COVID-19 & Tech responses: Legal opinion

Matthew Ryder QC, Edward Craven, Gayatri Sarathy & Ravi Naik

Table of Contents

I. INTRODUCTION AND EXECUTIVE SUMMARY

1. As part of its response to the COVID-19 pandemic, the UK Government has announced its intention to deploy a range of digital and data-driven solutions to monitor public health and provide the Government with information on the spread of the pandemic. The central technological solutions are (i) smartphone contact tracing (ii) data sharing and (iii) immunity passports. Those proposals, insofar as they have been made public, are still in embryonic form. We have been asked by the *Open Society Foundation* to provide a preliminary opinion on the legal framework concerning the right to privacy and protection of personal data under which those proposals will need to be considered.

2. Our assessment is necessarily limited to the consideration of proposals, rather than a concrete plan, as at the time of drafting it is not clear which of the alternatives that could be deployed will in fact be introduced. As we are instructed to consider the human rights impacts only, we have not covered wider regulations that may have consequences for digital responses, such as the Digital Economy Act 2017.

3. Our conclusions are summarised as follows:

Contact tracing

3.1. There are broadly two types of smartphone contact tracing system: centralised or decentralised. Both systems would engage the right to respect for private life under Article 8 of the European Convention on Human Rights ("ECHR"). Any interference with Article 8 would have to be in accordance with the law, proportionate and necessary. We consider that the decentralised systems, such as the "DP3T" system, are likely to be in accordance with the law, proportionate and necessary. In contrast, a centralised system would result in a significantly greater interference with users' privacy and require greater justification. We note that there are epidemiological reasons that may support the need for a centralised system, but the uncertainty as to the efficiency, uptake and utility of a centralised system would have to be addressed with sufficient evidence before its introduction could be justified.

3.2. It is not clear from the current proposals if contact tracing through the use of the app would be mandatory or voluntary. A mandatory smartphone app would be a significant measure, both legally and culturally. Our view is that there would need to be a clear and detailed legal basis for a mandatory system, set out in specific legislation.

Data sharing between public and private sector

3.3. The Government has announced plans to (i) share data held by health care organisations and create a "data store" and (ii) establish arrangements for sharing data between public authorities and private companies to assist in combating the COVID-19 pandemic. We believe there are a number of legal problems with the plans announced thus far:

(1) The Government has issued notices which appear to require a broad range of recipients, including "Local Authorities", "Arm's length bodies of the Department

of Health and Social Care" and "Organisations providing health services" to process confidential patient information generated outside, as well as within, the NHS. Insofar as the notices require data generated outside the NHS to be processed, they appear to exceed the scope of the regulations on which the Government has relied to authorise such activity.

(2) The data sharing arrangements that the Government has announced for the creation of a data store for purposes relating to the COVID-19 pandemic currently lack sufficient clarity and detail to comply with the data protection principles set out in Article 5 of the General Data Protection Regulation ("GDPR"). Further, the Government has not provided sufficient information to explain how such data sharing arrangements will comply with the guidelines in the *Draft Data Sharing Code of Practice* published by the Information Commissioner's Office ("ICO"). That Code, reflecting the requirements of the GDPR, requires (amongst other things) that a data sharing arrangement is in place to prescribe (i) the purposes of data sharing; (ii) the respective roles of the parties and their access to the data concerned; and (iii) the procedures to allow data subjects to realise their rights under the GDPR and the Data Protection Act 2018 ("DPA").

3.4. Given the nature of the data likely to be shared, the Government will need to undertake a data protection impact assessment ("DPIA") prior to the processing of any personal data under these proposals (for both contact tracing and data sharing). Additionally, and for the purposes of transparency, we believe the results of that DPIA should be made public. Those steps may be in progress, but we are not aware of them having been completed thus far.

Immunity passports

3.5. On 2 April 2020, the Government announced its intention to develop "immunity certificates". No proposals of any kind have yet been forthcoming.[1] Such a step would engage a number of fundamental rights under the ECHR and EU/UK legislation concerning the right to privacy and protection of personal data. Any proposals would require very substantial evidential justification to show that they are necessary and proportionate. We note that the World Health Organisation ("WHO") has cast doubts on the effectiveness of immunity passports, particularly where the medical evidence to support any form of "immunity" short of a vaccination remains unclear.

4. In order to assist with understanding the basis for the conclusions set out in this Opinion, it includes four annexes:

4.1. A list of defined terms used in this Opinion is contained in **Annex 1**.

[1] On immunity certificates, we recommend the detailed analysis of Ada Lovelace Institute in its report: 'Exit through the App Store', p.42 (*Ada Lovelace Institute*, 20 April 2020) <https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf> ("Ada Lovelace Report") accessed 28 April 2020.

4.2. A detailed analysis of the applicable legal provisions is contained at **Annex 2**.

4.3. A summary of statements from the ICO, European Data Protection Board ("EDPB") and others expressing their views on smartphone contact tracing is contained in **Annex 3**.

4.4. A summary of the relevant statements, notices and blogposts relating to the Government's data sharing plans is contained in **Annex 4**.

5. Finally, we note that the UK Government has consistently stated that it would be guided by the evidence and advice of experts when it comes to responding to the COVID-19 pandemic. This includes matters such as determining the duration of "lockdown", social distancing, business activity and other measures. The same emphasis on guidance from a broad range of experts should also apply to any attempt to use data-driven solutions. These are complex issues requiring expertise in technical capabilities, law and human rights. The indication that there is currently consultation between NHSX and the ICO, National Data Guardian's Panel and the Centre for Data Ethics and Innovation, as well as with representatives from Understanding Patient Data are all positive steps and is to be welcomed. Government consultation and cooperation with a wide range of experts will be important to address concerns and ensure that any system has public trust.

II. CONTACT TRACING

Background

1. Contact tracing is a measure implemented to trace persons who have been exposed to a probable or confirmed case of COVID-19 and who are in danger of developing or have developed the disease. Contact tracing has the potential to reduce the transmission and spread of the outbreak, assist epidemiologists with the modelling and monitoring of the disease and facilitate the eventual easing of the lockdown.

2. Contact tracing has been previously carried out manually in response to other epidemics and in the early stages for the current epidemic in the UK, through interviews with infected people. Governments across the world are, however, now seeking to use smartphones as a proxy for monitoring individuals by determining which smartphones have been close to each other for relevant periods. Through that information, data is collected to indicate which persons may have been close enough to infect each other.

3. These smartphone apps enable alerts and warnings to be communicated to users if they have been in close proximity with an individual who has confirmed positive for COVID-19 and to ask those individuals to self-quarantine. Beyond merely alerting individuals, by connecting additional data to proximity data, public health authorities can assess infection patterns to make containment decisions at a local or national level.

4. Importantly, the efficacy of the data gained from such smartphone apps depends on a high level of adoption by smartphone users.[2]

5. Every proposal currently under consideration in the UK involves members of the public installing a contact tracing app that utilises Bluetooth technology standard that already exists on smartphones. Through Bluetooth, the phone emits anonymous "identifiers" / "keys" – simple numeric "messages" – to other smartphones that receive them. That process creates a data trail for every smartphone of its proximity to other smartphones.

Decentralised vs Centralised

6. There are two broad approaches to the analysis and storage of data collected by a contact tracing app:

   6.1. **Centralised models**: A centralised model involves the transmission by a central server of random identifiers to be transmitted by a user's smartphone. Other smartphones in proximity to that phone then detect the identifiers and transmit this information back to the central server.[3] If a person tests positive for COVID-19, the identifiers that their phone has received from other phones can be uploaded (either under compulsion of law or voluntarily depending on the contingent legal structure) together with the times and

[2] A report to NHSX from Oxford University academics on 16 April 2020 concluded that the COVID-19 pandemic could be suppressed with 80% of all smartphone users, or 56% of the population overall, using a contact tracing app: see §16 below.

[3] Examples of centralised systems in Europe include NTK (Germany) and ROBERT (France)

duration of contact and optionally other device information. The identifiers are decrypted, and notifications can be sent to proximate phones suggesting or requiring their users to self-isolate or take other measures. Because the central server has information about both those who have been infected and those who have been close to them, it enables further data (e.g. their location or other personal information) to be connected together at speed and scale.

6.2. **Decentralised models:** The main characteristic of a decentralised model is that identifiers are generated on a user's device and cannot be matched by any central server. When a patient is diagnosed positive for COVID-19 the identifiers that their smartphone has *transmitted* are uploaded (rather than those it has *received*). Other smartphones can access these data and establish whether it has been in proximity to the infected individual's smartphone. If a smartphone identifies matches to a confirmed COVID-19 patient's identifiers, then a notification can be generated to the user. The nature and content of that notification, as in the centralised model, is not prescribed by the system. This model ensures that the proximity of persons to COVID-19 patients is not known to any central server or authority.

7. **DP3T:** The decentralised protocol that has received the most interest is entitled Decentralized Privacy-Preserving Proximity Tracing or "DP3T",[4] a secure and decentralised system using Bluetooth Low Energy technology. DP3T is a "low-cost decentralized proximity tracing" protocol. This involves phones generating Bluetooth "send" keys which are transmitted to other phones in close proximity and then stored as Bluetooth "receive" keys on the device.[5]

If a user is diagnosed with COVID-19, they will be authorised by the health authorities to instruct their smartphone to upload their Bluetooth "send" keys to a server. The server acts *solely* as a communication platform which holds the anonymous Bluetooth "send" keys of those who have tested positive for COVID-19. Other smartphones then periodically query the server for a list of Bluetooth "send" keys from the smartphones whose users have tested positive for COVID-19 and download them onto the device. If a smartphone making such a query has stored a record that matches any of the infected Bluetooth "send" keys downloaded from the server as Bluetooth "receive" keys, it reveals that the phone has been in physical proximity with an infected person and the app computes the user's risk score. Importantly, the match between the Bluetooth "send" and "receive" keys occurs *on device*, not on the server. If the score is above the threshold, the phone initiates a notification process on the app.[6]

Importantly, under the DP3T system the public health authority and/or epidemiologists are not notified that a user has been in contact with an infected person. The fact that someone has been notified that they may have been in proximity to an infected person occurs on their device and remains entirely private to them. However, that person may consent to share with the public

---

4 Prof Carmela Troncoso et al, 'Decentralized Privacy-Preserving Proximity Tracing' (*GitHub,* 12 April 2020) <https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf> accessed 19 April 2020.

5 Bluetooth signals have a range of about 30 feet or 9 meters. See 'App-based contact tracing may help countries get out of lockdown' (*The Economist*, 16 April 2020) <https://www.economist.com/science-and-technology/2020/04/16/app-based-contact-tracing-may-help-countries-get-out-of-lockdown> accessed 27 April 2020.

6 A pictorial representation is available here: https://ncase.me/contact-tracing/.

authority that they have received that notification. No location or precise timing information is shared. The data shared enables the public health authority and/or epidemiologists to create a first-degree proximity graph around an infected person, but it does not reveal any information about wider social encounters. DP3T is compatible with the Apple / Google Initiative, set out below.

Apple / Google proposals

8. In addition to these proposals, on 10 April 2020, Apple and Google released a joint specification indicating that they would launch application programming interfaces ("APIs") and operating system-level technology to assist in enabling contact tracing ("Apple / Google Initiative").[7] The Apple / Google Initiative has three important features:

   8.1. It allows interoperability of Bluetooth communication between smartphones (i.e. it enables different types of smartphone to communicate with one another).

   8.2. It eliminates an existing limitation on Bluetooth technology and allows it to function even when a smartphone is locked.[8]

   8.3. It limits that improved functionality to apps that work on a decentralised system. A centralised smartphone contact tracing app would have poor (if any) functionality on those operating systems. This has frustrated the plans of some health authorities who were hoping to develop a centralised system based on the improved Bluetooth functionality that exists under the Apple / Google Initiative.[9]

9. For those reasons, the Apple / Google Initiative is important to the efficacy of a contact tracing app.

The NHS position

10. On 22 April 2020, a blogpost by Matthew Gould, Chief Executive of NHSX, stated that NHSX was developing a contact tracing app that would "*store anonymous proximity information securely on your phone and will only share that information with the NHS when you allow it to*" and "*only ever be used in the interests of providing care, public health management and relevant research. Users will always have the right to delete the app, and their data*".[10]

---

7 Apple, 'Apple and Google partner on COVID-19 contact tracing technology' (*Apple*, 10 April 2020) <https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/> accessed 19 April 2020.

8 The poor uptake of a Bluetooth contact tracing app in Singapore – TraceTogether – is largely blamed on this limited functionality. See, for example, Alex Hern and Kari Paul, 'Apply and Google team up in bid to use smartphones to track coronavirus spread' <https://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-app-privacy> (*The Guardian*, 10 April 2020) accessed 28 April 2020.

9 Alex Hern, 'NHS in standoff with Apple and Google over coronavirus tracing' (*The Guardian,* 16 April 2020) <https://www.theguardian.com/technology/2020/apr/16/nhs-in-standoff-with-apple-and-google-over-coronavirus-tracing>; Alex Hern, ''France urges Apple and Google to ease privacy rules on contact tracing' (*The Guardian,* 21 April 2020) <https://www.theguardian.com/world/2020/apr/21/france-apple-google-privacy-contact-tracing-coronavirus> accessed 28 April 2020; Alex Hern, 'NHS in stand-off with Apple and Google over coronavirus tracing' (*The Guardian*, 16 April 2020) <https://www.theguardian.com/technology/2020/apr/16/nhs-in-standoff-with-apple-and-google-over-coronavirus-tracing> accessed 19 April 2020.

10 Matthew Gould, 'Tech on the Frontline – how NHSX partners are delivering at pace' (*NHSX,* 21 April 2020) <https://www.nhsx.nhs.uk/blogs/tech-frontline-how-nhsx-partners-are-delivering-pace/> accessed 28 April 2020.

