Supplementary Written Evidence from Dr Orla Lynskey, *Department of Law, London School of Economics, and* Dr Michael Veale, *Faculty of Laws, University College London* (COV0093)

Introduction

We are writing as two academics in the fields of data and privacy law to provide the Committee with written evidence to supplement, specify and extend the oral evidence we gave on 4th May 2020. Dr Orla Lynskey is an Associate Professor at the London School of Economics, and Dr Michael Veale is a Lecturer at University College London. Dr Michael Veale is one of the co-authors of the DP-3T decentralised Bluetooth contact tracing protocol which the Apple-Google system is based upon, and which is being deployed in countries including Switzerland, Austria, Estonia, Latvia and Germany.

Our evidence below focuses primarily on the application of existing UK law, and the potential role of UK regulators. We consider which systems are less vulnerable to abuse and mission creep in the UK context.

However, it is important to note that *all* applications (e.g. centralised or decentralised) are vulnerable to abuses of power, for instance, irrespective of the particular application used individuals may be compelled to produce their device by employers; immigration officers, or even private service providers such as restaurants.[1] These problems are inherent to any system that provides individuals, centrally or locally, with a risk score. In other work, led by Professor Lilian Edwards, we have contributed to a draft *Coronavirus (Safeguards) Bill* which we point the committee to as a foundation for legislation governing more than just data protection and privacy in this area.[2]

Centralisation

There is a considerable body of weight lending support to a decentralised model over a centralised system. Article 25 GDPR poses an obligation on controllers to design systems in a way that integrates the data protection principles in an effective manner, in particular the principle of data minimisation. The Council of Europe has clearly stated that applications should be 'based on an architecture which relies as much as possible on processing and storing of data on devices of users'.[3] Senior legal practitioners have stated that the development of this capacity would constitute 'a significant and unprecedented step in the government's surveillance of the public'.[4] The ICO has noted that the 'starting point for contact tracing should be decentralised systems that look to shift processing on to individuals' devices'. Furthermore, they note that 'pseudonymous identifiers should be generated on the device if possible'. Identifiers in a centralised system are typically generated on

[1] See, for instance, The Australian, 'No App? Leave your name and number', 4 May 2020. https://www.theaustralian.com.au/nation/coronavirus-australia-no-app-leave-your-name-and-number/news-story/4b8a3f9ab4ebb87847794475d977bcb4

[2] Lilian Edwards and others (2020) *The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates*. https://doi.org/10.31228/osf.io/yc6xu

[3] Council of Europe, Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 28 April 2020.

[4] *Matthew Ryder QC, Edward Craven, Gayatri Sarathy & Ravi Naik*, 'Covid-19 & Tech Reponses: Legal Opinion', 3 May 2020, [32]. https://www.matrixlaw.co.uk/wp-content/uploads/2020/05/Covid-19-tech-responses-opinion-30-April-2020.pdf

the server, because there is a 'master key' that turns all the numbers any individual emits from their device into permanent, persistent identifiers.

Academic opinion has warned against centralisation. A group of almost 200 UK academics have cautioned against this centralised approach urging that 'It is vital that in coming out of the current crisis we do not create a tool that enables large scale data collection on the population', while a group of almost 600 international academics cautioned very similarly.[5]

Decentralised systems are designed with epidemiologists in mind. Decentralised systems are capable of providing data to epidemiologists to understand the disease, doing second order contact tracing, and revoking risk notifications that have been triggered by mistake or where evidence to change them comes to light.

Interoperability

The need for interoperability. Given that viruses do not respect borders, and the key role of the UK as a transit hub and home to people and families including many nationalities, international students and tourists, interoperability is key to easing the social and economic lockdown, and managing the virus while borders remain open plays a key role in that. Interoperability means that individuals can 'roam' with their app, as well as encounter 'roaming' users at home, and both receive and deliver risk alerts in relation to those they encounter.

Decentralised and centralised systems cannot interoperate. Decentralised and centralised systems are not compatible with each other without seriously compromising the entire privacy and security of both systems.[6] Decentralised systems, however, interoperate and federate in a straightforward way.[7]

A reliance on self-reporting might endanger interoperability. The EU Commission has recommended that 'only authorised parties can confirm and infection or trigger a warning'[8], with particular focus on interoperability, as authorised flags from abroad about someone's infection status can be used as a way to insert and propagate false alerts. If neighbouring countries predominantly rely on tests in the first instance, rather than self reporting, this could cause issues with interoperability, as such countries may not consider the UK's results reliable enough.

