Written evidence from Dr Audrey Guinchard, School of Law, University of Essex and Dr Subhajit Basu, School of Law, University of Leeds

We are writing as two academics working in the fields of data protection law and regulation of emerging technologies. Dr Audrey Guinchard is a Senior Lecturer (Law), the University of Essex and Dr Subhajit Basu is an Associate Professor (Law) at University of Leeds and Chair of BILETA. Dr Guinchard latest paper has focused on DeepMind, now absorbed by Google Health UK. Dr Basu is co-author of the critically acclaimed book Privacy and Healthcare Data: Choice of Control to Choice and Control. Routledge, 2016)

Our submission focuses on answering the first question: 'What steps need to be taken to ensure that measures taken by the Government to address the COVID-19 pandemic are human rights compliant?'

Summary of proposed steps:

1. The Government needs to publish its reasoning as to how the high risks to human rights have been assessed and whether or not they could be mitigated (potential issue 1.1). This reasoning is a prior condition to assess the need for prior consultation of the ICO (issue 1.2). It is also the basis for arguing that the publication of the DPIAs is needed to foster transparency as the GDPR mandates, and trust of the general public as Government aspires (issue 1.3).

2. The Government needs to look beyond the seven data protection principles referred to by the Committee in its report HC 343/HL19, namely: Articles 28, 35 and 36 GDPR.

   The Government needs to ensure that the collaboration between NHS X and its private partners has adequate structures and processes to ensure that the processing is compliant and does not violate the GDPR and human rights (see potential issue 2).

   In the longer term, the Government would benefit from revisiting the collaboration procedures in place to ensure that the decisions taken along the way do not focus solely on the functionality of the digital product. The decisions also need to anticipate compliance with data protection laws beyond the seven data protection principles.

3. Beyond the pandemic, the Government should look at how the ICO could be restructured and how a framework could be developed for more formal dialogue between public authorities and the ICO concerning the development and use of digital technologies (issue 3).

4. Finally, the Government should consider how it could weave more efficiently the digital technologies into its management of public health beyond Covid-19 app. It may want to consider a public consultation leading to a White paper. (issue 4)

Introduction – Our focus and objectives

We are not opposed to the 'contact tracing app' or the collaboration between the public and private sectors. Our focus is to improve the environment in which this app is being developed. The lack of details unwittingly creates a climate of secrecy which is not conducive for this app to be perceived by the public as trustworthy, workable and useful.

In this submission, we are not repeating what has been discussed; instead, we want to add to the existing discussions, bringing to the Committee new perspectives on the current debate about the Covid-19 app and beyond this pandemic. These additional points can be addressed by relying on the existing legal framework: the GDPR and the Human Rights Act 1998.

We think that the Covid-19 issues are not specific to the pandemic. Some of the problems reflect the recurring challenges that the NHS faces for the development and use of digital technologies. Consequently, in the medium and longer terms, - not just for Covid-19 app-, we believe that some possible reforms, not yet discussed before the Committee, could improve the enforcement of the GDPR in connection with human rights.

<u>Potential issue 1</u> – Identifying potential serious violations of human rights – Cascading effects

1.1 – What are the possible high risks to human rights?

The collaboration involves the processing of sensitive personal data, i.e. health data, which on principle cannot be processed (Article 9(1) GDPR) unless specific grounds apply (Article 9(2) GDPR). The legal grounds exist and have been explained.[1] We do not want to go back on this discussion. However, we want to remind the Committee that the processing remains an exception and that, as all exceptions in the law, it calls for a restrictive interpretation that

[1] Article 9 GDPR see ICO, *Guidance on GDPR*, accessed 14 May 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

colours the balance of human rights inherent to the GDPR (Recital 4) and conducted in light of the Human Rights Act 1998.

The exact impact on human rights is difficult to predict at this stage, for lack of details. So far, the discussion seems to focus disproportionately on security breaches and their human rights implications. As Levy identified, not all scenarios can be identified from that angle.[2] Nevertheless, some infringements can already be foreseen, beyond the apparent effect on the right to privacy and the right to health.