11. On 24 April 2020, a further blogpost by Mr Gould and Dr Geraint Lewis explained that a contact tracing app had been developed and provided some detail of its specifications:

> *Once you install the app, it will start logging the distance between your phone and other phones nearby that also have the app installed using Bluetooth Low Energy.*
>
> *This anonymous log of how close you are to others will be stored securely on your phone. If you become unwell with symptoms of COVID-19, you can choose to allow the app to inform the NHS which, subject to sophisticated risk analysis, will trigger an anonymous alert to those other app users with whom you came into significant contact over the previous few days.*
>
> *The app will advise you what action to take if you have been close to someone who has become symptomatic – including advising you to self-isolate if necessary. The exact advice on what you should do will depend on the evolving context and approach. It will be based on the science, and will be approved by the Chief Medical Officer. Scientists and doctors will continuously support us to fine-tune the app to ensure it is as helpful as possible both to individuals and to the NHS in managing the pandemic.*
>
> *In future releases of the app, people will be able to choose to provide the NHS with extra information about themselves to help us identify hotspots and trends. Those of us who agree to provide this extra information will be playing a key role in providing additional information about the spread of COVID-19 that will contribute towards protecting the health of others and getting the country back to normal in a controlled way, as restrictions ease.*
>
> *The data will only ever be used for NHS care, management, evaluation and research. You will always be able to delete the app and all associated data whenever you want. We will always comply with the law around the use of your data, including the Data Protection Act and will explain how we intend to use it. We will be totally open and transparent about your choices in the app and what they mean. If we make any changes to how the app works over time, we will explain in plain English why those changes were made and what they mean for you. Your privacy is crucial to the NHS, and so while these are unusual times, we are acutely aware of our obligations to you. Just as the NHS strives at all times to keep your health records confidential, so it will keep the app data secure. Patient confidentiality is built in to the NHS. It is one of our key values.*
>
> *We have prioritised security and privacy in all stages of the app's development, starting with the initial design, and user testing. We have drawn on expertise from across government and industry to review our design and help test the app. We are working with Apple and Google on their welcome support for tracing apps around the world. As part of our commitment to transparency, we will be publishing the key security and privacy designs alongside the source code so privacy experts can "look under the bonnet" and help us ensure the security is absolutely world class.*

12. On 27 April 2020, the BBC reported that the NHS (assisted by the UK intelligence agency, GCHQ) had opted to reject compatibility with the Apple / Google Initiative and would be launching a centralised contact tracing app. This is consistent with some of the earlier NHS

indications,[11] notwithstanding that more recent announcements had appeared to be more aligned with a decentralised app. It is remains unclear what the features of the NHS system would be and what the overall objective of using a centralised system is, beyond alerting potentially infected people and advising them to self-quarantine. Similarly, it is not clear what other data that will be added to / amalgamated with data gleaned from contact tracing in order to improve its functionality.

13. Further, even though it appears that the use of the proposed NHSX app will be voluntary, it is not clear whether its use would be incentivised by, for example, penalising those who refuse to use the app or upload their data by applying more punitive "lockdown" measures or by refusing provision of a service or access to a venue or an event.[12] In this regard, on 18 April 2020, Buzzfeed reported that officials were considering how to enforce use of the app, potentially introducing measures to require individuals to download the app if they wanted the easing of lockdown restrictions to apply to them. [13]

Analysis of "contact tracing" systems

Is digitised contact tracing necessary?

14. As a preliminary matter, we note there remains concerns about whether it is necessary to deploy smartphone technology for contact tracing at all at present, rather than using existing forms of manual contact tracing that were used to monitor, for example, the Ebola crisis.[14] A *"Rapid Evidence Review"* by a consortium of experts and published by the Ada Lovelace Institute on 20 April 2020 ("Ada Lovelace Report") concluded:[15]

> *"There is currently insufficient evidence to support the use of digital contact tracing as an effective technology to support the pandemic responses. The technical limitations, barriers to effective deployment and social impacts demand more consideration before digital contact tracing is deployed."*

---

11 The earlier intention to develop a centralised app was reflected in the statements from Oxford University academics working with NHS and news reports of the intention of ministers See, e.g., Leo Kelion, 'Coronavirus: UK considers virus-tracing app to ease lockdown' (*BBC*, 31 March 2020) <https://www.bbc.co.uk/news/technology-52095331> accessed 28 April 2020; Oxford University, 'Using a mobile app for contact tracing can stop the epidemic' (undated) <https://045.medsci.ox.ac.uk/mobile-app> accessed 28 April 2020; Statement from Health Secretary, Matt Hancock MP, Daily Briefing, 12 April 2020; Robert Hinch et al, 'Effective Configurations of a Digital Tracing App: A report to NHSX' (16 April 2020) <https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf> accessed 28 April 2020; Alex Hern, 'NHS in stand-off with Apple and Google over coronavirus tracing' (*The Guardian*, 16 April 2020) <https://www.theguardian.com/technology/2020/apr/16/nhs-in-standoff-with-apple-and-google-over-coronavirus-tracing> accessed 28 April 2020.

12 Such punitive measures are not a feature of the app, but a way of incentivising its use. Theoretically, they could be applied to both centralised and decentralised systems, but would be more difficult to impose on the latter where the identity of users, their contacts, and their response to alerts remains unknown to the central server

13 Alex Wickham, 'Revealed: The UK's "Three Stage" Exit Strategy to East the Coronavirus Lockdown" (BuzzFeed, 18 April 2020) <https://www.buzzfeed.com/alexwickham/coronavirus-uk-lockdown-three-stage-exit-plan?ref=hpsplash> accessed on 19 April 2020.

14 See, e.g., Ross Anderson, 'Contact Tracing in the Real World' (*Light Blue Touchpaper*, 12 April 2020) https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/ accessed 19 April 2020; Sean McDonald, 'The Digital Response to the outbreak of COVID-19' (*Centre for International Governance Innovation,* 30 March 2020) https://www.cigionline.org/articles/digital-response-outbreak-covid-19; 'Monitoring Being Pitched to Fight Covid-19 Was Tested on Refugees' (*Bureau of Investigative Journalism,* 28 April 2020) <https://www.thebureauinvestigates.com/stories/2020-04-28/monitoring-being-pitched-to-fight-covid-19-was-first-tested-on-refugees> accessed 28 April 2020.

15 Ada Lovelace Report (n 1), p.32.

15. To this end, we note the Belgian authorities have decided against using any technological contact tracing and instead will rely on manual contact tracing.[16] Until very recently, the only voluntary smartphone contact tracing app in use was the *TraceTogether* app in Singapore, which was downloaded by 17% of the population.[17] On 26 March 2020, the *CovidSafe* app was launched in Australia, and in its first few days has achieved relatively high levels of early adoption.

16. The likely level of adoption is an important feature in whether a contact tracing app is effective and necessary. By simulating a city of one million people, researchers at the University of Oxford found that 80% of smartphone users in the UK (i.e. 56% of the national population) would need to install a contact-tracing app in order for it to be effective in suppressing the COVID-19 pandemic. Even if app uptake is low, however, the University of Oxford team estimated that such technology could still reduce the number of cases of the disease and deaths.

17. Nevertheless, if, as the Ada Lovelace Report suggests, there is insufficient evidence to support effectiveness and reliability[18] of smartphone contact tracing at all, then the existing proposals – even under a decentralised system – may not be proportionate and lawful. It is right that before examining the respective merits of centralised or decentralised systems, there should be evidence that the technology underpinning both is effective and reliable. However, without attempting to reach a conclusion on that issue, which would require review of the evidence on the technical capability of any system, we have gone on to consider the legal issues in play in relation to both systems on the basis that the initial evidential hurdle is overcome.

18. For reasons set out at §§53-64 below, subject to sight of the specific proposals, it is our view that there may be good reasons to adopt a decentralised or centralised system involving the use of technology, in preference to a system of manual contact tracing. We have proceeded on this basis below.

Human rights analysis of contact tracing systems

19. We consider there to be two aspects of the current proposals that give rise to particular human rights considerations:

    i. The **processing** of personal data; and

    ii. The **mandatory** use of any app.

20. We address each in turn.

i. Processing of personal data

21. The contact tracing system introduced by the UK Government must be compatible with:

---

16 Marine Strauss, 'Belgium will not use coronavirus contact tracing apps' (*Reuters*, 24 April 2020) <https://uk.reuters.com/article/uk-health-coronavirus-belgium-tracing/belgium-will-not-use-coronavirus-contact-tracing-apps-minister-idUKKCN2261S9> accessed 28 April 2020.

17 'How will the UK's new contact tracing programme work?' (*FT*, 26 April 2020) < https://www.ft.com/content/4a282a0f-5a9f-4f7d-a313-231975d231bd> accessed 28 April 2020.

18 This would include matters such as adequate testing, manageable notifications, false positives etc.

21.1. the right to privacy guaranteed by Article 8 of the ECHR, as well as Articles 7 and 8 of the EU Charter of Fundamental Rights ("Charter");

21.2. the principles relevant to the protection of personal data set out in the GDPR, the "E-Privacy" Directive and the DPA.[19]

22. We address these regulations below.

Is Article 8 ECHR engaged?

23. Article 8 of the ECHR confers on everyone a qualified right to "*respect for his private and family life, his home and his correspondence*". Not every act of processing of personal data would engage Article 8. Rather, the touchstone for the engagement of Article 8(1) is whether an individual enjoys a "reasonable expectation of privacy" in respect of that information. Further, the concept of "private life" is a broad term not susceptible to exhaustive definition. The European Court of Human Rights has held that "private life" covers:[20]

> "*the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by art.8. Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family. Information about the person's health is an important element of private life.*"

24. It follows that the data processing as part of contact tracing is likely to be covered by the concept of "private life" for the purposes of Article 8. In our view, it seems inevitable that any of the proposed centralised systems are likely to involve the processing of "personal data" in some way. This is because the purpose of a centralised system is usually to allow a health authority to obtain access not merely to basic information about who may be infected, but also to those with whom they have been in contact, combined with other information from which identification or individuation could occur. The collection of such data over a period, to draw up a pattern of movements, would be sufficient to amount to an interference with Article 8.[21]

25. In contrast, it is not inevitable that a decentralised system would involve the processing of "personal data". A number of those promoting smartphone contact tracing have suggested that the generation of anonymous Bluetooth keys to carry out contact tracing – either in a de-centralised or centralised system – would not engage the regime for the protection of personal data at all, on the basis that the data concerned is not "personal data" (see Recital 26 and Article 4(1) GDPR and s.3 DPA 2018).[22] In turn, the implication would be that such processing would not engage Article 8.

---

19 An exhaustive analysis of those regimes is beyond the scope of this paper, as that legislation covers a wide range of matters that will apply to the deployment of contact tracing technology, such as the application of the research exemptions and the need for records of data processing records. Rather, we focus on those legislative provisions insofar as they relate to human rights.

20 *S v United Kingdom* (2009) 48 EHRR 50 §66-67.

21 See, e.g., *Uzun v. Germany*, no. 35623/095, 2 September 2010, §66.

22 See, e.g., Information Commissioner's Statement in response to the use of mobile phone tracking data to help during the coronavirus crisis (*ICO*, 28 March 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-

26. We acknowledge that most proposed schemes support the pseudonymisation of data in an attempt to make it entirely anonymous, and that this may be possible at various stages of the contact tracing process. However, from the information published by technical experts, we take the view that it is at least strongly arguable that such pseudonymisation could not entirely *prevent* identification of the infected person and person whom they have contacted. Data is "personal data" for the purposes of the GDPR and DPA if (1) it is capable of indirectly identifying the user by further information that might come to be in the hands of the data controller, unless there is an insignificant risk of identification; or (2) the data concerned individuates the user.[23]

27. Our view is that, even on a decentralised scheme as proposed by DP3T, there remains a possibility that the data concerned would constitute personal data by the following routes:

    27.1. DP3T acknowledge that in extreme circumstances, a person may be indirectly identified under that system. However, those risks are said to be remote and would necessitate significant effort. We note, in any event, that the preponderant view in the tech community is that almost all "anonymised" data can be "de-anonymised" and re-identification is relatively straightforward with sufficient points of reference.[24]

    27.2. Alternatively, it is arguable that a Bluetooth identifier key may itself be personal data if that data "individuates" a person, following the principles as set out by the Court of Appeal in *Vidal-Hall* [25] and the Hight Court in *Bridges*[26]. Bluetooth may be a mark which is capable of singling out and distinguishing a user from others through the process of individuation, even if it does not name the user.

28. For the reasons set out above, we consider that the systems of contact tracing that have been proposed are at risk of processing some "personal data" and will engage Article 8 ECHR and the EU/UK data protection regime. The remainder of our Opinion proceeds on that basis.

29. Against that legal framework, the assessment of whether an infringement of privacy is justified distils into three important questions:

    i. What is the extent of the interference?

    ii. Is the interference 'in accordance with the law' - including whether it contains necessary safeguards to protect persons against arbitrary use?

    iii. Is the interference necessary and proportionate?

30. We address each in turn.

---

blogs/2020/03/statement-in-response-to-the-use-of-mobile-phone-tracking-data-to-help-during-the-coronavirus-crisis/> accessed 15 April 2020.

23 See *Bridges v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at §§116-121.

24 See, e.g., De Montjoye et al, 'On the privacy-conscientious use of mobile phone data' (Scientific Data, 11 December 2018) <https://www.nature.com/articles/sdata2018286> accessed 15 April 2020. See also de Montjoye et al, 'Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask' (*Computational Privacy Group*, 2 April 2020) <https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/> accessed 29 April 2020.

25 *Vidal-Hall et al v Google* [2016] QB 1003 at §115: See Annex 2 at §§48-50.

26 *R (Bridges) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at §§116-121.

i. *What is the extent of the interference?*

31. In a centralised system the level of interference with privacy may be substantial. Such a system is not only likely to inherently identify users but may also combine that smartphone contact tracing data with other available data such as location data, clinical data, or other information from users or available in other datasets. In doing so, a centralised system has the potential to give a central authority an understanding of a "social network" of smartphone users' movements and interactions. It is, of course, true that additional information may be provided voluntarily by users under both a centralised or decentralised system. However, a centralised system is *designed* to collect more detailed information, compared to a decentralised system, which may have advantages from an epidemiological perspective for tracking and monitoring the spread of the disease. .

32. Such a development would however be a significant and unprecedented step in the Government's surveillance of the public.

33. It may be argued that collecting the public's contact data in this way is of little substantive difference to the collection of location data in private datasets to which the Government can already obtain access.[27] In our view, there is not a clear parallel between the two. Private location datasets primarily consist of location data given to private companies with the purported consent of users of certain smartphone apps. That is fundamentally different from a centralised contact tracing system carried out by the Government, through which information about contacts may be obtained without users' consent and with a different level of granularity about their social network than can be provided by location data alone.