Incompatibility with the Republic of Ireland. The Republic of Ireland has announced they are no longer pursuing a centralised model, and instead 'opted to progress development on the basis of a more 'de-centralised' or 'distributed model'. This means that the matching of contact traces occurs on each individual's mobile phone and is not held centrally by the health services.'[9]

---

[5] https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/

[6] Ulrich Luckas and others (2 May 2020) Interoperability of decentralized proximity tracing systems across regions. https://drive.google.com/file/d/1mGfE7rMKNmc51TG4ceE9PHEggN8rHOXk/edit

[7] ibid.

[8] EU Commission, 'Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States' (Version 1.0), 15 April 2020, p.13.

[9] Dáil Statement and Briefing for Minister Harris. National app for Covid-19 (30th April 2020) http://www.ossiansmyth.ie/wp-content/uploads/2020/05/Statement-and-briefing-for-Minister-on-national-app-for-Covid-19-D%C3%83%C2%A1il-30-04-2020.docx

Incompatibility with Member States of the European Union. We note that the direction of travel in the European Union appears strongly towards decentralised approaches. In a recent resolution, the European Parliament "points out that [..] the generated data are not to be stored in centralised databases, which are prone to potential risk of abuse and loss of trust and may endanger uptake throughout the Union" and "demands that all storage of data be decentralised".[10] We also take note that the EDPB sought "to underline that the decentralised solution is more in line with the minimisation principle."[11]

Anonymous v Personal Data

Individuals must be identifiable not necessarily identified. In a contact tracing system such as the system proposed by NHSX, individuals may not be identified but remain *identifiable*. The data processed are therefore not 'anonymous' in a technical or a legal sense. According to the GDPR, personal data are any information relating to an identified or *identifiable* individual.[12] An identifiable individual is one who while not immediately identified (by name, for instance) who can be identified once additional information is added to the original data processed. In making the assessment of whether an individual is identifiable, the GDPR requires us to consider all means that are reasonably likely to be used to identify the person.

Pseudonymous data are personal data. Pseudonymous data, such as those processed by the NHSX app, constitute personal data. The GDPR additionally highlights that individuals may be 'associated with online identifiers provided by their devices, applications, tools and protocols', highlighting that data unconnected to names or more conventional means of identification can still count as personal data.[13] Pseudonymous data can be linked back to an identifiable individual with relative ease, particularly if combined with additional data later volunteered by app users, or sensor networks either controlled by the public sector or possible to requisition data from under investigatory powers legislation. A range of research indicates the ease with which social network data can be reidentified with knowledge of only a few of the nodes.[14] Furthermore, a few points of even coarse location data can locate people quickly in large datasets. Given the intention to use the first part of the postcode, individuals with unique trips to different parts of the country in a day (e.g. Southampton to Canterbury to Edinburgh) could be identified on the basis of the postcode associated with their contacts.

Re-identification by NHSX is legally possible. While it has been suggested that re-identification is unlikely as it constitutes a criminal offence[15], this is in situations where the re-identification occurs without the consent of the controller (in this case, NHSX). However, this does not prevent a pivot in purpose of the processing and the re-identification of the data with the consent of the controller.

---

[10] European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)), para 52.

[11] European Data Protection Board (2020) *Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*.

[12] GDPR, art 4(1).

[13] GDPR, recital 30.

[14] See eg Kumar Sharad and George Danezis, 'An Automated Social Graph De-Anonymization Technique' [2014] arXiv:14081276 [cs]; Laura Radaelli and others, 'Quantifying Surveillance in the Networked Age: Node-Based Intrusions and Group Privacy' [2018] arXiv:180309007 [cs].

[15] Matthew Gould, Evidence to Science and Technology Committee, 27 April 2020.

Moreover, while it is a criminal offence to knowingly or recklessly re-identify de-identified data, it is a defence to argue that, for instance, re-identification was in the public interest.[16]

Purpose Limitation

Purpose limitation requires that purposes are 'specific' rather than vague. A core tenet of data protection regimes worldwide is purpose limitation. According to this principle, personal data should be collected for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes'.[17] In this instance, the purposes of this application have been broadly defined as helping the NHS, public health and research purposes.[18] Such broadly stated purposes are not sufficiently specific to enable the application of other data protection principles and to assess the necessity and proportionality of the principles. Further processing for research purposes (by the public or private sector and irrespective of the objectives of the research), is prima facie not incompatible processing.[19] This is particularly important as app users may nevertheless want further clarification about what parameters, if any, will be set for the future re-use of this data for research purposes. Given the sensitive nature of the data, there may be particular public reservations about this data being repurposed for commercial purposes unrelated to public health.