For example, some members of the French university institute of INRIA have published a short document, for the general public to read, wanting to raise awareness on a serious potential issue of discrimination.[3] The scenario they put forward is as follow. The lockdown has eased, employer interviews three different individuals, hiding for each a smartphone with the digital contact tracing app on. Each interviewee has the app; one tests positive for Covid-19; the interviewer receives a notification. Will, the interviewer, decide that hiring the interviewee is not worth the risk, or on the contrary, in the (false?) belief that herd immunity can be built on, it will favour the interviewee who has had Covid-19, as employers and slave owners used to do for those who contracted 'yellow fever' in 19th century New Orleans?[4] Whichever decision the modern employer will take, how will the interviewees know whether or not the positive or negative testing for Covid-19 influenced the decision? The potential discrimination is likely to remain invisible.

Our questions/comments

- Because the processing of health data remains an exception, have NHS X and its partners considered how this perspective affects the balance of human rights?
- Have violations of human rights, such as the one highlighted in the scenario above, been considered?

1.2 – The high risks' cascading effect on the need for prior consultation

The Data Protection Impact Assessments (DPIAs) are the main legal tool to assess the processing's human rights implications. Two points need to be considered.

1. The prior consultation of the supervisory authority is not required unless the controller cannot mitigate the high risks. The ICO indicated indeed that prior consultation for the Covid-19 app was not needed. Nevertheless, NHS X informally asked the ICO to review the DPIA 'for the Isle of Wight trial and for a national rollout.'[5]

The level of high risks to human rights involved is beyond any doubt. Whether they can be mitigated is a different matter. In the scenario above in issue 1, we cannot see how the high

---

[2]Ian Levy, "NCSC. The security behind the NHS contact tracing app," (May 4, 2020). https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

[3] (in French) Xavier Bonnetain, "Le traçage anonyme, dangereux oxymore. Analyse de risques à destination des non-spécialistes (website)," 23 April 2020 , https://risques-tracage.fr. The team is from INRIA which the same university research centre (but not the same team) that participated to the PEPP-PT research.

[4] Kathryn Olivarius, "The Dangerous History of Immunoprivilege," *The New York Times*, April 12, 2020, https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html.

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/dpia-for-the-nhsx-s-trial-of-contact-tracing-app/.

risk can be mitigated unless the user switches Bluetooth off, which defeats the very purpose of the app.

Comment. Consequently, we find it difficult to accept the assessment of both the ICO and NHS X that all high risks can be mitigated and thus, we consider that the prior consultation of the ICO is mandatory.

2. Furthermore, we would like to bring to the Committee's attention Article 36(5) GDPR which allows a Member State to require 'prior consultation and obtain prior authorisation from the supervisory authority […] including [when the] processing [is] in relation to social protection and public health.' This gives the legal basis for the Government to require more stringent measures for Covid-19 app and would benefit the management of public health beyond the pandemic.

1.3 – The high risks' cascading effect on the publication of the DPIA

Neither the GDPR nor the Data Protection Act 2018 requires the publication of the DPIAs to the general public. Not publishing them goes against the stated objective of fostering trust as there is no way in knowing which risks have been contemplated, whether they could be mitigated, and if so, how they have been addressed.

Given that the Government wants 60% at least of the population to download and use the app, the degree of transparency needs to be greater than the letter of the law mandates. It is our view that NHS X needs to provide this explanation.

This was the approach of Taunton and Somerset NHS Trust for the project of the Streams app in collaboration with DeepMind, now subsidiary of Google Inc. In order to foster the trust of its patients in the future app, Taunton decided to publish their DPIAs and provided information on the DPIA in a non-technical language.[6]

Our question:

- Given the need to foster trust, why the publication of the DPIAs, to the general public, not just to the ICO, is not considered as a necessary element?

<u>Potential issue 2</u> – Governance of the collaboration – Building a culture of compliance

Compliance with the GDPR and Human Rights does not stem solely from respecting the seven data protection principles. It depends on a broader culture of compliance reflected in other sections of the GDPR.

[6] Guinchard, Audrey, Basu, Subhajit "Restoring Trust into the NHS: promoting data protection as an 'architecture of custody' for the sharing of data in direct care" (February 5, 2020). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589551

2.1 Processes and structures

NHS X indicated it works notably (but not exclusively) with Microsoft, Google, Palantir, Amazon Web Services and Faculty AI,[7] VMware Pivotal Labs, Zurla, and the BBC.[8] This collaboration needs to respect the rules set out in the GDPR, notably Article 28 GDPR. Controllers (NHS X) have to choose processors (the companies which act on behalf of NHS X) who can demonstrate compliance with data protection by design (Article 28(1) GDPR); if the processors' track record does not give full confidence, and controllers choose these processors, then they have to ensure that all safeguards will be put in place for processors to be fully compliant.[9] Furthermore, processors have the duty to assist controllers in fulfilling their obligations, with an expectation to be pro-active (Article 28(3) GDPR), instead of being passive recipients of the controllers' instructions as before the GDPR.[10]

The implementation of the GDPR by some of the companies NHS X has chosen has been recently challenged either formally, by a data protection regulator,[11] or informally by academic scientists.[12] Their initial challenges could increase the difficulties inherent to collaboration as well as the chances to have more blind spots.