34. In a decentralised system, the level of interference is likely to be minimal. Of itself, it would provide no ability for a health authority or other Government department to form a social network of smartphone users' contacts, because there would be no disclosure of information to anyone other than individual users on their device, apart from the publication of anonymous "identifiers" from the smartphones of users who were infected.

ii. *Is an interference in accordance with the law?*

35. Article 8 is a qualified, not absolute, right. This means that interferences with that right may be justified. Article 8(2) provides the framework to justify interferences. Article 8(2) states that a precondition for any interference with a person's right to respect for private life is that it should be "in accordance with the law". This does not require a bespoke legal framework for the interference as a matter of domestic law. It rather requires that the law is not so wide or indefinite as to permit interference with the right on an arbitrary or abusive basis. In *R (Gillan) v Comr. of Police of the Metropolis* [2006] 1 AC 307 at §34, Lord Bingham of Cornhill observed that "*the*

[27] For an example of the pervasive nature of such location data collection see Thompson and Wurzel, 'One Nation Tracked' (*New York Times*, 19 December 2019) <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> accessed 28 April 2020.

lawfulness requirement in the Convention addresses supremely important features of the rule of law". This in turn requires:[28]

> *"the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope and discretion conferred on the competent authorities and the manner of its exercise."*

36. Thus, the data processing involved in operating a contact tracing app, including the manner in which any discretion for the use of that data will be exercised, should be clear and sufficiently predictable for individuals to foresee how it will operate and regulate their conduct accordingly. This does not mean that the law has to codify the answers to every possible issue which may arise with the deployment of new technology. It is enough that it lays down principles which are capable of being predictably applied to any situation.

37. There is not yet any bespoke legislative provision that sets out the requirements of a contact tracing app. In our view, the "quality of law" requirement under Article 8(2) is largely met through the fact that data processing under any contact tracing scheme will have to comply with the legal framework for data processing set out in the GDPR and DPA 2018.[29] That detailed legislation lays down principles which are relevant to the processing of data involved in contact tracing and contains a framework for the enforcement through the Information Commissioner and the courts. The following data protection principles under Article 5 GDPR are of particular relevance (but not exhaustive):

37.1. The processing of such data would have to be done lawfully, fairly and in a transparent manner (Article 5(1)(a) GDPR).

The requirement for legality requires that the processing of data must be permissible under Article 9 GDPR for health data and other "special categories" of personal data and Article 6 GDPR for other personal data. We consider that the processing of personal data would be permissible under two bases:

i. where the purpose of processing the personal data is to manage and monitor the spread of an epidemic in the public interest: Articles 6(1)(d), 6(1)(e), 9(2)(g), 9(2)(h) and 9(2)(i) GDPR; s.10 and Schedule 1, paragraphs 2(2)(f) and 3 DPA, and Article 15(1) of the E-Privacy Directive; or

ii. where the user has provided "freely given, specific, informed and unambiguous indication" consent for the processing of their personal data: Articles 6(1)(a) and 9(2)(a) GDPR and Article 5(3) of the E-Privacy Directive.

---

28 *Catt v the United Kingdom*, no 43514/15, 24 January 2019, §94

29 See, example, *R (Catt) v ACPO* [2015] AC 1065 at §11 (per Lord Sumption), §47 (per Lady Hale).

However, we share concerns raised by both the Information Commissioner on 17 April 2020[30] and the European Data Protection Supervisor, Wojciech Wiewiórowski on 24 April 2020[31] that consent may not be a sustainable basis for such processing, because of (amongst other things) the difficulty in managing the withdrawal of such consent. Accordingly, we consider the 'public interest' to be the safest appropriate basis for such processing to be carried out.

In addition, the processing of data would need to meet the requirements of fairness and transparency.

37.2. Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Article 5(1)(b) GDPR)

The purpose limitation requirements ensure that individuals understand what data is collected and for what reasons, and that it is not processed in unforeseeable or unexpected ways. Adherence to purpose limitation principles would require specificity of the reasons for collecting and processing data and, in turn, guard against "mission drift". Specification of the purpose will also ensure that individuals understand if the app is being deployed for individual proximity notification or for wider purposes such as monitoring the spread of the virus.

Further, data should not be used in ways that are not foreseeable to the individuals whose data it is. Thus, an important qualification to the position taken in the NHSX blog, which states that, "*If we make any changes to how the app works over time, we will explain in plain English why those changes were made and what they mean for you*", is that the subsequent use of data is not at their discretion but limited by the purpose limitation principle.

37.3. Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5(1)(c) GDPR)

Data minimisation would ensure that superfluous data is not processed and ensure that data is only processed as needed to achieve the purpose for the introduction of the contact tracing app. Thus, data should not be used beyond what is strictly necessary to achieve the end goal of the app. For example, where the purpose is proximity notification, only the minimum data needed to achieve that end should be processed.

38. In addition to the application of the data protection principles, there are further concepts within the data protection regime that would need to be addressed.

a. Transparency and DPIA

39. The requirements of transparency in Articles 5(1)(a), 13 and 14 GDPR – and the need for "data protection by design and default" under Article 25 GDPR – would require the provision of clear

[30] Information Commissioner's Opinion, 'Apple and Google joint initiative on COVID-19 contact tracing technology' (17 April 2020).

[31] See, for example, RENEW EUROPE Webinar on COVID-19 contact tracing apps (at 01:50) <https://re.livecasts.eu/webinar-on-contact-tracing-apps> accessed 28 April 2020.

and understandable information to individuals as to how the app would work, what data processing would be involved and the mitigation strategies employed to minimise interferences with rights. Transparency would not be achieved by bundling such information into terms of service agreements, given individuals are unlikely to digest this information in this form.[32] Rather, this information should be made clear through a standalone and publicly accessible document with clear rights for individuals, such as the right to access,[33] rectification[34] and erasure[35] of data. We note that the burden would be on the controller (i.e. the entity or entities controlling the app) to show compliance with these principles under the accountability principle in Article 5(2) GDPR.

40. We are of the view that such transparency would be best achieved through a DPIA that is made widely and publicly available, with appropriate views from the ICO on that DPIA also made public.[36] Article 35 GDPR provides that, where a type of processing is "*likely to result in a high risk to the rights and freedoms of individuals*", the controller must carry out a DPIA. We note the ICO's "*Examples of processing 'likely to result in high risk'*" include "*Innovative technology*" and "*Tracking*" [37]. Further, Article 36 GDPR requires that the controller must consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

41. Our view is that any proposed measure for contact tracing is likely to result in high risk to the rights and freedoms of individuals, particularly considering the use of new technologies that involve tracking. We consider that these technologies must be the subject of a DPIA and consultation with the ICO prior to the processing of personal data.

b. Safeguards

42. In order to be in accordance with the law, there must also be sufficient safeguards to protect the use of contact tracing apps and data from abuse including "scope drift" or "mission creep". There are two obvious ways that such data may be used beyond an immediate response to the current pandemic.

43. *First*, we note that the Oxford University academics involved in the design of the NHSX app have produced a report on the ethics of using contact tracing apps suggesting that there might be legitimate grounds for storing data collected indefinitely as a resource for research purposes.[38] Health research and scientific purposes are legitimate bases under Article 5(1)(b) GDPR, but

---

32 See Recital 32 GDPR and EDPB, *Guidelines on Consent under Regulation 2016/679* (wp259rev.01). See also Joint Committee on Human Rights, *The Right to Privacy (Article 8) and the Digital Revolution* (30 October 2019) <https://publications.parliament.uk/pa/jt201919/jtselect/jtrights/122/122.pdf> accessed 28 April 2020.

33 Article 15 GDPR.

34 Article 16 GDPR.

35 Article 17 GDPR.

36 We note that the Australian Government have conducted an equivalent of a DPIA. It is published here: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

37 ICO, 'Examples of processing 'likely to result in high risk' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>

38 Michael Parker et al, 'The ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic' (*GitHub*, 9 April 2020) <https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/The%20ethics%20of%20instantaneous%20contract%20tracing%20using%20mobile%20phone%20apps%20in%20the%20control%20of%20pandemics.pdfm> accessed 19 April 2020.

there would need to be adequate oversight to ensure that such research fell within the purposes for which the data was collected.

44. *Second*, there is a significant concern among human rights advocates that the contact tracing capability that will be put in place is susceptible to being adopted and used by both private companies and intelligence gathering surveillance for other purposes. This may happen both through use of the data gathered through COVID-19 contact tracing for other purposes, but also through use of the contact tracing capability on smartphones for purposes not relating to COVID-19, e.g. intelligence gathering and other national security concerns.

45. We note that intelligence services are be able to gain access to datasets and equipment capability through warrants authorised under the Investigatory Powers Act 2016. At present, the oversight of such activity would be carried out by the ICO in relation to compliance with the GDPR and DPA 2018 and the Investigatory Powers Commissioner's Office in relation to powers exercised under the Investigatory Powers Act 2016. Whether such oversight powers are sufficient will need to be assessed when the details of the contact tracing scheme are released and the potential ways it may be used become clearer.

46. An additional safeguard would be to enact specific legislation to prohibit use of such datasets by law enforcement or even intelligence services. This approach, at least with regard to law enforcement, has been taken in Australia. We note the Biometric Commissioner's recent statement that "*if surveillance of coronavirus is regarded as valid only during the pandemic then it is important that public trust in such a process is encouraged by regulation approved by Parliament as to the limitations of that surveillance.*"[39]

c. Automated decision making

47. Under Article 22 GDPR, individuals retain the right not to be subject to a decision which "*produces legal effects concerning him or her or similarly significantly affects him or her*" based solely on an automated processing of data without having their views taken into consideration. There is a risk that contact tracing could produce "significant affects" for individual users, such as their ability to leave their home. To this end, we note the joint statement of the Chair of Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe statement that "*users of the digital tracing system should 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.*"[40]

---

[39] Biometrics Commissioner, 'Biometrics Commissioner statement on the use of symptom tracking applications' (21 April 2020) <https://www.gov.uk/government/news/biometrics-commissioner-statement-on-the-use-of-symptom-tracking-applications>. We further note commitment of the Australian Government not to allow the police to access such data "even with a warrant" and the legislative changes introduced in Australia to limit the impact of new technologies introduced to deal with Covid-19. See: https://www.bbc.co.uk/news/world-australia-52433340 and https://www.health.gov.au/resources/apps-and-tools/covidsafe-app. It is not entirely clear whether such prohibition would include intelligence services.

[40] Joint Statement on Digital Contact Tracing Alessandra Pierucci, 'Joint Statement on Digital Contact Tracing' (28 April 2020) <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7>

d. E-Privacy

48. In addition to the requirements under the GDPR and DPA, the "E-Privacy" Directive[41] would be engaged, as the technology will involve the "storage" of information on the terminal equipment of a user. The requirements under Articles 5(3) and 15 of that Directive require such a measure to satisfy the conditions of necessity, appropriateness and proportionality, each of which are considered in more detail at §§53-64 below.

e. Summary

49. The points advanced above set out the minimum requirements that the processing of personal data would have to meet in order to be compliant with the GDPR and be in accordance with the law for the purposes of Article 8 ECHR.

50. Similarly, the processing of personal data involved in contact tracing might not necessarily need specific legislation if it is sufficiently constrained through compliance with data protection law. However, clear legislative provisions setting out the purposes and use of that data would clearly be desirable. Their absence would, at the very least, give rise to concern as to whether there is sufficient clarity as to scope of the processing.[42]

51. Further, we recognise that there are areas not covered within the existing data protection regime. In particular, the regime applies only between data controllers and data subjects. It does not protect against the collective impacts that such technology may have. For instance, the collation of such data can allow for detailed demographic information that could be used to discriminate against groups of people on the basis of location etc. The mechanisms to address such collective harms are a policy consideration and not a matter on which we have been instructed to opine.[43]

52. In addition to the requirement for an interference to be in accordance with the law, it would also have to be proportionate and necessary.

iii. *Proportionality and necessity*

53. Like the Court of Justice of the European Union and ECtHR, the English courts have adopted a strict necessity test in considering any derogation from the rights under Article 8 ECHR or protection of personal data under the UK/EU data protection regimes. For example, in *R (Open Rights Group) v. Secretary of State for the Home Department* [2020] 1 WLR 811, concerning the legality of the immigration exception in Schedule 2 to the DPA 2018, Supperstone J made clear that any exception to the protection of personal data was only available insofar as it is "*necessary*" to achieve a legitimate aim. He stated:

---

41 The E-Privacy Directive is implemented in domestic law by the Privacy and Electronic Communications (EC Directive) Regulations 2003/2426.

42 By analogy see *Catt v UK* (2019) EHRR 7 at §§92-104.

43 We note the proposed The Coronavirus (Safeguards) Bill 2020, by Edwards et al available here: <https://osf.io/preprints/lawarxiv/yc6xu/>.

> *"41. In Guriev v. Community Safety Development (UK) Ltd ... Warby J stated "the test of necessity is a strict one, requiring any interference with the subject's rights to be proportionate to the gravity of the threat to the public interest. The exercise therefore involves a classic proportionality analysis"*
>
> *42. [...] The requirements of necessity and proportionality provide, in my view, an adequate set of safeguards to protect individual data subject rights. As Lord Sumption JSC stated in Catt [2015] AC 1065 (para 11), the rules governing the scope and app of measures, as well as minimum safeguards, "need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them. Their application, including the manner in which any discretion will be exercised, should be reasonably predictable, if necessary with the assistance of expert advice. But except perhaps in the simplest cases, this does not mean that the law has to codify the answers to every possible issue which may arise. It is enough that it lays down principles which are capable of being predictably applied to any situation.""*

54. See also *R (El Gizouli) v. Secretary of State for the Home Department* [2020] 2 WLR 857 at §158, where Lord Kerr explained that:[44]

> *"I consider that the requirement that the data be limited to that which is strictly necessary behoves the data controller to make an assessment of what, in the context of the DPA, is strictly necessary and, since it is accepted that the Home Secretary did not have regard to his duties as data controller, the special circumstances gateway was not available. Moreover, it is not enough to say that the data protection provisions were substantially met, where direct, personal evaluation was required."*

55. The necessity requirements within the DPA require close scrutiny by any decision-maker introducing a contact tracing app. Under the data protection regime, such necessity requirements apply to *any* data controller, whether a public authority or private entity.[45]

56. The legal principles for assessing necessity are well established.[46] The proportionality assessment comprises four steps:[47]

    i. whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;

    ii. whether it is rationally connected to the objective;

    iii. whether a less intrusive measure could have been adopted without unacceptably compromising the objective; and

    iv. whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

---

44 See also, §§9, 158, 210

45 The scope of the obligations on a private entity data controller, such as an employer, are beyond the scope of this analysis.