Data controllership does not prevent data sharing. Matthew Gould stated, in a response to the Commons STC, that data will 'be probably under the joint data controllership of DHSC, NHS England and NHS Improvement'.[20] Controllership does not delimit any boundaries with who data can or cannot be shared with. As a consequence, it does not provide reassurance that, for example, data will not be shared with the Home Office for immigration purposes. In addition,

Data Minimisation

Only the minimum amount of data necessary to achieve a purpose should be processed. The NHSX app is designed in a manner that allows for the incremental inclusion of volunteered data, including location data. Such data is not necessary for the sole purpose of proximity tracing and the EDPB has explicitly noted that such apps should not be tracing individual movements but proximity. In particular, it notes that mobility traces of individuals are 'inherently highly correlated and unique' and thus vulnerable to re-identification.[21] Moreover, when location data is combined with proximity data, it necessarily reveals the location of others, making consent a necessary yet insufficient legal basis for its collection.

Erasure and the 'Right to be Forgotten'

The NHSX needs a clear plan to deal with data erasure requests. We note that Matthew Gould stated in his evidence to this Committee that 'The data can be deleted as long it is on your own device. Once it is uploaded, it becomes enmeshed in wider data, and the technical difficulties of deleting it at

[16] DPA 2018, s.171(3).
[17] GDPR, art 5(1)(b).
[18] Matthew Gould, Evidence to Science and Technology Committee.
[19] GDPR, arts 5(1)(b) and 89(1).
[20] Matthew Gould, Evidence to Science and Technology Committee, Q378.
[21] European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, [20].

that point become tricky'.[22] Given that individuals' device identifiers are held both on the phone and the server, singling out an individual to erase their data is technically possible.[23] Locating the data should be easy if good data management practices are followed. NHSX would require a clear legal justification if they were to refuse erasure requests, rather than just a reliance on an unspecified technical difficulty.

Data Accuracy

Data processed should be accurate. Allowing alerts, or the 'amber' cascade, on the basis of self-reporting risks entailing a significant increase in false positives as such it stands in tension with the principle of data accuracy[24] which provides that processed personal data shall be accurate. It is worth noting that the French Minister for Digitalisation, Cédric O, wrote that an application can only be useful if it ensured only individuals who actually tested positives can declare themselves in the app.[25]

The NHSX's app appears not to function on iPhones accurately, endangering this principle. It has been widely reported that the NHSX's app uses workarounds to function in the background on Apple devices, without having to keep the screen unlocked and app foregrounded the entire time in an individual's pocket or bag as has been required in Australia and Singapore (which if mandated could potentially construe an ECHR Article 8 violation, given the importance of the data phones hold and the risk of it being stolen or obtained unlocked by a thief or public authority). It is worth noting that both Australia and Singapore report moving to the Apple-Google decentralised approach.[26] The NHSX's app appears to not allow iPhones to recognise each other when they are locked and in an individual's bag or pocket during an encounter unless someone with an Android phone is nearby, which has the effect of 'waking' them up. If this individual with the Android only enters at the end of the encounter, the iPhones will not appear to have been with each other for a long time. This is a significant population-level accuracy problem, resulting from attempting to work around Apple's privacy protection, avoidable by adopting a decentralised system.[27] It may be an acceptable accuracy risk if there was no way to increase the accuracy, but as noted, decentralised systems that will not encounter this problem are prevalent across the world.

Transparency and Accountability

High risk processing requires an impact assessment and full transparency requires its timely publication. The GDPR requires data controllers to conduct an impact assessment when there is a 'high risk' to the rights and freedoms of individuals. Such a high risk exists when, amongst other circumstances, there is 'processing on a large scale of sensitive personal data'.[28] This is undoubtedly the case here as there is proposed population wide processing of sensitive health data. While not

---

[22] Evidence by Matthew Gould to the JHRC, 4 May 2020.

[23] See generally Michael Veale and others, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105.

[24] GDPR, art 5(d).

