the severity of the situation and the toll this is taking in lives and economic damage. We want the public health efforts to succeed. We are not saying that contact tracing does not have a place in this effort: it's not a case of privacy at any price. However, it's essential people trust this app, if only so that enough people use it to make it effective.

We have the somewhat thankless role of pointing out risks: a duty to warn, if you like, unless we know privacy is being protected proportionately. Often in our field a good result is only indirectly apparent through the absence of negative consequences. But, we live in a post-Snowden world where our experience shows that the public always prefer privacy by design over being asked to implicitly trust a central authority be that government or commercial organisation.

So:

1. We need to understand the balance that has been drawn between the privacy risks we all know are inherent in the centralised model and the public health benefits so that we can judge if we feel that it is appropriate. Please understand that despite the UK government having promised transparency there has been none in this area, and that very lack of transparency has caused people to question whether anyone has truly factored in the privacy risks. This concern is exacerbated as many of our continental colleagues, who have been fully transparent in their designs, are saying that they have done the calculation and decided on the decentralised route, which relies upon privacy by design, not having to trust a central authority. We are left wondering what additional public health benefits will the UK receive that our German, Austrian, Latvian, Estonian, Finish, and Irish cousins will not, and specifically is that difference worth the extra risk to privacy.

2. Collecting the level of data sought by the centralised model could be a slippery slope to surveillance - how can we be sure that the data will be used only for controlling the

pandemic, will be deleted when no longer required, and cannot be deanonymised to, for example, build contact maps. Will the UK government undertake to put in place the transparency, legislation, oversight that is necessary to protect this level of personal data collection? Without this how can we be sure that this sort of tracking will not become the new normal for other notifiable diseases where everybody had to have the app in perpetuity, which then leads to the obvious risk of general state tracking.

3. How will any extra data being collected such as the optionally requested age, general, ethnicity, be kept separate from the core app data in order to prevent the obvious risk this poses for making deanonymisation easier.

4. And finally, will you make the technical detail of the NHSX app public, and the DPIA, before going live with the app so that the privacy and security community have enough time to scrutinise, and feedback any concerns.