46 See Annex 2, §§20-22.

47 *Bank Mellatt v HM Treasury (No. 2)* [2014] AC 700 at §20 (per Lord Sumption) and §74 (per Lord Reed).

57. In our view, the first two steps are likely to be easily satisfied in relation to the need for a contact tracing app in the context of an unprecedented global pandemic.

58. However, in assessing step (3) it will be important to be clear on the *specific objective* of the contact tracing technology. There are a range of proposals put forward, each with different utility for different purposes.

59. One purpose may be to alert members of the public to the risk that they may be infected followed by the use of other methods – such as obtaining information by consent or manual contact tracing – to enable authorities to obtain the additional data needed to formulate policy, carry out research and allocate resources. This would in effect be a proximity alerting device. In such circumstances, it is difficult to see how any contact tracing app beyond the decentralised system proposed by DP3T would be necessary and satisfy the third and fourth steps.

60. In contrast, if the health authorities' objective for the app is much broader – including using the app to gather additional data beyond just alerting potentially infected people, so that the spread of the virus can be closely monitored on a granular and individual level – arguments for a centralised system may be stronger. The greater amount of data that would be collected in a centralised system is an important benefit in its favour. However, any such argument will require much more factual justification. That legal assessment is likely to be determined by the following evidential issues:

- What is the stated purpose and objective of the app and exactly what data does it intend to gather?
- Is there technical evidence to suggest that it will be effective in gathering the data needed to fulfil that objective?
- What is the participation required from the public to make that app effective?[48]
- Can that participation be achieved voluntarily?
- Can the data be obtained in less intrusive ways, for example by the app simply triggering notifications, but the users providing the further information in other ways?
- How intrusive is the use of this app compared to existing interferences with privacy, such as manual contact tracing, or voluntary smartphone location tracking?

61. Insofar as a decentralised system is concerned, we further note:

- The ICO and EDPB suggest that the DP3T proposal complies with the requirements for "data protection by design and by default" under Article 25 GDPR and the principle of "data minimisation" under Article 5 GDPR.

[48] A report to NHSX from Oxford University academics on 16 April 2020 concluded that the COVID-19 pandemic could be suppressed with 80% of all smartphone users, or 56% of the population overall, using a contact tracing app. Robert Hinch et al, 'Effective Configurations of a Digital Tracing App: A report to NHSX' (16 April 2020) <https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf> accessed 28 April 2020

- Technical measures, including data anonymisation and pseudonymisation, the processing of personal data on device to avoid unlawful access to the data, deletion of the data concerned after 14 days and the requirement of explicit consent, are inherent within the DP3T system, to protect the rights of data subjects.

- Public authorities would not have access to any anonymised and aggregated data on social distances, and the number or location of people who may be infected.

- European states[49] are increasingly choosing to deploy a decentralised system, such as the DP3T protocol.

62. In our view, a voluntary decentralised system, such as DP3T, involving the processing of personal data on users' devices, is the least intrusive of the existing proposals and may have little difficulty satisfying the requirements of necessity and proportionality.

63. The more difficult question is whether the decentralised model is sufficient to achieve the public health objective, including whether it would need to be made compulsory in order to have the effectiveness it needs. There is, however, insufficient evidence before us that addresses the points made at §60 above to justify a mandatory app, which we consider further below. It is also significant that the European Parliament and others appear to favour a voluntary decentralised system and have not suggested it would be inadequate to meet contact tracing objectives.

64. Considering the matters raised above, we are of the view that the DP3T system would be likely to present a justified, proportionate and necessary interference with Article 8 ECHR and comply with the requirements of the data protection legislation. In contrast, a centralised system may provide some additional functionality but also involves a greater interference with individual rights. We acknowledge in particular that a centralised system may have increased epidemiological utility, but the uncertainty as to the efficiency, uptake and efficacy of such a centralised system would have to be addressed with sufficient evidence before its introduction could be justified. There is insufficient evidence before us at present to explain how the deployment of a centralised system would be the least intrusive means to achieve effective contact tracing, in preference to a decentralised system supplemented by voluntary disclosure of additional information to provide that increased functionality. A clear indication of what a centralised system's objectives are, it's efficacy and likely uptake and why the Government considers it is necessary for contact tracing, in preference to a decentralised system, would be critical in order to establish its compliance with Article 8 and/or relevant data protection legislation.[50]

ii. <u>Mandatory use of the app for all smartphone users</u>

65. For the reasons outlined above, we do not consider specific new legislation would be necessary in order for a voluntary smartphone contact tracing system to be lawful if it is sufficiently

49 Most recently, Germany has endorsed and taken up DP3T, following Switzerland, Austria, Estonia. Most states are still considering their position.

50 We suggest that this is done through a DPIA, as to which see §39 - 41

constrained through compliance with data protection law. Nevertheless, such legislation may be desirable and provide clarity and scrutiny as well as enhancing transparency and public trust.

66. However, it is our view that specific legislation would be *essential* for a compulsory or mandatory contact tracing system. This is not merely because of the greater nature of the interference with Article 8 ECHR that a mandatory system would involve, but also because it would need to specify clearly the following matters:

- Who would be placed under the obligation and in what circumstances?
- What, if any, exceptions apply?
- What sanctions would be imposed on those who did not comply?
- What powers would be given to police and others to enforce those sanctions?

67. We emphasise that a centralised and mandatory system, if combined with other data, would potentially provide the Government with a wholly unprecedented level of granular data about the social network of the majority of the population. Even in the midst of a serious pandemic we believe such interference would require an equally unprecedented level of evidential justification to meet legal requirements and ensure public confidence.

III. DATA SHARING BETWEEN PUBLIC AND PRIVATE SECTOR

Arrangements for the Collection of Confidential Patient Information

68. We have two principal concerns about the current legality of the Government's data sharing plans. The first is that the mandatory notices under which such data sharing occurs appear to be deficient for the purposes the Government intends. The second is that a plan to create a "data store" through which to share data with a number of private data companies does not comply, thus far, with data protection principles.

Data sharing under COPI Notices

i. The Notices

69. On 17 March 2020, the Health Secretary and NHS England directed NHS Digital to establish and operate a system for the collection and analysis of data in connection with "COVID-19 Purposes". Paragraph 2 of those directions sets out the "COVID-19 Purposes".[51] They include understanding the risk to public health; identifying locating and collecting information about patients; monitoring and managing the response to COVID-19; delivering services to patients and carrying out research and planning around COVID-19.

70. The Health Secretary also issued four notices pursuant to regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 ("COPI Regulations") to require NHS Digital to process confidential information for the purposes in regulation 3(1), in so far as those purposes related to the COVID-19 pandemic. The COPI Notices were issued to:

70.1. NHS England & Improvement dated 20 March 2020 ("COPI Notice 1");

70.2. NHS Digital dated 17 March 2020 ("COPI Notice 2");

70.3. *"Organisations providing health services, general practices, local authorities and arm's length bodies of the Department of Health and Social Care"* dated 20 March 2020 ("COPI Notice 3");

70.4. *"All GP practices in England, whose IT systems are supplied by The Phoenix Partnership (TPP) or Egton Medical Information Systems (EMIS) or Egton Medical Information Systems (EMIS) [...] to require them to release primary care patient data, in respect of UK Biobank's consented participants only, to UK Biobank"* ("COPI Notice 4").

71. Pursuant to paragraph 1 of COPI Notices 1 to 3, the purpose of the Notices is to require organisations to process confidential patient information for the purposes set out in regulation 3(1) of the COPI Regulations.

---

[51] NHS Digital, 'COVID-19 Public Health Directions' <https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/covid-19-public-health-directions-2020> accessed 28 April 2020.

Legal Analysis

72. The COPI Notices appear to be legally deficient in that they seek to permit data sharing beyond that which the COPI Regulations permit.

73. The COPI Notices all expressly stipulate that the addressees of the Notices are required to process *"confidential patient information"*. In *Lewis v Secretary of State for Health* [2008] EWHC 2196 (QB) Foskett J stated (obiter) that the COPI Regulations can only regulate the processing of confidential information generated within a NHS context and cannot authorise the processing of confidential information which is generated outside the NHS.

74. However, none of the COPI Notices contain anything that explicitly or implicitly reflects that restriction. Since COPI Notice 3 is addressed to a broad range of recipients including "*Local Authorities*", "*Arm's length bodies of the Department of Health and Social Care*" and "*Organisations providing health services*", it is likely that some recipients of the Notice will be in possession of confidential patient data that was generated outside the NHS. If it is the Government's intention that data is shared under the COPI Notices includes that generated outside a NHS context, that is legally inconsistent with the comments of Foskett J in *Lewis*. Conversely, if the Government intends such sharing under the COPI Notices to exclude data generated outside a NHS context, that would not be clear to the recipients of those Notices.

75. Additionally, under regulation 7(2) of the COPI Regulations, no person may process confidential patient information unless they are a health professional or someone who owes an equivalent duty of confidentiality as would be owed by a health professional. COPI Notices 1, 2 and 3 refer to the need to comply with regulation 7, but do not explicitly indicate what this restriction entails in practice. COPI Notice 4 inexplicably does not refer to regulation 7 at all, which may be taken to imply, wrongly, that recipients of that Notice are not required to comply with the important restriction contained in that Regulation.

ii. Creation of a 'data store' through which to share data

The data store proposal

76. On 28 March 2020, NHSX published a blog post[52] explaining that the Government had commissioned NHS England and NHSX to develop a "data platform" or "data store" to provide those organisations with "*secure, reliable and timely data – in a way that protects the privacy of our citizens – in order to make informed, effective decisions.*" It stated that the data would remain under the control of NHS England.

77. The blog post made clear that private companies had been involved in creating the data store, including Microsoft, Palantir Technologies UK, Amazon Web Services, Google and Faculty (a London based AI technology specialist).

[52] Gould et al, 'The power of data in a pandemic' (*NHS Blog*, 28 March 2020) https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/ accessed 15 April 2020.

78. A *Guardian* article published on 12 April 2020[53] raised concerns about the involvement of the private companies, casting doubt on the role ascribed to them in the blogpost:

> *"The government had previously said it would use Faculty and Palantir in a Covid-19 data project. But the full scope of that operation, and the sensitive nature of patient-level data being used, is revealed in the documents seen by the Guardian. One portion of the project involves giving leaders in the NHS, Cabinet Office and Downing Street a live feed of "aggregate" statistics on hospitalisations, availability of critical care beds, ventilator orders and oxygen supplies.*
>
> *However, the documents also appear to show the project includes large volumes of data pertaining to individuals, including protected health information, Covid-19 test results, the contents of people's calls to the NHS health advice line 111 and clinical information about those in intensive care. [...]*
>
> *The documents also suggest that:*
>
> - *While anonymised, confidential 111 information in the Covid-19 datastore may include people's gender, postcode, symptoms, the mechanism through which any prescription was dispatched to them, and the precise time they ended the call.*
> - *The project appears to be using a "pseudo NHS number" to cross-match large datasets, including a master patient index, an existing NHS resource that uses "social marketing data" to segment the British population into different "types" at household level.*
> - *While not a current priority, phone location data could be used in the datastore after it was "offered" to the government by two private companies for help with contact tracing. The NHS declined to say which companies had offered the location data or how it would be used.*
> - *Faculty's proposed simulation of a policy described as "targeted herd immunity" was part of an NHSX and Faculty planning document considered around 23 March, more than a week after ministers insisted the controversial policy was no longer being contemplated."*

Legal Analysis

79. Neither the directions issued on 17 March 2020 by the Health Secretary, nor paragraph 1 of the COPI Notices provide for the sharing of data with the private companies set out above: Palantir, Amazon Web Services, Faculty and Google. At present it is entirely unclear how such data sharing is intended to take place, and whether the characterisation of the sharing in the NHSX blogpost is how the data will be shared with those private companies.

80. Additionally, if identifiable information is being shared between NHS Digital and the private companies, it must be compliant with the data protection regime. The sharing requirements are set out in the ICO's *Draft Data Sharing Code of Practice*:

80.1. a data controller must consider whether a DPIA is required and, if so, conduct a DPIA;

---

[53] Paul Lewis, David Conn and David Pegg, 'UK Government using confidential patient data in coronavirus response' (*The Guardian,* 12 April 2020) https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response accessed 15 April 2020.

80.2. a data sharing agreement must prescribe the purpose of the data sharing, rules governing the respective roles of the parties and access to the data concerned and procedures to allow data subjects to exercise their rights under Chapter III of the GDPR;

80.3. when sharing data, the data controller must follow the data protection principles set out in Article 5 GDPR, including the obligation to ensure that the arrangements safeguard the right to protection of personal data by design;

80.4. the data controller must identify a lawful basis for processing personal data.

81. These data sharing requirements are legally significant and cannot be ignored by the NHS and partners with whom it wishes to work. We note that, in July 2017, an ICO investigation found that the provision of 1.6 million patients details by the Royal Free NHS Foundation Trust to Google DeepMind for the purpose of clinical safety testing did not comply with data protection principles in force at the time under the Data Protection Act 1998, namely, Principle 1 (lawfulness, fairness and transparency), Principle 3 (data minimisation), Principle 6 (rights of the data subject) and Principle 7 (integrity and confidentiality). The processing of patient records by DeepMind, for which the patients had not given informed consent, differed significantly from what they might reasonably have expected to happen to their data when presenting at the Royal Free.[54]

[54] ICO Decision Notice, 'RFA0627721 – provision of patient data to DeepMind' (3 July 2017) <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf> accessed 15 April 2020.

IV. IMMUNITY PASSPORTS

82. On 2 April 2020, Matt Hancock MP stated that the Government was considering the possibility of issuing "immunity" certificates to allow the immune to return to work.[55] On 28 April 2020, the Chief executive of NHSX, Matthew Gould, told the Commons science and technology committee that NHSX has been approached by "any number of organisations" who can provide the technology for immunity passports. He added that NHSX is in the "very early stages" of looking through immunity passports as a solution.[56]

Legal analysis

83. At present, as far as we are aware, there are no plans to introduce immunity passports[57]. We understand that it is not even clear whether it is scientifically possible for immunity to be assessed reliably, prior to a vaccine being developed.