The law, therefore, raises the following questions:

- For the processors which compliance had recently been challenged, have questions been asked by NHS X or ICO about the changes they would have had to introduce to respond to criticisms?

---

[7] Matthew Gould, Indra Joshi, and Ming Tang, "The power of data in a pandemic," (March 28, 2020). https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/. Matthew Gould ; House of Commons Science and Technoogy Committee, "Oral evidence: UK Science, Research and Technology Capability and Influence in Global Disease Outbreaks," HC 136. Questions 302-384;

[8] House of Commons Science and Technoogy Committee, "Oral evidence: UK Science, Research and Technology Capability and Influence in Global Disease Outbreaks," HC 136. Questions 302-384

[9] EDPS, "EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725."

[10] As clearly explained by the ICO https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

[11] (in English) CNIL, "Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.," (January 21, 2019). https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.; Google was investigated by the CNIL, upon request by Article 29 WP, Letter of 16 October 2012 on Article 29 WP website (now archived) and was found non-compliant; NYOB, May 13, 2020, https://noyb.eu/en/complaint-filed-against-google-tracking-id; ; regarding the subsidiary DeepMind, ICO Letter on the investigation, July 3, 2017 https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf;' regarding the merger with Fitbit, EDPB, "Eighteenth EDPB Plenary Session," (February 20, 2020). https://edpb.europa.eu/news/news/2020/eighteenth-edpb-plenary-session_en.
For Microsoft: a summary by those who audited the firm is available at Privacy Company, "New DPIA on Microsoft Office and Windows software: still privacy risks remaining (long blog)," (July 29, 2019). https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-long-blog. The full reports in English and in Dutch are published, https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise; at EU level: EDPB, "EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals" October 21, 2019, https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en

[12] Marisa Franco, "Palantir has no place at Berkeley: they help tear immigrant families apart," *The Guardian*, May 31, 2019, https://www.theguardian.com/commentisfree/2019/may/31/palantir-berkeley-immigrant-families-apart

- Which processes have shown the willingness to put in place structures for compliance specifically with Article 28 GDPR? For example, which processes exist that allow for each processor to raise the alarm 'if in [their] opinion, an instruction [from the controller NHS X] infringes [the GDPR]' with regard to their duty to 'make available to the controller all information necessary to demonstrate compliance […] and allow and contribute to audits' (Article 28(3) & (3)(h) GDPR)? By comparison, NHS X has in its Ethics Advisory Board, two professors of law, with different and complementary expertise that can raise different human rights issues.[13]
- What processes are in place that ensures NHS X has communicated its instructions clearly, that they have been followed and will continue to be followed until further notice?

In the longer term, these questions need to be considered for all collaborations between the public and private sectors. The draft NHS Digital Health Technology Standard of February 2020 could be a starting point to develop a strategy to foster an environment where these questions are considered.

2.2 - Transparency about the collaboration for the Covid-19 app

NHS X has not explained the criteria used for choosing the companies, other than having previous experience of working with some of them,[14] despite the potential implications on human rights. It had not explained either the safeguards it needs to put in place. [15]

The GDPR requires this explanation from NHS X to the ICO, but not to the general public.

The Government wants 60% at least of the population to download and use the app. Therefore, we argue that the current situation demands more transparency than the letter of the law mandates. Transparency is a legal requirement under Article 5(1)(a) GDPR. The spirit of this requirement militates for a wider application than otherwise mandated in order to bring trust in Government.

Our question:

- What are the reasons for NHS X not to provide this explanation?

[13] Deepmind dismantled its ethics advisory board upon merger with Google.
[14] House of Commons Science and Technoogy Committee, "Oral evidence: UK Science, Research and Technology Capability and Influence in Global Disease Outbreaks," HC 136. Questions 302-384.
[15] NHS X stated that no sharing of data will take place with the private sector or with the Home Office, House of Commons Science and Technoogy Committee, "Oral evidence: UK Science, Research and Technology Capability and Influence in Global Disease Outbreaks,"NHC 136, Q 378, 382.

