Supplementary evidence from the Information Commissioner's Office (COV0099)

Thank you for the opportunity to give evidence to your Committee on 4 May. The subsequent report produced by the Committee is timely and I welcome the spotlight it has placed on protecting privacy and data protection by design for the contact tracing app.

Given the focus in the report on oversight and enforcement I wish to provide some further information and clarify my advisory and enforcement functions, the importance of both, and how they interact.

The ex-ante and ex-poste responsibilities of any regulator are integral to the effective regulation of both the development and deployment of innovative products or services. In such circumstances regulators need to strike a fine balance between enabling innovation in the public interest and protecting the public from the potential harm which poorly informed innovation may intentionally or inadvertently cause.

Both the GDPR and the Data Protection Act 2018 provide these functions to the ICO and they operate in a complementary manner. Early advice will help organisations address risk and get data protection and privacy protections 'right first time', whilst decision making on compliance still rests with the organisation as the controller under data protection law. The public can also have confidence that the ICO has strong powers to address complaints and concerns after data usage has occurred.

It is common for regulators to have both these early stage advisory and engagement functions alongside enforcement. The Financial Conduct Authority (FCA) is just one example in addition to the ICO. Both the FCA and ICO provide regulatory sandboxes - providing advice within a clear regulatory framework and still preserving the ability to take regulatory action should organisations go on to fail to comply with the law.

The report at page 12 states:

"To guard against mission creep it cannot be left to the Information Commissioner's Office to be the only body with powers of oversight or sanction; such an Office is not designed to monitor the significant rights-based implications that app based surveillance raises and, in addition, the Information Commissioner has been involved in the development of the app".

I would like to correct this statement contained in the report. My evidence to the Committee made clear that my office has not been involved in the development of the app. I mentioned this at a number of places in my evidence, but the most relevant quote is:

"We consider ourselves to be the independent body because we are not sitting at the design table. We have been given some technical material, and we have

looked at it. We expect to look at the data protection impact assessment, which is the key document for us to critique and comment on. We also expect to monitor how the public respond to the app when it is rolled out. We will take complaints and do investigations and audits, but it is also really helpful that NHSX wants to talk to the independent regulator at the design phase to make sure that privacy and security are built in. However, we are not across every document and every plan about what is coming next. We can play both the expert adviser and the enforcer."

At the time of my evidence my office had yet to see the Data Protection Impact Assessment (DPIA) completed for the Isle of Wight trial, or indeed to have seen the app itself.

My office continues to discharge its duties set out in law; giving advice on data protection regulatory compliance to make sure those developing the app are clear about the standards set out in law and the standards we, as the regulator expect. We have offered advice, as I believe would any regulator in a similar position, and we consider this to be both appropriate and good regulatory practice.

Through the clear governance systems and processes underpinning the way our regulatory advice is provided, we retain independence as a regulator in order to make appropriate decisions around audit, investigation and enforcement as roll out of the app moves forward. Through this approach, we are seeking to maximise the opportunity for new and innovative technology to be developed in ways which comply with data protection law, but we are also reserving and preserving our ability to take regulatory action should relevant compliance standards fail to be met.

I hope this information is helpful to the Committee. If you have any further questions, please do not hesitate to get in touch.

11/05/2020