84. The introduction of profiling and immunity passports would involve a significant interference with the rights under Article 8 ECHR, Articles 7 and 8 of the Charter and the EU/UK legislation on the right to privacy and protection of personal data.

85. Further, if an individual's health status was partly classified on the basis of their location or immigration status, it might give rise to stigmatisation and indirect discrimination. Article 21 of the Charter and Article 14 ECHR prohibit discrimination on the grounds of social origin, birth and property. By way of example, excluding a group of individuals who live in areas with poorer standards of healthcare from benefiting from measures to ease quarantine and access services, compared to others who live in more affluent areas, is likely to amount to a difference in treatment, which must be justified. It is also likely to engage the public sector equality duty under s.149 of the Equality Act 2010, giving rise to the need to conduct an equality impact assessment. Other rights under the ECHR which are also likely to be engaged are Article 5 (right to liberty) and Article 11 (freedom of assembly and association).

86. Any measures for immunity passports must also operate within a legal framework and in a reasonably predictable manner (see §53 above). There is (at the very least) significant doubt as to whether these requirements are capable of being satisfied by any system of immunity certification.

87. Absent further information, we have seen no basis on which it could be said that profiling and immunity passports are strictly necessary, appropriate and proportionate to the objective of managing and monitoring the spread of COVID-19. Any such proposal would require objective evidence to substantiate the factual and technical case that such a significant interference with fundamental rights is justified. To this end, we note that the WHO questioned the necessity of such immunity passports, noting "*At this point in the pandemic, there is not enough evidence about the*

---

55 Harry Cockburn, 'Coronavirus: How mass testing and health passports could ease UK lockdown' (*The Independent,* 2 April 2020) <https://www.independent.co.uk/news/health/coronavirus-testing-uk-health-passports-certificates-lockdown-end-when-a9442866.html> accessed 15 April 2020.

56 https://www.hsj.co.uk/coronavirus/nhsx-exploring-coronavirus-immunity-passports/7027527.article

57 We note the concerns that contact tracing apps on smartphones may act as a proxy for immunity passports (see: Patrick McGee, Hannah Murphy, and Tim Bradshaw, "Coronavirus apps: the risk of slipping into a surveillance state" (*Financial Times*, 28 April 2020).

effectiveness of antibody-mediated immunity to guarantee the accuracy of an "immunity passport" or "risk-free certificate"."[58]

88. We further note that the medical knowledge on COVID-19 remains both incomplete and in flux[59] and, at present, it is not clear what basis "immunity" would be measured against; particularly where the reality of "immunity" is unknown and not capable of definition.

89. We would be pleased to consider the matter further if proposals to introduce profiling and immunity passports are published.

[58] WHO, 'Immunity passports in the context of COVID-19' (24 April 2020) <https://www.who.int/publications-detail/immunity-passports-in-the-context-of-covid-19> accessed 28 April 2020.

[59] See, e.g., David Wallace-Wells, 'We Still Don't Know How the Coronavirus Is Killing Us' (*New York Magazine,* 26 April 2020) < https://nymag.com/intelligencer/2020/04/we-still-dont-know-how-the-coronavirus-is-killing-us.html> accessed 28 April 2020.

V. CONCLUSION

90. Our analysis and conclusions are set out above, in the body of this Opinion and Executive Summary. Our view is that a detailed and thorough evidential basis will need to be advanced for any technological measure the Government introduces in response to the COVID-19 pandemic.

91. To gain such evidence, those formulating policy may wish to draw widely and deeply on the knowledge of technologists, academics, oversight bodies and other experts on data protection. They may also wish to consider recommendations on the need for an independent panel of such experts to provide advice on the use of data, in a similar way to expert advice provided by medical and scientific experts in other contexts. We note that a number of analyses of technological solutions to COVID-19 have suggested the need for oversight mechanisms and sunset clauses for any new powers.[60] We endorse those views.

92. We would be pleased to discuss any aspect of this Opinion with those instructing us.

RAVI NAIK	MATTHEW RYDER QC	GAYATRI SARATHY
	EDWARD CRAVEN	
AWO	*Matrix*	*Blackstone Chambers*

30 April 2020

[60] See, e.g., Ada Lovelace Report (n.1), p.10.

ANNEX 1: DEFINED TERMS

Communicable disease	an infectious disease caused by a contagious agent which is transmitted from person to person by direct contact with an infected individual or by indirect means such as exposure to a vector, animal, fomite, product or environment, or exchange of fluid, which is contaminated with the contagious agent	Decision No 1082/2013 on serious cross-border threats to health("**2013 Decision**"), Article 3(b)
Communications data	the "who, when, where, how and with whom" of a communication, which comprises of subscriber data, service data and traffic data.	*Davis* [2016] 1 CMLR 13 §13
Confidential patient information	(a) the identity of the individual in question is ascertainable – (i) from that information, or (ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and (b) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.	NHSA 2006, s.251(11)
Consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her	GDPR, Article 4(11) (see also Article 7 GDPR)
Contact tracing	measures implemented in order to trace persons who have been exposed to a source of a serious cross-border threat to health, and who are in danger of developing or have developed a disease	2013 Decision, Article 3(c)
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law	GDPR, Article 4(7) See also *Ittihadieh v. 5-11 Cheyne Gardens RTM Co Ltd* [2018] QB 256 §§70–71
Data concerning health	personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status	GDPR, Article 4(15) DPA, s.205
Data subject	identified or identifiable living individual to whom personal data relates	GDPR, Article 4(1) DPA 2018, s.3(5)
Epidemiological surveillance	systematic collection, recording, analysis, interpretation and dissemination of data and analysis on communicable diseases and related special health issues	2013 Decision, Article 3(d)
Location data	any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service	E-Privacy Directive Article 2(c)
Medical purposes	the purposes of any of –	NHSA 2006, s.251(12)

	(a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services, and (b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment	
Patient information	(a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and (b) information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information.	NHSA 2006, s.251(10)
Personal data	any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	GDPR, Article 4(1) DPA 2018, s.3(2) and (3)
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction	GDPR, Article 4(2) DPA 2018, s.3(4)
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller	GDPR, Article 4(8)
Profiling	any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements	GDPR, Article 4(3)
Pseudonymisation	the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person	GDPR, Article 4(5)
Public health	all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality	Regulation 1338/2008 on Community statistics on public health and health and safety at work, Article 3(c)

Public health measure	a decision or an action which is aimed at preventing, monitoring or controlling the spread of diseases or contamination, combating severe risks to public health or mitigating their impact on public health	2013 Decision, Article 3(f)
Serious cross-border threat to health	a life-threatening or otherwise serious hazard to health of biological, chemical, environmental or unknown origin which spreads or entails a significant risk of spreading across the national borders of Member States, and which may necessitate coordination at Union level in order to ensure a high level of human health protection	2013 Decision, Article 3(g)
Service data	information relating to the use made by any person of a communications service and for how long, e.g., itemised telephone records showing the date, time and duration of calls and to what number each call was made.	*Davis* [2016] 1 CMLR 13 §13(b).
Subscriber data	information held or obtained by a communications service provider in relation to a customer, for example their name, address and telephone number.	*Davis* [2016] 1 CMLR 13 §13(a).
Traffic data	data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof	E-Privacy Directive Article 2(b)

ANNEX 2: LEGAL PROVISIONS AND CASE LAW

A. EUROPEAN CONVENTION ON HUMAN RIGHTS AND HRA 1998

1. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life guaranteed by Article 8.[61] Article 8, which is given effect in domestic law by the Human Rights Act 1998, provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The meaning of "private life"

2. The concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person, aspects of a person's physical and social identity, name and other means of personal identification.[62]

3. The phrases "*physical and psychological integrity*" and "*physical and social identity*" are the central value protected by Article 8 and have been described as *the "personal autonomy of every individual ... [which] marches with the presumption of liberty enjoyed in a free polity; a presumption which consists in the principle that every interference with the freedom of the individual stands in need of objective justification*": *R (Wood) v. Comr. of Police of the Metropolis* [2010] 1 WLR 123, §§20-21.

4. Yet the reach of Article 8(1) is not without limit. In *Wood* at §22 (cited with approved by Lord Toulson in *In re JR 38* [2016] AC 1131 at §22), Laws LJ stated:

> "This cluster of values, summarised as the personal autonomy of every individual and taking concrete form as a presumption against interference with the individual's liberty, is a defining characteristic of a free society. We therefore need to preserve it even in little cases. At the same time, it is important that this core right protected by Article 8, however protean, should not be read so widely that its claims become unreal and unreasonable. For this purpose, I think there are three safeguards, or qualifications. First, the alleged threat or assault to the individual's personal autonomy must (if Article 8 is to be engaged) attain 'a certain level of seriousness'. Secondly, the touchstone for Article 8(1)'s engagement is whether the claimant enjoys on the facts a 'reasonable expectation of

---

61 *Satakunnan v. Finland*, no. 931/13, 27 June 2017, §137.

62 *S and Marper v. United Kingdom*, no. 30562/04, 4 December 2008, §66.

privacy' (in any of the senses of privacy accepted in the cases). Absent such an expectation, there is no relevant interference with personal autonomy. Thirdly, the breadth of Article 8.1 may in many instances be greatly curtailed by the scope of the justifications available to the state pursuant to Article 8.2."

5. The systematic collection and storage of data relating to the "private life" of an individual may amount to an interference within the meaning of Article 8 even if that data was collected in a public space or concerned exclusively the person's professional or public activities. In *S and Marper v. United Kingdom*, no. 30562/04, 4 December 2008, which concerned the retention of biometric information in the form of DNA and fingerprint samples, the ECtHR emphasised the significance of the protection of personal data as part of protecting Article 8(1) rights:

> "67. The mere storing of data relating to private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained. …
>
> 103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention."

6. In that case, the ECtHR held that cellular samples and DNA profiles taken by the police in criminal investigations were, by their nature and the amount of personal information contained, covered by the concept of "private life". Even if the information could be considered objective and factual, it concerned unique aspects of identity as well as being relevant to health issues. Fingerprints contained less information but also constituted personal data; they contained external identification features comparable to personal photographs or voice samples and were unique to the persons concerned. However, since fingerprints were less data sensitive than DNA samples and profiles, the ECtHR held that the justification of interference might be less onerous.[63]

7. *Uzun v. Germany*, no. 35623/095, 2 September 2010, concerned the lawfulness of GPS surveillance of a German national as part of a criminal investigation. The ECtHR held that, while information about movement obtained by a GPS tracking device was less intrusive as not revealing a person's conduct, opinion or feelings, the collection of data over a period to draw up a pattern of movements and the processing and use of that data amounted to an interference

63 *S and Marper*, §§70-77, 80-86.

with private life.[64] Similarly, in *Shimovolos v. Russia*, no. 30194/09, 21 June 2011, the ECtHR found that the collection and storage of data relating to a human right's activities movements amounted to an interference with his private life as protected by Article 8(1).[65]

8. In *Z v Finland,* no. 22009/93, 25 February 1997, the ECtHR stated at §38 that:

> "the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.
>
> Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community.
>
> The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention."

9. *R (Bridges) v. Chief Constable of South Wales Police* [2020] 1 WLR 672 concerned the use by the police of automatic facial recognition cameras in public spaces. The Divisional Court held that Article 8(1) is engaged "*if biometric data is captured, stored and processed, even momentarily*". In this regard, "*the fact that the process involves the near instantaneous processing and discarding of a person's biometric data...does not matter*" (§59).

"In accordance with the law"

10. The concept of "in accordance with the law" requires the impugned measure to have some basis in domestic law and meet quality of law requirements concerning accessibility and foreseeability as to the circumstances in which and conditions under which authorities are empowered to interfere with the rights under Article 8.

11. For domestic law to meet this requirement, it must afford adequate legal protection against arbitrariness and indicate with sufficient clarity the scope and discretion conferred on the

---

64 *Uzun v. Germany*, no. 35623/095, 2 September 2010, §§49-53.
65 *Shimovolos v. Russia*, no. 30194/09, 21 June 2011, §66.

competent authorities and the manner of its exercise. In *R (Gillan) v. Comr. of Police of the Metropolis* [2016] 2 AC 307 at §34, Lord Bingham explained the requirement as follows:

> "The lawfulness requirement in the Convention addresses supremely important features of the rule of law. The exercise of power by public officials, as it affects members of the public, must be governed by clear and publicly accessible rules of law. The public must not be vulnerable to interference by public officials acting on any personal whim, caprice, malice, predilection or purpose other than that for which the power was conferred. This is what, in this context, is meant by arbitrariness, which is the antithesis of legality. This is the test which any interference with or derogation from a Convention right must meet if a violation is to be avoided."

12. The general principles applicable to the "in accordance with the law" standard were set out by the Divisional Court in *R (Bridges) v. Chief Constable of South Wales Police* [2020] 1 WLR 672:

> "(1) The measure in question (a) must have "some basis in domestic law" and (b) must be "compatible with the rule of law", which means that it should comply with the twin requirements of "accessibility" and "foreseeability": *Sunday Times v United Kingdom* (1979) 2 EHRR 245; *Silver v United Kingdom* (1983) 5 EHRR 347; and *Malone v United Kingdom* (1984) 7 EHRR 14 .
>
> (2) The legal basis must be "accessible" to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must also be "foreseeable" meaning that it must be possible for a person to foresee its consequences for them and it should not "*confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself*": Lord Sumption JSC in *P* [2019] 2 WLR 509, para 17.
>
> (3) Related to (2), the law must "*afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise*": *S v United Kingdom* 48 EHRR 50, paras 95 and 99.
>
> (4) Where the impugned measure is a discretionary power, (a) what is not required is "*an over-rigid regime which does not contain the flexibility which is needed to avoid an unjustified interference with a fundamental right*" and (b) what is required is that "*safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights*": per Lord Hughes JSC in *Beghal v Director of Public Prosecutions* [2016] AC 88, paras 31-32. Any exercise of power that is unrestrained by law is not "*in accordance with the law*".
>
> (5) The rules governing the scope and application of measures need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them: per Lord Sumption JSC in *Catt*, at para 11.
>
> (6) The requirement for reasonable predictability does not mean that the law has to codify answers to every possible issue: per Lord Sumption JSC in *Catt*, at para 11."