[25] Cédric O (3 May 2020) 'StopCovid ou encore?' https://medium.com/@cedric.o/stopcovid-ou-encore-b5794d99bb12

[26] On Australia, see https://www.theguardian.com/australia-news/2020/may/05/covid-safe-app-downloads-ios-android-iphone-australian-government-covidsafe-tracking-how-to-download-install-works-working-problems-australia-coronavirus-contact-tracing, on Singapore, see https://tracetogether.zendesk.com/hc/en-sg/articles/360046475654-20-April-2020-One-Month-On

[27] See https://www.theregister.co.uk/2020/05/05/uk_coronavirus_app/

[28] GDPR, art 35(3)(d).

mandated, the GDPR states that, where appropriate, the data controller should seek the view of the data subject - individual app users - or their representatives.[29]

Prior Consultation. While the ICO has to date been informally consulted regarding the app, this would not constitute 'prior consultation' as required by Article 36 GDPR where the impact assessment reveals a high risk of processing that cannot be mitigated to an acceptable level. *All possible contact tracing systems* suffer from several flaws that cannot be mitigated, such as the ability for a determined attacker to work out the infection status of their neighbour, and the risk for false data to be broadcast in a so-called 'relay attack'. Because it can be proven that these cannot be mitigated,[30] it is clearly arguable that Article 36 prior notification is a mandatory requirement in this situation. This is legally required *before processing starts*, i.e. before an app is rolled out across the United Kingdom.

Impact assessment. The failure to make the impact assessment available to the wider public in advance of the launch of the app on the Isle of Wight and in anticipation of its imminent rollout across England stands in contrast to publicly provided assurances of transparency.

Open source code. It is commendable that the code is pledged to be released open source, although this has not happened at the time of writing. However, it is important that it is not just the app that is open sourced, but the *backend server* too. In a centralised system, this is the part that requires the most scrutiny. Releasing only the source code of the app only reveals the part of the iceberg that is above the water. Other implementations internationally have open sourced their backend servers.[31] Security should not rely on obscurity: modern cryptography and privacy engineering designs systems so they are secure despite all of their parts being known.

Review and Oversight

Functional review requires actions to stem from recommendations. NHSX has consulted a range of stakeholders in the development of the app including the National Data Guardian Panel, Understanding Patient Data group and the CDEI. It has also created an Ethics Advisory Board. Proposals for alternative input mechanisms at the design phase have however been mooted. For instance, the Ada Lovelace Institute recommends the creation of a 'Group of Advisors on Technology in Emergencies' (GATE) in order to review evidence and advise on the design and implementation of the application. It may be that the Ethics Advisory Board could play a similar role. However, at present, as noted by Dr Marion Oswald, the terms of reference of this Board does not indicate what consequences follow from their recommendations and, in particular, whether a public response will be provided to such recommendations.[32]

Oversight should be independent and subject to proper procedures. Beyond this initial input, an independent oversight mechanism is required to conduct real-time scrutiny of the operation of the app. The ECtHR has identified conditions for oversight in the context of intelligence surveillance where, as

[29] GDPR, art 35(9).

[30] The DP-3T Project (2020) Privacy and Security Attacks on Digital Proximity Tracing Systems. https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf

[31] See eg https://github.com/DP-3T/dp3t-sdk-backend

[32] Tweet by Marion Oswald. https://twitter.com/Marion_InfoLaw/status/1257562592572252166

in the current context, individual abuse is easy and there are implications for democracy as a whole. These are that oversight should be independent; impartial and which has adopted its own rules of procedure.[33] The ICO, whose independence is guaranteed by the GDPR, would meet these conditions. While academics have raised concern regarding the dual investigative and enforcement role of data protection authorities, this does not fall foul of the independence criterion. Oversight conducted by the ICO would benefit from the ICO's experience but, more significantly, the Office's extensive investigative and enforcement powers.