Potential issues beyond the pandemic

This process of developing the Covid-19 app brings to pre-existing light issues. Now is the right to tackle them.

<u>Potential issue 3</u> – Supporting the ICO

The Committee raised questions about the role played by the ICO for the Covid-19 app and more generally as per its 2019 report on *The Right to Privacy (Article 8) and the Digital Revolution.*[16]

Indeed, insufficient enforcement leaves a vacuum, where others are forced to take decisions which are not within their role[17] and which they do not necessarily want to take, as Microsoft made it clear for facial recognition.[18]

Short communications, often without reasoning, raise more questions than bring answers, fuelling suspicion that the protection accorded to the users is insufficient. The Covid-19 situation highlights this practice of short, non-specific, communication style.

The proposal for an independent monitoring body may be adequate for the Covid-19 app, but will not bring sufficient support to the ICO in meeting the challenges it faces on a daily basis and which are emphasised during the pandemic.

Our suggestions:

Three avenues could be explored:

- The Financial Conduct Authority, which monetary penalties are similar to those of the ICO, has three internal divisions: advisory, investigatory, and decision-making. Adopting a similar structure would go a long way to avoid real or perceived conflicts of interest. Justice needs to be done as much as seen to be done.
- Formally recognising a right for public authorities to consult the ICO, with an obligation for the ICO to publish the ensuing opinion, would also help prevent future issues related to human rights. For example, the French data protection legislation gave the legal power for public authorities to seek advice from the French regulator, the CNIL. This power was used for the French Covid-19 app, also based on a centralised approach, and the CNIL published its opinion, with reserves, on 24 April 2020.[19]

---

[16] Joint Committee on Human Rights The Right to Privacy (Article 8) and the Digital Revolution, Third Report of Session, October 2019, see also Guinchard, Audrey, Basu, Subhajit Restoring Trust into the NHS: promoting data protection as an 'architecture of custody' for the sharing of data in direct care (February 5, 2020). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589551.

[17] Ada Lovelace Institute, "Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis." 10;

[18] Microsoft called for regulation of facial recognition, Joseph Menn, "Microsoft turned down facial-recognition sales on human rights concerns," *UK Reuters*, April 17, 2019, https://uk.reuters.com/article/uk-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUKKCN1RS2FY. Brad Smith, "Facial recognition: It's time for action," *Microsoft*, December 6, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.

[19] The French app uses a centralised approach as the UK one, CNIL, "Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid »," (April 24, 2020), French only

- The balance between issuing a short statement or blog post, and providing a longer more reasoned opinion, could be reviewed and clear criteria established for good practice in using one or the other or both.

Potential Issue 4 – 'Exercise Cygnus'

Exercise Cygnus conducted in October 2016 involved all major departments (including NHS), and local authorities across Britain. As we understand, it showed gaping holes in terms of preparedness, resilience and response plans. The report published by the Guardian (not yet confirmed or denied by the Department of Health) does not seem to mention the use of digital technologies. The capability to create digital contact tracing apps already existed in 2016; the NHS was already considering apps for some specific direct care issues as part of its strategy to enhance care.[20] This raises the question as to why the use of digital apps to support the response to the exercise was discussed.

Our question

- Why in 2016 were the digital technologies not considered? To have done so would have increased government capability to respond and save lives. It would have given public authorities the time to consider complex issues of human rights without the pressure of an unfolding real-time pandemic. For example, they could have considered the potential for discrimination resulting from false positives created by the use of apps.[21]
- Should the Government consider a public consultation leading to a White paper to explore the development and use of digital technologies as part of its public health management strategy?

21/05/2020

---

https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_d application_mobile_stopcovid.pdf.

[20] Deepmind NHS digital; NDG and ICO were not opposed to the use of the technology but were critical of the approach taken.

[21] Isle of Wight trial; The project was announced on 18 March 2020; the live testing started on 5 May 2020. Andrea Downey, "NHSX working on coronavirus contact tracking app," *Digital Health*, March 20, 2020, https://www.digitalhealth.net/2020/03/nhsx-coronavirus-contact-tracking-app/.; Department of Health and Social Care, "Coronavirus test, track and trace plan launched on Isle of Wight," news release, May 4, 2020, https://www.gov.uk/government/news/coronavirus-test-track-and-trace-plan-launched-on-isle-of-wight?utm_source=a173ba14-521f-4a3e-9d0a-78113de8d648&utm_medium=email&utm_campaign=govuk-notifications&utm_content=daily