13. There are various stages at which data protection issues under Article 8 may arise, including during collection, storage, use and communication of data.[66] The level of precision required of domestic legislation depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed.[67]

14. In *S and Marper*, the ECtHR concluded that, in the context of proceedings challenging the legality of arrangements for the retention and use of fingerprints and DNA, it was necessary for there to be "*detailed rules governing the scope and application of measures*" so as to provide sufficient guarantees against the risk of abuse and arbitrariness.[68] The Court went on to state:

> "103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any … use of personal data as may be inconsistent with the guarantees of this article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse. The above considerations are especially valid as regards the protection of special categories of more sensitive data and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family.
>
> 104. The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime. However, the intrinsically private character of this information calls for the court to exercise careful scrutiny of any state measure authorising its retention and use by the authorities without the consent of the person concerned."

15. In the context of secret measures of surveillance by authorities, compatibility with the rule of law requires that domestic law provides adequate protection against an arbitrary interference with rights under Article 8. *Weber v. Germany* concerned an admissibility decision on the lawfulness of general surveillance of a proportion of international satellite communications. The Court applied the six minimum safeguards which should be set out by a regime of bulk interception of communications:

---

66 *Catt v. United Kingdom*, no. 43514/15, 24 January 2009, §§94-95.
67 *S and Marper v. United Kingdom*, no. 30562/04, 4 December 2008, §§95-96.
68 *S and Marper*, §99.

(1) the nature of the offences which may give rise to an interception order;

(2) a definition of the categories of people liable to have their telephones tapped;

(3) a limit on the duration of telephone tapping;

(4) the procedure to be followed for examining, using and storing the data obtained;

(5) the precautions to be taken when communicating the data to other parties; and

(6) the circumstances in which recordings may or must be erased or the tapes destroyed.[69]

16. The *Weber* safeguards do not apply with the same rigour outside the specific context of surveillance of telecommunications. In *Uzun*, the Court held that, whilst it is not barred from "*gaining inspiration*" from *Weber*, the "*rather strict standards ... are not applicable as such to cases such as the present one, concerning surveillance via GDP of movements in public spaces and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations.*"[70]

17. The Court applied the "*more general principles*" on adequate protection against arbitrary interference with Article 8 set out in *S and Marper*.[71] It found that the interference with the Applicant's rights was in accordance with the law, referring to the following elements of the regime:

(1) the duration of surveillance measures was subject to a requirement of proportionality;

(2) surveillance could only be ordered against a person suspected of a criminal offence of considerable gravity or, in limited circumstances, against a third person suspected of being in contact with the accused;

(3) the courts could review the legality of a measure of surveillance and, in the event that it was found to be unlawful, had discretion to exclude the evidence obtained thereby from use at the trial.

18. In *Ben Faiza v. France*, no 31446/12, 8 February 2018, the complaint concerned the real-time geolocation of the Applicant's vehicle by GPS. Applying *Uzun*, the ECtHR found that French

69 *Weber & Saravia v Germany*, no 54934/00, 29 June 2006, §95.
70 *Uzun v. Germany*, no. 35623/095, 2 September 2010, §66.
71 *ibid.*

law did not, at the relevant time, prescribe the scope of the authorities' discretion with sufficient clarity.[72]

19. The Applicant also complained about the use of Article 77-1-1 of the Criminal Procedure Code, a power of a prosecutor to request documents or data relevant to an investigation from third parties, which was used to request historic cell tower data in relation to him from a telephone company. The ECtHR considered that the power, which applied only to existing records necessary for the purpose of a pending criminal investigation, was sufficiently foreseeable.[73] The regime contained the following features: (i) it was subject to prior authorisation by a prosecutor; (ii) if the documents concerned lawyers or journalists (amongst others), they could not be delivered without their consent; and (iii) the criminal courts could review the legality of the measure and exclude any material obtained unlawfully from the trial.[74]

"Necessary in a democratic society"

20. An interference is "necessary in a democratic society" for a legitimate aim if it answers to a "pressing social need", if it is proportionate to the legitimate aim pursued and if the reasons adduced by the authorities to justify it are "relevant and sufficient". The ECtHR leaves a "margin of appreciation" to states in this assessment. Similarly domestic courts leave a "margin of discretion" to competent authorities in relation to their decision making.[75]

21. The evaluation of whether the reasons cited for the interference are relevant and sufficient remains subject to review by the Court for conformity with the requirements of the Convention. In *AMV v. Finland*, no. 53251/13, 23 March 2017, the ECtHR set out the relevant principles as follows:[76]

> "82. … [I]n order to determine the proportionality of a general measure, the Court must primarily assess the legislative choices underlying it. In accordance with the principle of subsidiarity, the quality of the parliamentary and judicial review of the necessity of the measure is of particular importance in this respect, including to the operation of the relevant margin of appreciation (see, mutatis mutandis, *Animal Defenders International v. the United Kingdom* [GC], no. 48876/08, § 108, ECHR 2013 (extracts)).
>
> 83. A margin of appreciation must, inevitably, be left to the national authorities, who by reason of their direct and continuous contact with the vital forces of their countries are in principle better placed than an international court to evaluate local needs and conditions

72 *Ben Faiza v France*, no 31446/12, 8 February 2018, §§58-61.
73 *ibid*, §§69-76.
74 *ibid*, §§32, 35, 73.
75 *S and Marper*, §§101-102; *Catt*, §109.
76 *AMV v. Finland*, no. 53251/13, 23 March 2017, §§82-84.

(see *Maurice v. France* [GC], no. 11810/03, § 117, ECHR 2005-IX). This margin will vary according to the nature of the Convention right in issue, its importance for the individual and the nature of the activities restricted, as well as the nature of the aim pursued by the restrictions. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see, for example, *Parrillo v. Italy* [GC], no. 46470/11, § 169, ECHR 2015; and *Dubská and Krejzová*, cited above, § 178). … [T]he margin is also reduced where a particularly vulnerable group is subjected to differential treatment on grounds that are not specifically linked to relevant individual circumstances.

84. The procedural safeguards available to the individual will be especially material in determining whether the respondent State has, when fixing the regulatory framework, remained within its margin of appreciation. In particular, the Court must examine whether the decision-making process leading to measures of interference was fair and such as to afford due respect to the interests safeguarded to the individual by Article 8 (see Connors, cited above, § 83; *Buckley*, cited above, § 76; and *Chapman v. the United Kingdom* [GC], no. 27238/95, § 92, ECHR 2001-I)."

22. The four-part test to meet the requirement of proportionality was set out by the Supreme Court in *Bank Mellat v. HM Treasury (No 2)* [2014] AC 700 at §74 in the following terms:

(1) whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;

(2) whether it is rationally connected to the objective;

(3) whether a less intrusive measure could have been adopted without unacceptably compromising the objective; and

(4) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

B. EU CHARTER OF FUNDAMENTAL RIGHTS

23. Article 7 of the Charter guarantees every person the right to respect for their family life, home and communications. Article 8 makes express provision for the protection of personal data:

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

24. Article 52(1) provides that any limitation on the exercise of rights under the Charter is subject to the principles of proportionality and necessity. Article 52(3) states that, insofar as the Charter contains rights which correspond to rights guaranteed under the ECHR, the meaning and scope of the rights shall be the same.

25. The Charter remains in force until "exit day", i.e. 31 December 2020, pursuant to s.1A of the European Union (Withdrawal Agreement) Act 2018 ("EUWA"). Pursuant to s.5(4) EUWA, the Charter is not part of domestic law on or after exit day. However, under s.5(5) EUWA, the exclusion of the Charter does not affect the retention in domestic law on or after exit day in accordance with EUWA of any fundamental rights or principles which exist irrespective of the Charter. The EUWA does not affect the obligations of the UK under ECHR, and the requirement that public authorities act compatibility with the ECHR in accordance with the HRA 1998.

C. GDPR AND DPA 2018

26. The GDPR, which regulates the processing of personal data, provides a legal framework for privacy and data protection. The recitals are important to the contextual and teleological interpretation of the operative provisions of the GDPR. The following are relevant here:

(1) Recital 26 states that the principles of data protection apply to information concerning an identified or identifiable person and not anonymous information or personal data rendered anonymous. This requires *"account to be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identity the natural person directly or indirectly"*.

(2) Recital 35 explains that the meaning of *"data concerning health"* includes a number or symbol which uniquely identifies a person for health purposes.

(3) Recitals 46 and 52-54 refer to circumstances in which the processing of special categories of personal data, including data concerning health, is lawful, e.g. where it is necessary for reasons of the public interest such as the "*monitoring epidemics and their spread*" and "*the management of health or social care services and systems*".

27. Article 1 indicates that the GDPR applies to the processing of "*personal data*".

28. Article 4 defines "personal data" as follows:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

29. Article 5 sets out the six principles relevant to the processing of personal data:

1 Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

30. Article 6 provides that processing of personal data is lawful in certain circumstances:

6(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; …

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

31. Article 9 prohibits the processing of special categories of personal data, including data concerning health, unless one of the exceptions in sub-paragraph 2 is satisfied:

9(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

9(2) Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; …

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; …

9(3) Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

9(4) Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

32. Articles 12 to 22 set out the rights of the data subject, including (amongst other things) the right to be informed of the processing of personal data.

33. Article 23 sets out the exceptions which allow Member States to restrict those rights. This includes where restriction of rights is a necessary and proportionate measure to safeguard public security (Article 23(1)(c)); other important objectives of general public interest of the EU or of a Member State, including public health (Article 23(1)(e)); or the protection of the data subject or the rights and freedoms of others (Article 23(1)(i)).

34. Article 25 specifies the requirements for data protection by design and default:

25(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention *to an indefinite number of natural persons.*"

35. Article 35 requires the data controller to undertake a data processing impact assessment ("DPIA") prior to processing where the type of processing is likely to result in a high risk to the rights and freedoms of individuals.

36. The DPA 2018 adapts and supplements the GDPR for UK domestic purposes.

37. Section 10 DPA 2018 sets out additional conditions relating to the processing of special categories of personal data set out in Article 9(1) of the GDPR, including data concerning health:

(1) Pursuant to s.10(2), processing meets the requirements of Articles 9(2)(h) or 9(2)(i) of the GDPR if it satisfies a condition in the paragraphs of Part 1 of Schedule 1 of DPA 2018:

(a) Paragraph 2 of Schedule 1 DPA 2018 is satisfied where processing is necessary for health or social care purposes.

(b) Paragraph 3 of Schedule 1 DPA 2018 is satisfied where processing is necessary for reasons of public interest in the area of public health and is carried out by or under the responsibility of a health professional or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(2) Pursuant to s.10(3), processing meets the requirements of Article 9(2)(g) of the GDPR only if it meets a condition in Part 2 of Schedule 1 of DPA 2018. In this regard, paragraph 6 of Schedule 1 is satisfied where processing is necessary in the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.

38. Part 3 of the DPA 2018 provides for the processing of personal data by competent authorities for criminal law enforcement purposes, implementing Directive 2016/680/EC. Law enforcement "competent authorities" under Schedule 7 of the DPA 2018 include not only police and prosecuting authorities, but *"any United Kingdom government department other than a non-ministerial government department"*.

D. E-PRIVACY DIRECTIVE

39. The protection of privacy is regulated by the E-Privacy Directive, which complements and particularises relevant provisions in the GDPR. The E-Privacy Directive is implemented in domestic law by the Privacy and Electronic Communications (EC Directive) Regulations 2003/2426.

40. Article 5(1) sets out the general principle of confidentiality of communications and related traffic data. Article 5(3) provides that the use of electronic communications networks to store or gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with the GDPR about (amongst other things) the purposes of the processing, and is offered the right to refuse such processing by the data controller.

41. Articles 6 and 9 require that, absent consent or the operation of Article 15(1), traffic data and location data must be erased or anonymised after a communication has taken place, except for the purpose of billing.

42. Article 15 provides an exemption in relation to legislative measures restricting the rights under Articles 5, 6 and 9 where it is a necessary, appropriate and proportionate measure (amongst other things) to safeguard public security:

> 15 Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

43. In Case C-275/06 ***Promusicae***, 29 January 2008, which concerned Telefónica's refusal to disclose the identities of persons who accessed phonograms in which the members of Promusicae had intellectual property rights, the CJEU at §§49-54 noted that, by the reference to Article 13(1) of Directive 95/46 (now Article 23 of the GDPR) in Article 15(1) of the E-Privacy Directive, Member States were entitled to adopt measures to restrict the obligation in Article 5(1) where it was necessary for the protection of the rights and freedoms of others (even though Article 15(1) did not include an exemption for situations that may give rise to civil proceedings). The same is likely to apply in respect of the other restrictions enumerated in Article 23 of the GDPR, set out at §33 above.

E. WHEN IS DATA "PERSONAL DATA"?

44. The definition of "personal data" under Article 4(1) of the GDPR and s.3(2) and (3) of the DPA 2018 requires that the data concerned must relate to a "data subject" – i.e. an "identified or identifiable natural person". Data can be considered "personal data" for the purposes of the EU/UK data protection regime by two possible routes: (a) indirect identification; or (b) individuation: see, e.g., *Bridges* at §115.

45. The first route, indirect identification by reference to further information that may come to be in the possession of the data controller, was considered by the CJEU in Case C-582/14 *Breyer v. Bundesrepublik Deutschland*, 19 October 2016. That case involved the storage of "dynamic" IP addresses (i.e. IP addresses which change with each new connection to the internet) by the Federal Republic of Germany each time Mr Breyer accessed internet sites run by the German

Federal institutions. The operators of the websites could identify Mr Breyer only if additional information was communicated by his internet service provider.

46. The CJEU noted that there is no requirement, for information to be treated as "*personal data*", for all the information enabling identification of the data subject to be in the hands of one person (§§43-44). The relevant question was whether the possibility of combining that information constituted "*a means likely reasonably to be used to identify the data subject*", which required considering whether identification of the data subject was "*prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant*" (§§45-46).

47. The CJEU concluded that the dynamic IP address constituted personal data because the operator had the means which may likely reasonably be used to identify the data subject with additional data which the internet service provider has about that person (§§48-49). See also Case C-434/16 *Nowak v. Data Protection Commissioner*, 20 December 2017 at §31; AG Bobek's Opinion in *Fashion ID v. Verbraucherzentrale NRW eV* [2020] 1 WLR 969 at §§56-58.