Consequences beyond data protection may lead to oversight gaps. An alternative proposal is for the creation of a temporary office in order to ensure real-time oversight of the functioning of the app. This alternative is worthy of consideration for a number of reasons. Most significantly, while the deployment of the app inevitably entails data protection issues, it also entails risks for other neighbouring rights including privacy and non-discrimination. In evidence, the ICO rightly indicated that the powers afforded to her by the legislative framework are wide-ranging and enable her, for instance, to assess the fairness of a data processing operation. The DPA 2018 and GDPR require personal data processing to be lawful. This means that not only should such processing have a legal basis (eg. consent or public interest) but it must also comply with all other legal frameworks. Nevertheless, there may be situations where the ICO's authority is contestable. Two examples suffice. First, we could imagine situations where individuals are compelled to display the app. This could be in order to enter a workplace or a restaurant, for instance. The act of displaying a phone would not constitute personal data processing: while the information displayed is personal data, it is arguably not *processed* within the meaning of the DPA. It is neither processed wholly or partly by automated means or forming part of a filing system. The person demanding access would not be a 'data controller'. While this would be a violation of privacy, it would not be a violation of data protection which is a closely related but distinct right.[34] Second, the ICO has gone beyond its European counterparts by according a substantive meaning to 'fairness' as a data protection principle. To date, data processing has been deemed to be unfair where it has either been misleading or lacking sufficient transparency, or where it has defied the reasonable expectations of the individual data subject. This concept of fairness does not however readily correlate to a substantive assessment of whether illegal discrimination on protected grounds has occured, for instance. Now may not be the time to put such open-textured terms to the test, when we can instead make more specific, clearer and more foreseeable temporary provisions.

Attribution of Powers. Such additional powers, for instance to ensure that an app was truly voluntary in nature and that no individual or third party suffered detriment as a result of a failure to download the app, could be attributed to the ICO. In considering options, it is also necessary to consider what would cause least confusion to individuals seeking redress and that such redress should be expedited to alleviate concerns as they arise. It is worth noting that the ICO may need additional resource alongside any new powers they have been provided with.

Automated Decisions

The GDPR and the Data Protection Act 2018 require 'qualifying significant decisions' based solely on automated processing to be authorised by law.[35]

---

[33] *Kennedy v UK* [2010] ECHR 682, [167].

[34] R v Secretary of State for the Home Department ex p David Davis MP, Tom Watson MP, Peter Brice and Geoffrey Lewis [2015] EWCA Civ 1185, [110].

Outputs for this app are solely automated for the purposes of data protection law. Outputs from the app are self-evidently based solely on automated processing. Having a gatekeeper or individual who looks after the whole system does not mean it is not automated. In order for a decision not to be solely automated, the Information Commissioner notes that human oversight both 'has to be active and not just a token gesture', meaning that 'a human reviews the decision before it is applied and has discretion to alter it'. At the scale of the app, it is not possible for a human to review every decision to either provide or not provide a risk alert at all, let alone in an active and not a token way.

Decisions are significant for the purposes of data protection law. Such decisions are rendered significant if they have a 'legal effect' or a 'similarly significant' effect.[36] Given the provisions of the Health Protection (Coronavirus) Regulations 2020, it is arguable that instructions from an NHS app have a legal effect. Even if they do not (for example, if it is made obvious in the app that such instructions are not binding), instructing someone to isolate or to socially distance in a heightened manner would be likely to have a significant effect on that person's life. It is worth noting that a decision is defined widely, and 'may include a measure'.[37] The Information Commissioner notes that a significant effect would be one with 'equivalent impact on an individual's circumstances, behaviour or choices [to a legal effect]'. This would include a major psychological impact, particularly in light of the 'enormous comms effort' which would 'require [the Government] to find messages and messengers that resonate in all the communities of the country'.[38] For avoidance of doubt, the Council of Europe has stated in relation to coronavirus contact tracing apps, in the context of to the international data protection instrument Convention 108 which the United Kingdom is party to, that '[i]t is clear that implications such as self-isolation and testing can have such significant effects'[39] and that '[u]sers of the digital tracing system must therefore not have consequences imposed on them without a clear facility to challenge these consequences, particularly in light of the inaccuracies or misrepresentations possible in such systems'.

The 'qualifying significant decisions' the app makes require a statutory basis. Qualifying significant decisions relating to health are forbidden unless there is explicit consent or a basis in law.[40] Data protection consent is a very high bar to meet in times of power imbalance, and the GDPR states that it 'should not provide a valid legal ground [..] in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority'.[41] As a consequence, the measure should be 'authorised by Union or Member State law'.[42] We believe this calls for specific primary legislation authorising the measures taken using this app, as well as safeguards including a process to request this decision be reconsidered, including by non-automated means.[43]

---

[35] GDPR, art 22.
[36] Data Protection Act 2018 s 14(2).
[37] GDPR, recital 71.
[38] Matthew Gould, Evidence to STC, Q339.
[39] Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe (28 April 2020). https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7
[40] GDPR, art 22(4).
[41] GDPR, recital 43.
[42] GDPR, art 22(2)(b).
[43] Data Protection Act 2018 s 14(4)(b).

6/05/2020