48. The second route for the identification of a person is if the data "individuates" that person. In *Vidal-Hall v. Google Inc* [2016] QB 1003, the Court of Appeal held that it was arguable (for the purposes of an application to serve proceedings out of the jurisdiction) that anonymous "BGI" or browser generated information (i.e. information about websites visited by a computer browser), constituted "personal data" for the purposes of s.1 of the Data Protection Act 1998 (§§106-133). The Court cited the Article 29 Working Party's Opinion (No 4/2007) on the concept of personal data, which stated (emphasis added):

> "In general terms, a natural person can be considered as 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group. Accordingly, the natural person is 'identifiable' when, although the person has not been identified yet, it is possible to do it … At this point, it should be noted that, <u>while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other 'identifiers' are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user.</u> Thus the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even inquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. <u>In other words, the possibility of identifying an individual no longer necessarily means the</u>

ability to find out his or her name. The definition of personal data reflects this fact … The European Court of Justice has spoken [in Criminal proceedings against Lindqvist (Case C-101/01 [2004] QB 1014 , para 27] in that sense when considering that 'referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data … within the meaning of … Directive 95/46/EC '. […]

The Working Party has considered IP addresses as data relating to an identifiable person. It has stated that 'internet access providers and managers of local area networks can, using reasonable means, identify internet users to whom they have attributed IP addresses as they normally systematically 'log' in a file the date, time, duration and dynamic IP address given to the internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of article 2(a) of the Directive."

49. The Court of Appeal at §115 rejected the submission that BGI was anonymous in that it neither named nor identified any person:

> "We think the case that the BGI constitutes personal data under section 1(1)(a) of the 1998 Act is clearly arguable: it is supported by the terms of the Directive, as explained in the working party's opinion, and the decision of the Court of Justice in the Lindqvist case (Case C-101/01) [2004] QB 1014 . […] The case for the claimants in more detail is this. If section 1 of the 1998 Act is appropriately defined in line with the provisions and aims of the Directive, identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others. It is immaterial that the BGI does not name the user"

50. The Court of Appeal considered that it was arguable that "*the BGI on its own identifies"* the claimants (§121). There was no conclusive determination of that issue as the claims were compromised.

F. RELATIONSHIP BETWEEN THE EU CHARTER AND DATA PROTECTION REGIME

51. The relationship between fundamental rights contained in Articles 7, 8 and 52 of the Charter and the EU data protection regime has been considered on a number of occasions, with the Court of Justice of the European Union laying down the minimum safeguards required where there has been an interference with the right to privacy and the protection of personal data, similar to those set out by the European Court of Human Rights and applying that case law by analogy.

Digital Rights Ireland

52. In Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April 2014, the CJEU held that Directive 2006/24/EC ("Data Retention Directive"), which required the retention of communications traffic and location data by network and service providers to allow competent national authorities to have access to that data for the purposes of fighting serious crime, was invalid. The CJEU at §§32-37 found there was a "*particularly serious"* interference with the rights under Articles 7 and 8 of the Charter, and the system for the protection of the right to privacy under Directive 95/46 (the predecessor of the GDPR) and the E-Privacy Directive.

53. The following principles are relevant:

(1) Any review of legislation interfering with data protection rights is strict, in view of the importance of the protection of personal data and the seriousness of the interference with that right. Derogations and limitations in relation to the protection of personal data must apply only insofar as strictly necessary (§§47-48, 52-53).

(2) The pursuit of an objective of general interest, such as the fight against serious crime, does not *in itself* mean the retention of personal data is necessary, irrespective of how fundamental that objective may be (§51).

(3) Legislation must lay down clear and precise rules governing the scope and application of the measure and impose minimum safeguards so that persons concerned have sufficient guarantees to protect their personal data against the risk of abuse and against any unlawful access and use of that data. The need for safeguards is greater where personal data is subjected to automatic processing and there is a significant risk of unlawful access to that data (§§54-55).

(4) There must be a relationship between the data retained and the objective pursued (§59).

(5) The legislation must lay down objective criteria by which to determine the limits of access to that data by competent authorities and the subsequent use of the data (§§60-61).

(6) The data concerned must not be retained beyond its usefulness for the objective pursued or according to the persons concerned. The determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary (§§63-64).

54. In that case the CJEU concluded that, whilst the data retention scheme genuinely satisfied an objective of general interest, the interference was disproportionate to the legitimate objectives

pursued by the Directive (§§56-69). The principles set out by the ECtHR were applied by analogy in interpreting the scope of Articles 7 and 8 of the Charter (§§54-55).

Re EU-Canada PNR Agreement

55. The principles in *Digital Rights Ireland* were re-stated in Opinion 1/15 *Re EU-Canada Passenger Name Record (PNR) Agreement* [2018] 1 CMLR 36, concerning the legality of the agreement envisaged between the EU and Canada on the continuous transfer of passenger name record (PNR) data with a view to that data being used and retained for the purpose of combating terrorism and forms of serious transnational crime.

56. The CJEU held that, in order to satisfy the principle of proportionality, the legislation must (amongst other things) indicate the circumstances and the conditions in which the measure applied, thereby ensuring that the interference is limited to what is strictly necessary. The considerations apply particularly where the protection of sensitive data is at stake (§§140-141, 190-191).

Tele 2 Sverige / Watson

57. In Joined Cases C-203/15 and C-698/15, *Tele 2 Sverige / Watson*, 21 December 2016, the CJEU considered the lawfulness of national legislation that permitted general and indiscriminate retention of all traffic and location data of subscribers and registered users of electronic communications, without exception, for the purpose of fighting crime.

58. The CJEU held that Article 15(1) of the E-Privacy Directive, read with Articles 7, 8, 11 and 52(1) of the Charter, precluded such national legislation.

59. However, Article 15(1) did not prohibit legislation permitting more targeted retention of location and traffic data, provided that the following criteria were satisfied:

    (1) The retention of data must be limited, with respect to categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted, to what was strictly necessary (§108).

    (2) The national legislation must lay down clear and precise rules governing the scope and application of the measure and impose minimum safeguards to ensure that the persons concerned have sufficient guarantees of protection of their personal data against the risk of misuse (§§109, 117-118).

(3) The data retained and the objective pursued must be sufficiently connected and the conditions governing access to that data circumscribe, in practice, the extent of the measure and the public affected (§110).

(4) The legislation must be based on objective evidence which makes it possible to identify the public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and contribute in one way or another to fighting serious crime or to preventing serious risk to public security (§111). The access to retained data must be restricted solely to the objective pursued (§125).

(5) Except in cases of validly established urgency, access of the competent authorities to the data concerned must be subject to prior review by a court or an independent administrative authority whose decision is made in response to a reasoned request by the competent authority (§120).

60. Following *Tele2/Watson*, the CJEU has confirmed that the objective pursued by access to the data must be proportionate to the seriousness of the interference with the fundamental rights of the person whose data is concerned. (see Case C-207/16 *Ministerio Fiscal*, 2 October 2018 at §§53-57 and also the Opinion of AG Campos Sanchez-Bordona in Case C-623/17 *Privacy International* at §§135-139.)

G. HEALTH AND SOCIAL CARE ACT 2012

61. Section 254 of the Health and Social Care Act 2012 ("2012 Act") enables the Secretary of State for Health and Social Care and NHS England to direct the Health and Social Care Information Centre (now known as NHS Digital) to establish and operate a system for the collection or analysis of information:

254(1) The Secretary of State or the Board may direct the Information Centre to establish and operate a system for the collection or analysis of information of a description specified in the direction.

(2) A direction may be given under subsection (1) by the Secretary of State only if –

(a) the Secretary of State considers that the information which could be obtained by complying with the direction is information which it is necessary or expedient for the Secretary of State to have in relation to the exercise by the Secretary of State of the Secretary of State's functions in connection with the provision of health services or of adult social care in England, or

(b) the Secretary of State otherwise considers it to be in the interests of the health service in England or of the recipients or providers of adult social care in England for the direction to be given.

(3) A direction may be given under subsection (1) by the Board only if the Board considers that the information which could be obtained by complying with the direction is information which it is necessary or expedient for the Board to have in relation to its exercise of functions in connection with the provision of NHS services.

…

(6) A function conferred by a direction given by the Secretary of State or the Board under subsection (1) is subject to directions given by the Secretary of State or (as the case may be) the Board about the Information Centre's exercise of the function.

H. NATIONAL HEALTH SERVICE ACT 2006 AND THE COPI REGULATIONS

62. Section 251(1) of the National Health Service Act 2006 ("NHSA 2006") confers a power on the Secretary of State to make regulations "*requiring or regulating the processing of prescribed patient information for medical purposes as he considering necessary or expedient in the interests of improving patient care or in the public interest.*" The provision is qualified as follows:

251(4) Regulations under subsection (1) may not make provision requiring the processing of confidential patient information for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such regulations, having regard to the cost of and the technology available for achieving that purpose.

…

251(7) Regulations under this section may not make provision for or in connection with the processing of prescribed patient information in a manner inconsistent with any provision of the data protection legislation.

63. The Health Service (Control of Patient Information) Regulations 2002 ("the COPI Regulations"), were made under s.60 of the Health and Social Care Act 2001, which was the predecessor of s.251 of the NHSA 2006.

64. Regulation 3 of the COPI Regulations sets out the circumstances in which confidential patient information may be processed:

3(1) Subject to paragraphs (2) and (3) and regulation 7, confidential patient information may be processed with a view to –

(a) diagnosing communicable diseases and other risks to public health;

(b) recognising trends in such diseases and risks;

(c) controlling and preventing the spread of such diseases and risks;

(d) monitoring and managing –

(i) outbreaks of communicable disease;

(ii) incidents of exposure to communicable disease;

(iii) the delivery, efficacy and safety of immunisation programmes;

(iv) adverse reactions to vaccines and medicines;

(v) risks of infection acquired from food or the environment (including water supplies);

(vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.

(2) For the purposes of this regulation, "processing" includes any operations, or set of operations set out in regulation 2(2) which are undertaken for the purposes set out in paragraph (1).

(3) The processing of confidential patient information for the purposes specified in paragraph (1) may be undertaken by –

(a)…

(b) persons employed or engaged for the purposes of the health service;

(c) other persons employed or engaged by a Government Department or other public authority in communicable disease surveillance.

(4) Where the Secretary of State considers that it is necessary to process confidential patient information for a purpose specified in paragraph (1), he may give notice to any body or person specified in paragraph (3) to require that body or person to process that information for that purpose and any such notice may require that the information is processed forthwith or within such period as is specified in the notice.

65. Regulation 7 of the COPI Regulations sets out the restrictions and exclusions on the processing of confidential medical information:

7(1) Where a person is in possession of confidential patient information under these Regulations, he shall not process that information more than is necessary to achieve the purposes for which he is permitted to process that information under these Regulations and, in particular, he shall –

(a) so far as it is practical to do so, remove from the information any particulars which identify the person to whom it relates which are not required for the purposes for which it is, or is to be, processed;

(b) not allow any person access to that information other than a person who, by virtue of his contract of employment or otherwise, is involved in processing the information for one or more of those purposes and is aware of the purpose or purposes for which the information may be processed;

(c) ensure that appropriate technical and organisational measures are taken to prevent unauthorised processing of that information;

(d) review at intervals not exceeding 12 months the need to process confidential patient information and the extent to which it is practicable to reduce the confidential patient information which is being processed;

(e) on request by any person or body, make available information on the steps taken to comply with these Regulations.

(2) No person shall process confidential patient information under these Regulations unless he is a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(3) For the purposes of paragraph (2) "health professional" has the same meaning as in section 69(1) of the Data Protection Act 1998."

66. In *Lewis v. Secretary of State for Health* [2008] EWHC 2196 (QB) at §§46-49, Foskett J stated (obiter) that the COPI Regulations do not extend to confidential information generated outside the NHS and could only be used to regulate the disclosure of patient information which has been generated within the NHS:

> "46. Against that background, and bearing in mind that the 2001 Act and its successor, the 2006 Act, appear to set out to ensure a proper framework by which patient information generated within the NHS may be distributed, the natural assumption is that the information to which the Act and the consequent Regulations apply is indeed information arising when a patient is seen within an NHS context. …
>
> 47. I have noted that Mr Jones argues that the Act and Regulations are not restricted to management issues within the NHS and that, accordingly, patient information could, as I understood his argument, be processed for the purposes of the management of private health services if the appropriate authority was given.
>
> 48. I respectfully agree that there is nothing explicit in the Act and or Regulations confining the information concerned to NHS-generated information but, as I have said, the whole context would seem to suggest this. Had the matter been fundamental, I would doubtless have been invited to look more closely at the whole Act, and, perhaps, its legislative history and background. In the course of the relatively short argument, I have not been so invited and, accordingly, can express no view other than that which I have expressed.

49. If I was forced to conclude, on the arguments I have heard, whether the procedures afforded by the Act and the Regulations are available for the authorisation of the use of confidential patient information generated outside the NHS, I would have to conclude that it did not." (emphasis in text)

ANNEX 3: SUMMARY OF STATEMENTS ON SMARTPHONE CONTACT TRACING BY ICO AND OTHERS

The Information Commissioner's Opinion

67. On 17 April 2020, the Information Commissioner issued an Opinion on the Apple / Google Initiative, concluding that:[77]

(1) The Apple / Google Initiative was aligned with the principles of data protection by design and default, on the basis that it was designed to only generate a limited amount of data from the user's Bluetooth identifier keys; upload the keys from a COVID-19 diagnosed user to the server and notify other users from that server, with the process only matching keys stored on a particular device (with the match only occurring on the device). It supported the development of apps that protect their users' identities, both before the risk of infection has been identified and when a notification is made via the app.

(2) The Apple / Google Initiative complied with the data minimisation and security principles and facilitated user control by ensuring that the installation of the app was voluntary, and that the uploading of Bluetooth keys required separate user consent. Certain matters relating to consent were unclear and must be addressed, e.g. the impact of consent withdrawal on the effectiveness of contact tracing and any notifications provided to other app users once a user diagnosed.

(3) However, if contact tracing apps are designed to use the Apple / Google API, but to collect data and use techniques beyond those envisaged by the Apple / Google Initiative, the data controller should ensure that it assessed the data protection implications of processing and that the processing is fair, lawful and transparent. There is an additional risk that third-party developers may also expand the use of apps beyond the stated purpose of contact tracing for the response to the COVID-19 pandemic.

(4) The processing of additional data may be legitimate and necessary to support the public health utility of a contact tracing app (e.g. to prevent false positives or assess compliance with isolation), but this would need to be assessed on a case-by-case basis and may involve a separate DPIA.

---

77 Information Commissioner's Opinion, 'Apple and Google joint initiative on COVID-19 contact tracing technology' (17 April 2020).

68. The Commissioner noted the similarity between the Apple / Google Initiative and DP-3T and noted that her views on the Apple / Google Initiative were equally applicable to the DP-3T proposal.

European Data Protection Board

69. On 19 March 2020, the European Data Protection Board ("EDPB") made a statement on the use of mobile location data, urging Member States to adopt the least intrusive solutions and robust safeguards:

> "In some Member States, governments envisage using mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19. This would imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area by phone or text message. Public authorities should first seek to process location data in an anonymous way (i.e. processing data aggregated in a way that individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ("cartography"). Personal data protection rules do not apply to data which has been appropriately anonymised. When it is not possible to only process anonymous data, the e-Privacy Directive enables Member States to introduce legislative measures to safeguard public security (Art. 15). If measures allowing for the processing of non-anonymised location data are introduced, a Member State is obliged to put in place adequate safeguards, such as providing individuals of electronic communication services the right to a judicial remedy.
>
> The proportionality principle also applies. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved. Invasive measures, such as the "tracking" of individuals (i.e. processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing. However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation)."

70. On 14 April 2020, following a request for consultation on contact tracing apps from the European Commission, the EDPB responded as follows:

(1) A contact tracing app which involved the collection of location data would violate the principle of data minimisation and create major security and privacy risks. The Commission endorsed this approach in their response following the consultation.

(2) A centralised or decentralised model might be valid alternatives, provided that adequate security measures are in place. However, the decentralised solution is more aligned with the data minimisation principle.

(3) Any automatic processing involved in contact tracing apps should work under the strict supervision of qualified personal in order to limit the occurrence of any false positives or negatives.

(4) Any data stored should not allow the re-identification of any other persons and should, in any event, be erased as soon as possible. After the COVID-19 pandemic is over, the system should not remain in use and the data collected should be erased or anonymised.

71. On 21 April 2020, the EDPB published guidelines on the use of location data and contact tracing tools, recommending that:

(1) The app should not collect unrelated or unnecessary information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers etc. Any additional information required to put in place contact tracing should remain on the user terminal and should only be processed when strictly necessary and with prior consent.

(2) A centralised or decentralised approach may be appropriate, provided that adequate security measures are in place and the effects on data protection/privacy of either alternative are properly considered.

(3) Any server must only collect the contact history or pseudonymous identifiers of an infected user as a result of a proper assessment made by health authorities and voluntary action, or only for the time to inform potentially infected users of their exposure.

(4) The reporting of users as COVID-19 infected on the app must be subject to proper authorisation by a test station or health care professional.

European Commission

72. On 8 April 2020, the European Commission issued a recommendation on the development of a common EU Toolbox of technological measures to address the COVID-19 pandemic, focusing on:[78]

(1) the use of apps for (amongst other things) contact tracing; and

[78] Commission Recommendation of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.

(2) the use of anonymised and aggregated data on mobility of populations in order to (a) model and predict the evolution of the disease; (b) monitor the effectiveness of social distancing and confinement; and (c) inform a co-ordinated strategy for exiting from the crisis.

73. The Commission's Toolbox was published on 16 April 2020.[79] The Commission noted that Member States must ensure that strong safeguards are in place to guarantee respect for privacy and data protection and the prevention of surveillance and stigmatisation, including but not limited to:

(1) voluntary installation, with clear and complete guidelines on the intended use and processing of the data collected;

(2) ensuring only authorised parties (e.g. public health authorities or laboratories) are entitled to confirm an infection and trigger a warning alert, e.g. by providing a QR code or sending a notification to enable the user to trigger a warning alert;

(3) automated/gentle self-dismantling, including deletion of all remaining personal data;

(4) safeguards to prevent the stigmatization of infected persons or close contacts of infected persons;

(5) safeguards to ensure the storing of proximity data on the device and encryption.

74. Subject to the applicable data protection regime, the Commission also stated that public health authorities may use anonymised or aggregated data from contact tracing to learn more about the transmission dynamics and adapt the public health response, and share that data with relevant health authorities and/or the EDPB to assist the understanding of the epidemic and transmissions dynamics.

European Parliament

75. On 17 April 2020, the European Parliament adopted a resolution on EU coordinated action to combat the COVID-19 pandemic and its consequences. Paragraph 52, on contact tracing apps, endorsed a decentralised approach to storage of the data concerned:

---

79 European Commission, 'Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States' (15 April 2020) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf> (accessed on 19 April 2020).

> "Takes note of the emergence of contact-tracing applications on mobile devices in order to warn people if they were close to an infected person, and the Commission's recommendation to develop a common EU approach for the use of such applications; points out that any use of applications developed by national and EU authorities may not be obligatory and 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; demands that all storage of data be decentralised, full transparency be given on (non-EU) commercial interests of developers of these applications, and that clear projections be demonstrated as regards how the use of contact tracing apps by a part of the population, in combination with specific other measures, will lead to a significantly lower number of infected people; demands that the Commission and Member States are fully transparent on the functioning of contact-tracing apps, so that people can verify both the underlying protocol for security and privacy, and check the code itself to see whether the application functions as the authorities are claiming; recommends that sunset clauses are set and the principles of data protection by design and data minimisation are fully observed."

Joint Statement on Contact Tracing by Scientists and Academics

76. On 19 April 2020, a number of scientists and researchers issued a joint statement on contact tracing. The statement expressed support for a decentralised approach and warned against the risks of "mission creep" of any proposal of contact tracing:[80]

> "Research has demonstrated that solutions based on sharing geolocation (i.e., GPS) to discover contacts lack sufficient accuracy and also carry privacy risks because the GPS data is sent to a centralized location. For this reason, Bluetooth-based solutions for automated contact tracing are strongly preferred when available.
>
> Some of the Bluetooth-based proposals respect the individual's right to privacy, whilst others would enable (via mission creep) a form of government or private sector surveillance that would catastrophically hamper trust in and acceptance of such an application by society at large. It is crucial that citizens trust the applications in order to produce sufficient uptake to make a difference in tackling the crisis. 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, either now or at a later time. Thus, solutions which allow reconstructing invasive information about the population should be rejected without further discussion. Such information can include the "social graph" of who someone has physically met over a period of time. …
>
> There are a number of proposals for contact tracing methods which respect users' privacy, many of which are being actively investigated for deployment by different countries. We urge all countries to rely only on systems that are subject to public scrutiny and that are privacy preserving by design (instead of there being an expectation that they will be managed by a trustworthy party), as a means to ensure that the citizen's data protection rights are upheld.
>
> The following principles should be at least adopted going forward:

---

[80] Joint Statement on Contact Tracing (19 April 2020) <https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view>

● Contact tracing Apps must only be used to support public health measures for the containment of COVID-19. The system must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose.

● Any considered solution must be fully transparent. The protocols and their implementations, including any sub-components provided by companies, must be available for public analysis. The processed data and if, how, where, and for how long they are stored must be documented unambiguously. Such data collected should be minimal for the given purpose.

● When multiple possible options to implement a certain component or functionality of the app exist, then the most privacy-preserving option must be chosen. Deviations from this principle are only permissible if this is necessary to achieve the purpose of the app more effectively, and must be clearly justified with sunset provisions.

● The use of contact tracing Apps and the systems that support them must be voluntary, used with the explicit consent of the user and the systems must be designed to be able to be switched off, and all data deleted, when the current crisis is over."

ANNEX 4: GOVERNMENT STATEMENTS ON DATA SHARING

Data Sharing under the Directions and COPI Notices

77. On 17 March 2020, the Secretary of State and NHS England directed NHS Digital to establish and operate a system for the collection and analysis of data in connection with "COVID-19 Purposes" ("the Directions"). Paragraph 2 sets out the COVID-19 Purposes:

- understanding Covid-19 and risks to public health, trends in Covid-19 and such risks, and controlling and preventing the spread of Covid-19 and such risks;
- identifying and understanding information about patients or potential patients with or at risk of Covid-19, information about incidents of patient exposure to Covid-19 and the management of patients with or at risk of Covid-19 including: locating, contacting, screening, flagging and monitoring such patients and collecting information about and providing services in relation to testing, diagnosis, self-isolation, fitness to work, treatment, medical and social interventions and recovery from Covid-19;
- understanding information about patient access to health services and adult social care services as a direct or indirect result of Covid-19 and the availability and capacity of those services;
- monitoring and managing the response to Covid-19 by health and social care bodies and the Government including providing information to the public about Covid-19 and its effectiveness and information about capacity, medicines, equipment, supplies, services and the workforce within the health services and adult social care services;
- delivering services to patients, clinicians, the health services and adult social care services workforce and the public about and in connection with Covid-19, including the provision of information, fit notes and the provision of health care and adult social care services; and
- research and planning in relation to Covid-19.

78. Pursuant to paragraph 8, NHS Digital may, or may be required by the Secretary of State or NHS England to, disseminate information it has obtained by complying with the Directions to those persons or organisations who require it for COVID-19 Purposes, where it would be lawful for NHS Digital to do so.

79. The Directions extend until 31 March 2022, to be reviewed six months following the date they come into force and every six months thereafter, unless they replaced or revoked by written notice.

80. The Secretary of State also issued four notices pursuant to regulation 3(4) of the COPI Regulations to require NHS Digital to process confidential information for the purposes in regulation 3(1), in so far as those purposes related to the COVID-19 pandemic. The COPI Notices were issued to:

(1) NHS England & Improvement dated 20 March 2020 ("**COPI Notice 1**");

(2) NHS Digital dated 17 March 2020 ("**COPI Notice 2**");

(3) "Organisations providing health services, general practices, local authorities and arm's length bodies of the Department of Health and Social Care" dated 20 March 2020 ("**COPI Notice 3**");

(4) "All GP practices in England, whose IT systems are supplied by The Phoenix Partnership (TPP) or Egton Medical Information Systems (EMIS) or Egton Medical Information Systems (EMIS) […] to require them to release primary care patient data, in respect of UK Biobank's consented participants only, to UK Biobank" ("**COPI Notice 4**").

81. Pursuant to paragraph 1 of COPI Notices 1 to 3, the purpose of the Notices is to require organisations to process confidential patient information for the purposes set out in regulation 3(1) of the COPI Regulations. They are only required to do so where (amongst other things) they are reasonably satisfied that the information is required for, and will be used solely for, purposes related to the COVID-19 pandemic and in accordance with regulation 7 of the COPI Regulations.

82. The COPI Notices expire on 30 September 2020, unless they are extended by further written notice.

83. NHS Digital's COVID-19 response transparency notice refers to Articles 6(1)(e), 9(2)(g), 9(2)(h), 9(2)(i) of the GDPR and s.10 and Schedule 1 paras 2(2)(f), 3 and 6(1) of the DPA 2018 as the legal basis for processing personal data under the Directions and the COPI Notices.[81]

Creation of a Data Store

84. On 28 March 2020, NHSX published a blog post[82] explaining that the Government had commissioned NHS England and NHSX to developed a "*data platform*" or "*data store*" to provide those organisations with "*secure, reliable and timely data – in a way that protects the privacy of our citizens – in order to make informed, effective decisions.*" It stated that the data would remain under the control of NHS England:

---

81 NHS Digital, 'Coronavirus (COVID-19) response transparency notice' (20 March 2020) <https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/coronavirus-covid-19-response-transparency-notice> (accessed on 15 April 2020).

82 Gould et al, 'The power of data in a pandemic' (NHS Blog, 28 March 2020) <https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/> (accessed on 15 April 2020).

"All NHS data in the store will remain under NHS England and NHS Improvement's control. Once the public health emergency situation has ended, data will either be destroyed or returned in line with the law and the strict contractual agreements that are in place between the NHS and partners."

85. The confidentiality of data is said to be protected as follows:

"The data brought into the back end datastore held by NHS England and NHS Improvement will largely be from existing data sources e.g. data already collected by NHS England and NHS Improvement, Public Health England and NHS Digital. All NHS data remains under NHS England and NHS Improvement control.

All the data held in the platform is subject to strict controls that meet the requirements of data protection legislation. GDPR principles will be followed, for example the data will only be used for Covid-19 and not for any other purpose and only relevant information will be collected. Any request to access data will be reviewed through a single process controlled solely by NHS England and NHS Improvement and NHSX."

86. The blog post made clear that the private sector has been involved in creating the data store:

- **NHSX** along with **NHS England and Improvement** are leading on this project working with multiple partners leveraging internal skills and also skills from the wider NHS family. The team is being led by the Director of AI, Indra Joshi, and Ming Tang, Director of Data/Analytics, NHS England/Improvement
- **Microsoft** is supporting NHSX and NHS England's technical teams, who have built a backend data store on Microsoft's cloud platform, Azure, to bring multiple data sources into a single, secure location. A G-cloud data processing contract is in place.
- **Palantir Technologies UK** is providing the software, Palantir Foundry, that powers the front end data platform. Palantir Foundry, which has been primarily developed in the UK, enables disparate data to be integrated, cleaned, and harmonised in order to develop the single source of truth that will support decision-making. Foundry is built to protect data by design. A G-cloud data processing contract is in place. Palantir is a data processor, not a data controller, and cannot pass on or use the data for any wider purpose without the permission of NHS England.
- **Amazon Web Services** (**AWS**) is helping to provide infrastructure and technologies that are enabling NHSX and its partners to quickly and securely launch the new Covid-19 response platform for critical public services at a time when it is important for public and private sector organisations to work together to combat this crisis. AWS has the highest score awarded by the NHS Data Security & Protection (DSP) Toolkit.
- **Faculty** is a London-based AI technology specialist that has an existing partnership with NHSX and is now supporting the development and execution of the data response strategy. This includes developing dashboards, models and simulations to provide key central government decision-makers with a deeper level of information about the current and future coronavirus situation to help inform the response.
- **Google:** The NHS is exploring the use of tools in the G Suite family to allow the NHS to collect critical real-time information on hospital responses to Covid-19. Data collected would be aggregated operational data only such as hospital occupancy levels and A&E capacity. It will not include any form of identifiable patient data.

87. NHSX states that, once the COVID-19 pandemic is contained, the data will be "destroy[ed] or return[ed] to NHS England and NHS Improvement" but notes that "*we hope to be able to use what we have learned from our technology partners to get better within the Government at data collection, aggregation and analysis in a way that protects the privacy of our citizens*" and "*[h]aving relevant data to hand will make our systems more resilient and better able to respond immediately to the next crisis – or even predict it before it happens.*"